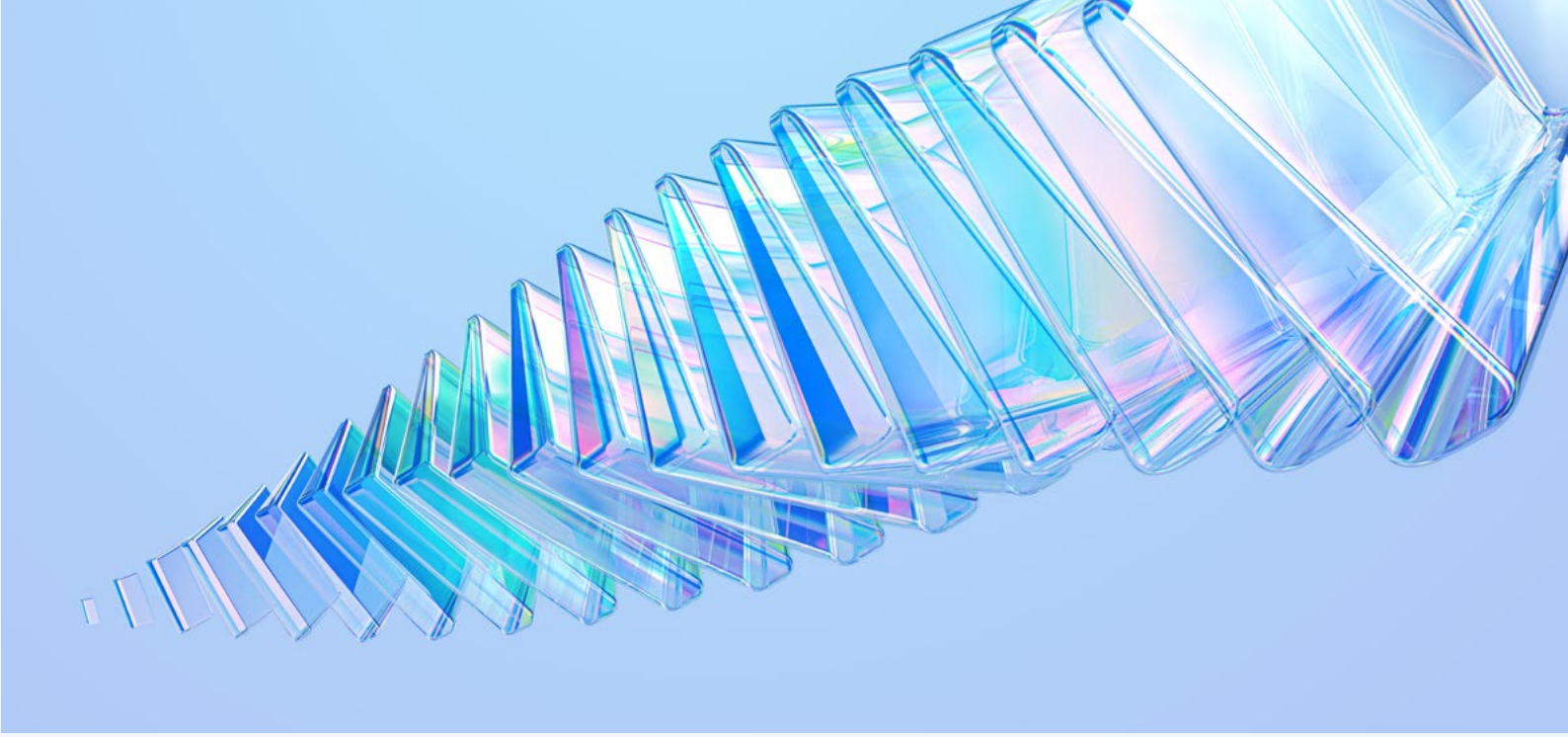
JET SECURITY TEAM

ИССЛЕДОВАНИЕ

КУРС НА АНТИХРУПКОСТЬ
СТРАТЕГИЧЕСКИЙ ОБЗОР КИБЕРУГРОЗ 2025

Инфосистемы Джет
JET.SU



АННОТАЦИЯ

Настоящий отчет представляет собой стратегический обзор киберугроз 2025 года, сформированный на базе практики реагирования и прогнозирования Jet CSIRT и экспертных команд «Инфосистемы Джет». Выводы основаны на ретроспективе расследованных атак в различных секторах.

2025 год стал проверкой пределов цифровой устойчивости: резонансные атаки на крупнейшие компании РФ показали хрупкость ИТ-архитектуры даже самых подготовленных игроков рынка — с высоким уровнем цифровизации и серьезными вложениями в ИБ.

Классическая, основанная на превентивных мерах модель безопасности, которая еще недавно демонстрировала надежность, теряет эффективность. Тренды 2025 года это подтверждают:

- более активное использование атакующими инструментов с поддержкой искусственного интеллекта, сокращающих затраты на атаку и снижающих требования к навыкам атакующего;
- коллаборации группировок, переиспользующих инфраструктуру друг друга;
- широкое использование собственных или переписанных инструментов для деструктивных воздействий на инфраструктуры, которые сложно обнаружить;
- активное использование скомпрометированных подрядчиков в качестве плацдарма для атаки.

Ситуация, в которой кризисы становятся катализатором развития, а работа под атакой и восстановление превращаются в управляемый процесс — новый уровень зрелости и ключевой фактор защиты от «черных лебедей», к которому постепенно двигается российский бизнес.

Тренды, приведенные в отчете, рассмотрены в контексте антихрупких[1] стратегий:

- Системное развитие и контроль
- Подготовка и прогнозирование
- Вовлечение и нападение
- Обнаружение и реагирование
- Защита, замедление, сдерживание
- Восстановление
- Адаптация и перестройка

Стратегии являются частью фреймворка Антихрупкой ИТ-архитектуры «Инфосистемы Джет». Фреймворк объединяет ключевые требования к инфраструктуре, кибербезопасности, сетям, чтобы помочь компаниям строить более устойчивые и защищенные системы.

[1] Антихрупкость ИТ позволяет принимать разнообразные удары (кибератаки, неожиданный уход вендоров, крупные аварии) с приемлемым для бизнеса ущербом, делать вывод из неприятностей и оперативно меняться.

КЛЮЧЕВЫЕ ВЫВОДЫ И ЦИФРЫ

01

По мере роста устойчивости компаний к DDoS-атакам и «обесценивания» дефейсов хакеры перешли к тактике «выжженной земли»: в **ТОП киберугроз**, ставших причиной нарушения работы бизнеса, вошли вирусы-шифровальщики (44%) и вайперы (32%), которые полностью уничтожают инфраструктуру.

02

Финансовые организации, компании в сфере недвижимости, а также ИТ-компании вошли в **ТОП-3 наиболее атакуемых отраслей** среди клиентов Jet CSIRT в 2025 году.

03

Основные причины взломов — уязвимости в общедоступных веб-приложениях, отсутствие мультифакторной аутентификации для внешних ресурсов, в том числе сервисов удаленного администрирования, атаки на подрядчиков и фишинг.

04

При **атаках на веб-приложения** 65% всех инцидентов связаны с проблемами в трех ключевых компонентах инфраструктуры: OpenSSH, Nginx и Apache HTTP Server.

05

В 83% компаний в рамках сканирования внешнего периметра выявлены **доступные административные интерфейсы**, из которых 19% использовали учетные данные по умолчанию. Вместе это даёт мгновенный и полный доступ к внутренней инфраструктуре без взлома.

06

Каждая вторая (53%) критическая уязвимость просканированных компаний **имела публичный эксплойт** и могла быть использована для немедленной атаки. В среднем по всем уязвимостям этот показатель составляет 29%.

07

У 40% фишинговых доменов, проиндексированных в 2025 году, **обнаружена MX-запись**. Это сигнал о профессионализации киберпреступности — злоумышленники вкладываются в настройку почтовой инфраструктуры, которая является «долгосрочным» инструментом для проведения фишинговых атак и коммуникации с потенциальными жертвами. Такие домены выглядят для систем защиты «чище», чем ретрансляция через публичные сервисы.

08

Мы фиксируем **снижение количества публикаций нелегитимных данных** более чем в два раза по сравнению с 2024 годом (с 328 до 158 уникальных инцидентов). При этом главным источником компрометации клиентских данных остается сектор электронной коммерции.

09

Пик напряженности по количеству DDoS-атак на российские компании пришелся на январь, май, сентябрь и октябрь 2025 года. Возможные причины — киберпреступные кампании, приуроченные к финансовым отчетам, праздникам или началу/ окончанию отчетных периодов, а также более низкая активность злоумышленников в летние месяцы. В ТОП-3 атакуемых отраслей вошли промышленность, телекоммуникации и финансовый сектор.

10

В среднем ежедневно **DDoS-атаками охвачено 1 466 хостов**, а в пиковые дни — до 8 532 хостов за сутки. Общее число уникальных атакованных хостов за год превысило 483,9 тысячи. Самая продолжительная атака длилась 10 дней.

11

Атакующие активно совершенствуются в использовании техник LOTL[2]: встроенные в ОС утилиты (powershell, bitsadmin или wmic) широко используются для мимикрии под легитимную активность.

12

Ключевым трендом становится «гибкая стратегия» — отказ от пяти-трехлетних горизонтов в пользу динамичных среднесрочных циклов (1–2 года). Руководители ИБ продолжают выбирать «осторожный» метод стратегического планирования, отдавая среди прочих предпочтение стратегии постепенного улучшения (60%).

13

В два раза выросло количество запросов на независимые аудиты систем резервного копирования. Создание защищенных хранилищ становится стандартным требованием при внедрении или модернизации СРК, что способствует увеличению спроса на объектные системы хранения (поддерживающие неизменяемость данных, Object Lock[3]) более чем в два раза.

14

Яркой тенденцией 2025 года стал **переход крупных компаний к регулярным тестовым восстановлениям данных** в изолированных контурах. Эта практику уже внедрили 74% организаций.

15

Компании продолжили наращивать финансирование систем непрерывности бизнеса и отработки действий при сбоях. Спрос на услуги по тестированию кризисного реагирования на кибератаки и разработке планов реагирования вырос более чем в два раза.

16

Наибольший интерес к киберучениям отмечается в финансовом секторе, государственных структурах и промышленных компаниях.

[2] Living Off The Land — стратегия использования легитимных инструментов операционной системы.

[3] Позволяет блокировать возможность логического удаления или изменения сохраненных копий в течение заданного периода, независимо от внешних действий (администраторов или вредоносного ПО).

АНТИХРУПКОСТЬ ИТ-АРХИТЕКТУРЫ — НОВЫЙ УРОВЕНЬ ЗРЕЛОСТИ РОССИЙСКОГО БИЗНЕСА

Антихрупкость в ИТ — концепция, согласно которой системы и компании должны быть спроектированы и построены таким образом, чтобы они не только выдерживали сбои и нарушения, но и извлекали из них пользу. Это способ достижения киберустойчивости, помогающий бизнесу выживать и становиться сильнее после ударов.

Традиционная парадигма информационной безопасности — «более высокие стены и широкие рвы» — долгое время базировалась на предотвращении атак и сейчас теряет свою эффективность. Чтобы заранее быть готовым к нападению, отреагировать до того, как злоумышленник нанесет ущерб, и быстро восстановиться, нужны комбинация и баланс разных стратегий защиты, смещение фокуса с превентивных мер в сторону мониторинга, восстановления и адаптации.

Мы сформулировали семь взаимосвязанных стратегий, которые должны быть в арсенале руководителя ИБ и которые легли в основу фреймворка Антихрупкой ИТ-архитектуры:

- Системное развитие и контроль
- Подготовка и прогнозирование
- Вовлечение и нападение
- Защита, замедление, сдерживание
- Обнаружение и реагирование
- Восстановление
- Адаптация и перестройка

Наша цель — дать сообществу открытый и практичный инструмент, который поможет эффективнее противостоять киберугрозам.

ФРЕЙМВОРК АНТИХРУПКОЙ ИТ-АРХИТЕКТУРЫ

ПОДГОТОВКА К ВТОРЖЕНИЮ

СТРАТЕГИИ

Системное развитие и контроль

Подготовка и прогнозирование

ПРИНЦИПЫ

[СР1]
Регулярно проверяет себя на прочность, непрерывно оценивает эффективность принятых мер, тренируется

[СР2]
Развивает ИБ оправданно с точки зрения экономики и нормальной работы бизнеса

[ПП1]
Понимает цену инцидента и объективно оценивает риски ИБ для бизнеса

[ПП2]
Знает своего врага (модель нарушителя)

СЛЕВА ОТ ВТОРЖЕНИЯ

СТРАТЕГИИ

Вовлечение и нападение

Защита, замедление, сдерживание

ПРИНЦИПЫ

[ВН1]
Деанонимизирует злоумышленников, применяет юридические меры

[331]
Внедряет изменения в ИТ и бизнес-процессы для достижения целей киберустойчивости

[332]
Поддерживает киберустойчивое состояние непрерывно

СПРАВА ОТ ВТОРЖЕНИЯ

СТРАТЕГИИ

Обнаружение и реагирование

Восстановление

ПРИНЦИПЫ

[ОР1]
Знает, как действовать на каждом этапе атаки, и имеет средства для этого

[В1]
Имеет «План Б» на случай катастрофического развития событий

ПОСЛЕ ВТОРЖЕНИЯ

СТРАТЕГИИ

Адаптация и перестройка

ПРИНЦИПЫ

[АП1]
Готова меняться в процессе достижения киберустойчивости и оперативно адаптировать свою работу в процессе отражения атаки

ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ

Проактивное управление инцидентами кибербезопасности

В 2025 году за период с января по конец ноября Центр мониторинга и реагирования на инциденты Jet CSIRT зафиксировал более 10 тысяч инцидентов ИБ. Хотя количественные показатели по числу инцидентов ИБ в 2025 году остались на уровне 2024-го, качественная картина угроз претерпела значительные изменения.

Наша команда в 2,5 раза чаще привлекалась к расследованию «громких» инцидентов, которые оказывали стратегическое влияние на системозначимые отрасли — от массовых к целевым операциям с высокой степенью подготовки, показавших хрупкость ИТ-архитектуры даже самых подготовленных игроков, с высоким уровнем цифровизации и серьезными вложениями в ИБ.

Ринат Сагиров,

руководитель департамента мониторинга и реагирования

Отмечается важный сдвиг в характере наших услуг по реагированию. Работа все чаще носит сквозной характер: от первичного анализа до комплексного восстановления. Мы регулярно участвуем в реабилитации инфраструктуры клиентов, помогая воссоздавать ее после серьезных инцидентов, когда требуется практически полное развертывание заново. А также закладываем фундамент антихрупкой архитектуры для ее дальнейшего развития и совершенствования.

Большинство инцидентов, которые фиксирует Jet CSIRT, анализируются с помощью SIEM/EDR/LM-систем, позволяющих делать запросы к историческим событиям и видеть общую картину инцидента. Ниже представлено распределение фиксируемых нами угроз по самым популярным категориям инцидентов Jet CSIRT, отражающее картину за год. В 2025 году очевидный пик напряженности пришелся на два периода — середина весны и последний квартал года.

Мартовский пик сформирован в основном инцидентами, связанными с заражением ВПО, вирусными эпидемиями или обнаружением нежелательных программ (в основном — AdWare, подозрительные браузерные расширения и переходы пользователями по подозрительным ссылкам).

Категория	ЯНВ	ФЕВ	МАР	АПР	МАЙ	ИЮН	ИЮЛ	АВГ	СЕН	ОКТ	НОЯ
[MI] Заражение вредоносным ПО											
[MNA] Вредоносная сетевая активность											
[NSA] Несанкционированный доступ к системам											

На первое место по числу атак среди клиентов сервиса Jet CSIRT вышли организации в сфере недвижимости (занимали второе место в 2024 году). Финансовые организации сместились на второе место и стабильно остаются в ТОП-3 уже четвертый год. Высокая стоимость данных, большое количество точек входа и возможность быстрой финансовой выгоды делают финансовый сектор одной из постоянно атакуемых отраслей.

Замыкают тройку лидеров IT-компании, которые, как правило, имеют непосредственный доступ в инфраструктуры более крупных организаций для оказания сервисных услуг. Значительная доля расследованных нами атак произошла по причине компрометации таких подрядных организаций.

Заражение вредоносным ПО

Случаи заражения хостов в защищаемом периметре в результате внешних атак, например, фишинга, а также обнаружение индикаторов компрометации в защищаемом периметре.

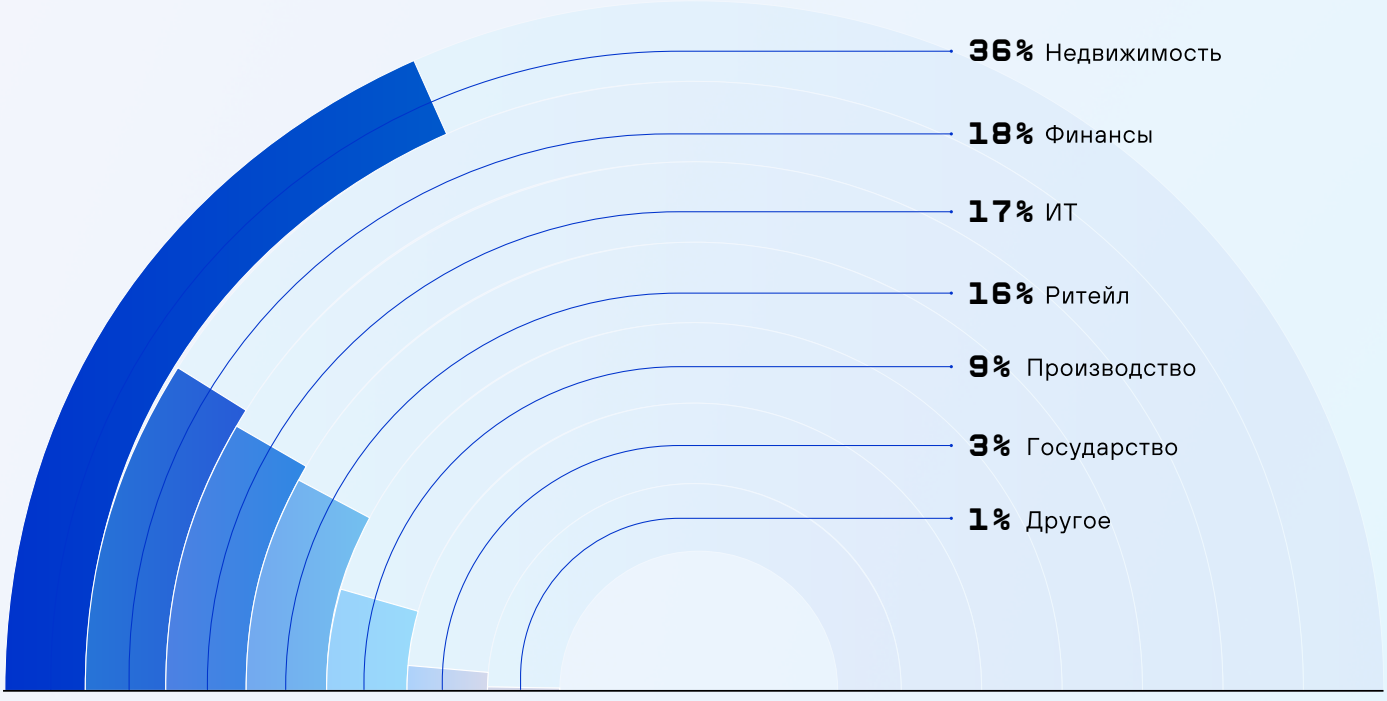
Вредоносная сетевая активность

Потенциально опасные внешнее попытки сетевого сканирования, выявление сетевых атак на периметр. Зачастую инциденты в данной категории выявляются благодаря интеграции сервисов Threat Intelligense.

Несанкционированный доступ к системам

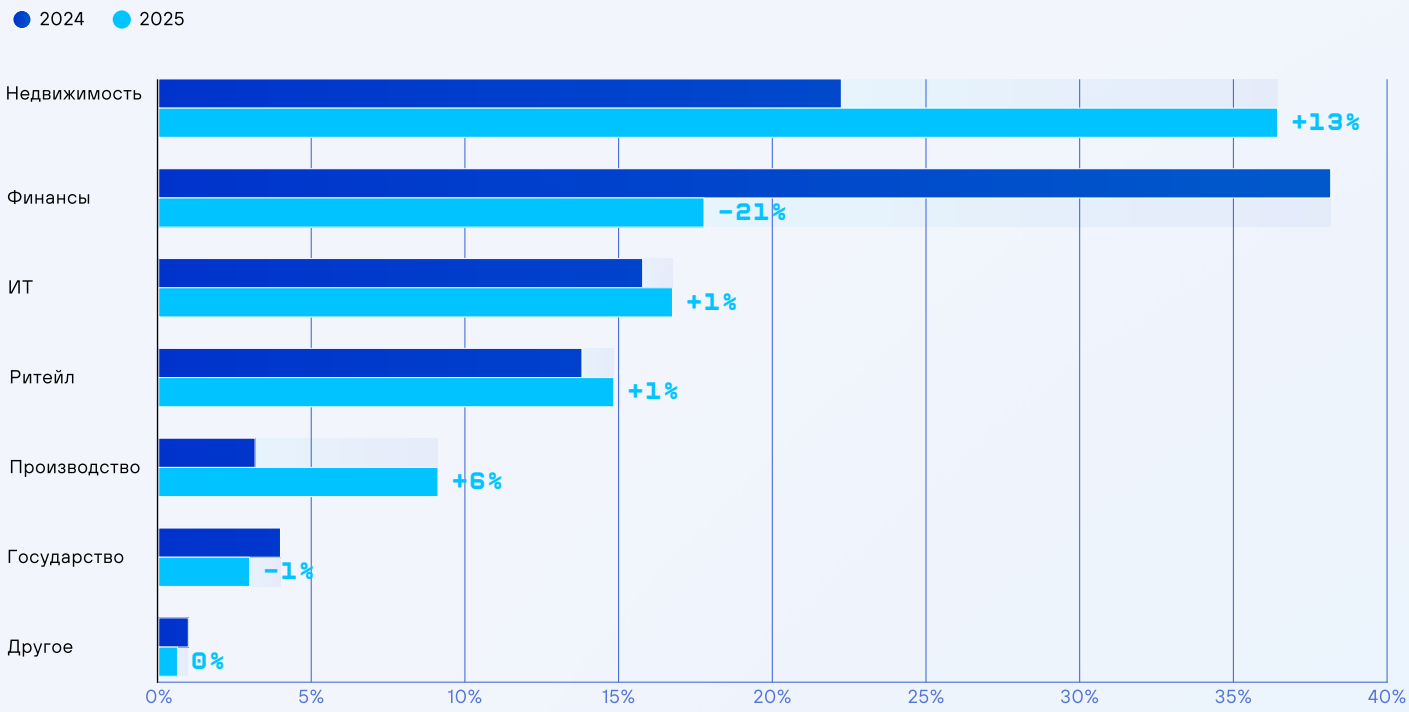
Инциденты, связанные с модификацией привилегий УЗ, их созданием и удалением, изменением состава ПО или другими изменениями конфигурации улов и СЗИ.

Распределение инцидентов по отраслям среди клиентов сервиса Jet CSIRT[4]



[4] Распределение основано на результатах обработки инцидентов, произошедших в инфраструктурах именно наших клиентов.

Сравнение инцидентов в отраслях по годам



Мы составили ежегодный список из ТОП-10 наиболее распространенных техник MITRE ATT&CK, которые чаще всего использовали атакующие. Данные получены в результате срабатывания правил корреляции, настроенных на выявление аномальной активности в компаниях, которые доверили нам защиту своей инфраструктуры.

Mitre_ID	Mitre_Name	ТОП-10 техник 2025 (%)
T1204	User Execution	43%
T1190	Exploit Public-Facing Application	19%
T1219	Brute Force: Password Guessing/ Password Spraying	12%
T1021	Exploitation for Defense Evasion	9%
T1562.001	Application Layer Protocol: Web Protocols	5%
T1071	Impair Defenses: Disable or Modify Security Tools	4%
T1110.001	Remote Access Software	3%
T1133	Proxy: Multi-hop Proxy	2%
T1046	Network Service Discovery	2%
T1090.003	External Remote Services	1%

Рейтинг техник достаточно сильно изменился по сравнению с 2024 годом. На первом месте, как и в прошлом году, находятся инциденты, связанные с действиями пользователей, приведших к заражению вредоносным ПО. Мы объединили в данном пункте все техники User Execution, но в основном — это подтехники T1204.001 (Malicious Link) и T1204.002 (Malicious File).

На втором месте остаются атаки публично-доступных веб-приложений, а на третье место поднялись инциденты, связанные с перебором паролей. В прошлом году в ТОП попала только техника T1110.001 (Brute Force: Password Guessing), в этом же периоде был заметный прирост Password Spraying, поэтому мы объединили их и расположили на третьем месте.

Mitre_ID		Mitre_Name	2025	Mitre_ID	Название техники	2024
T1204		User Execution		T1204	User Execution	
T1190		Exploit Public-Facing Application		T1190	Exploit Public-Facing Application	
T1110	+ 4	Brute Force: Password Guessing/ Password		T1219	Remote Access Software	
T1211	new	Exploitation for Defense Evasion		T1021	Remote Services	
T1071.001	new	Application Layer Protocol: Web Protocols		T1562.001	Impair Defenses: Disable or Modify Tools	
T1562.001	- 1	Impair Defenses: Disable or Modify Security Tools		T1071	Application Layer Protocol	
T1219	- 4	Remote Access Software		T1110.001	Brute Force: Password Guessing	
T1090.003	+ 2	Proxy: Multi-hop Proxy		T1133	External Remote Services	
T1046		Network Service Discovery		T1046	Network Service Discovery	
T1133	- 2	External Remote Services		T1090.003	Proxy: Multi-hop Proxy	

1. T1204 — User Execution

К этой технике относятся инциденты, связанные с заражением узлов вредоносным ПО, а также случаи обнаружения индикаторов компрометации в защищаемом периметре, например, по хэш-сумме вредоносного элемента или другим паттернам. Основная часть инцидентов по-прежнему связана с неосторожными действиями пользователей (посещение сомнительных сайтов, установка недоверенных расширений), что обычно приводит к заражению AdWare, которое устраняется автоматически или ручной очисткой.

2. T1190 — Exploit Public-Facing Application

Вторая по распространенности техника — эксплуатация публично доступных веб-приложений. Мы относим к ней как успешные попытки атак, так и неуспешные/заблокированные или же несработавшие попытки использования эксплоитов, что также может представлять интерес для расследования. Чаще всего в наших расследованиях за этот год фигурировали Microsoft Exchange и популярная в российском сегменте CMS «1С-Битрикс». В последних кейсах мы сталкивались с эксплуатацией уязвимостей в Zimbra, Roundcube, Remedy, TrueConf.

3. T1110 — Brute Force: Password Guessing/ Password Spraying

Методы перебора паролей и других учетных данных. В этом году мы отмечаем существенный рост инцидентов типа Password Spraying — когда один пароль «распыляется» на множество учетных записей и таким образом осуществляется перебор. Злоумышленники чаще стали использовать данную технику в уже скомпрометированной инфраструктуре для первоначального доступа, повышения привилегий, горизонтального распространения и развития атаки.

4. T1211 — Exploitation for Defense Evasion

К данной технике относятся атаки, направленные на эксплуатацию уязвимостей для обхода средств защиты. В этом году мы фиксируем значительный прирост таких случаев: атакующие чаще применяют методы, позволяющие действовать быстрее и уклоняться от обнаружения.

5. T1071.001 — Application Layer Protocol: Web Protocols

Категория вредоносной сетевой активности, которая включает в себя атаки с применением веб-протоколов прикладного уровня, чаще — для взаимодействия с командными серверами (C2). В то время как в прошлом году нельзя было выделить один преобладающий протокол, в этом году злоумышленники перешли в основном на HTTP/HTTPS.

6. T1562.001 — Impair Defenses, Disable or Modify Tools

В рамках данной техники мы фиксируем инциденты с модификацией/отключением средств защиты: антивирусных агентов, агентов EDR, DLP и прочих СЗИ. Злоумышленники заинтересованы в том, чтобы как можно дольше оставаться необнаруженными, поэтому эта техника остается популярной.

7. T1219 — Remote Access Software

Техника заключается в установке в инфраструктуре жертвы средств удаленного управления для закрепления, наиболее яркими и распространенными примерами таких программ являются AnyDesk, Team Viewer, Ammy Admin, Radmin, TightVNC и другие. Как и прежде, данные инциденты зачастую связаны с нарушением политик безопасности, когда пользователи устанавливают себе подобные программы для удаленного администрирования корпоративных ресурсов.

8. T1090.003 — Proxy: Multi-hop Proxy

Включает инциденты, связанные с использованием прокси со множественными прыжками (например, сети Tor и i2p). Злоумышленники продолжают использовать Tor и другие многоуровневые анонимные прокси для скрытия истинного источника атак или организации обратной связи (backdoor) со скомпрометированными активами.

9. T1046 — Network Service Discovery

Данная категория содержит инциденты внешнего и внутреннего сканирования, а также другие приемы внешней разведки. В большинстве случаев по результатам анализа данных инцидентов мы выходим на различные краулеры сервисов поиска общедоступных устройств в интернете (например, таких как Shodan). Поэтому в логику правил выявления инцидентов данной категории интегрированы данные систем Threat Intelligence и фиды угроз, которые добавляют контекст к событиям и позволяют реагировать только на потенциально серьезные попытки атак.

10. T1133 — External Remote Services

К данной технике относятся инциденты, связанные с атаками на внешние сервисы, такие как VPN, VNC и другие. Зачастую после таких атак злоумышленники также могли получить доступ к внутренней инфраструктуре. Для полноценного использования данной техники злоумышленникам необходимо каким-то образом обзавестись легитимными учетными данными — украсть, перехватить или сбрутить. Последнее зачастую происходит в результате недостаточного контроля за «теневой» инфраструктурой.

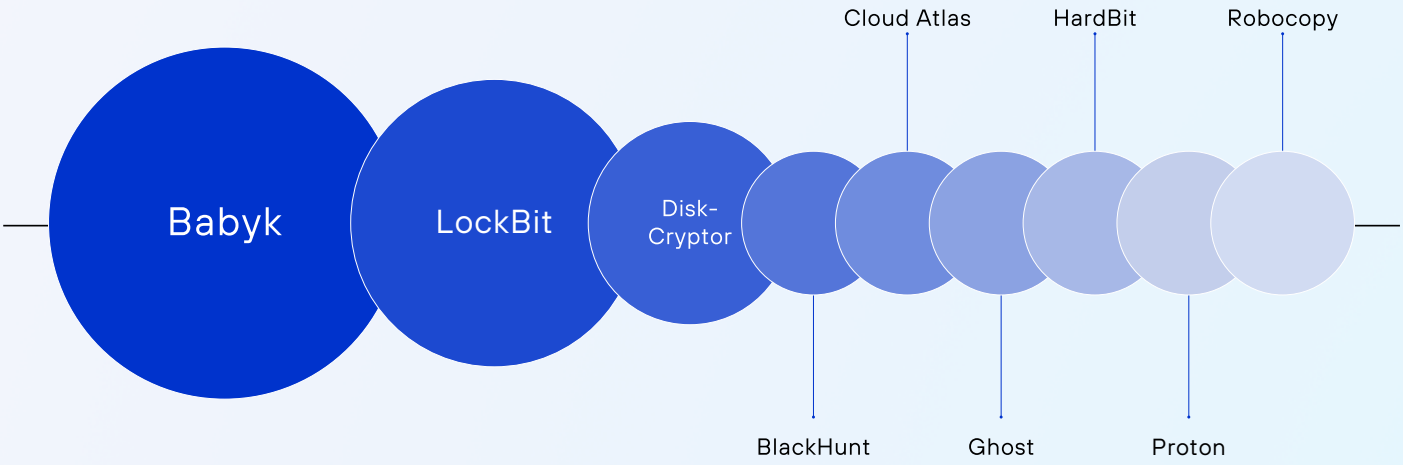
Киберкриминалистика

В 2025 году команда Jet CSIRT расследовала громкие инциденты в сферах ритейла, ИТ, транспорта и грузоперевозок, здравоохранения и страхования. С конца августа–начала сентября наша команда все чаще сталкивается с запросами на проведение глубокого киберкриминалистического расследования. Данные расследования отличаются необходимостью проведения анализа непосредственно пораженных активов (серверов, образов виртуальных машин, АРМ и прочего), что требует больше времени и подключения ресурсов более опытных аналитиков.

В ТОП киберугроз, ставших причиной нарушения доступности бизнес-сервисов, вошли вирусы-шифровальщики (44%) и вайперы (32%), которые полностью уничтожают инфраструктуру.

ТОП киберугроз 2025 года по результатам расследований команды Jet CSIRT

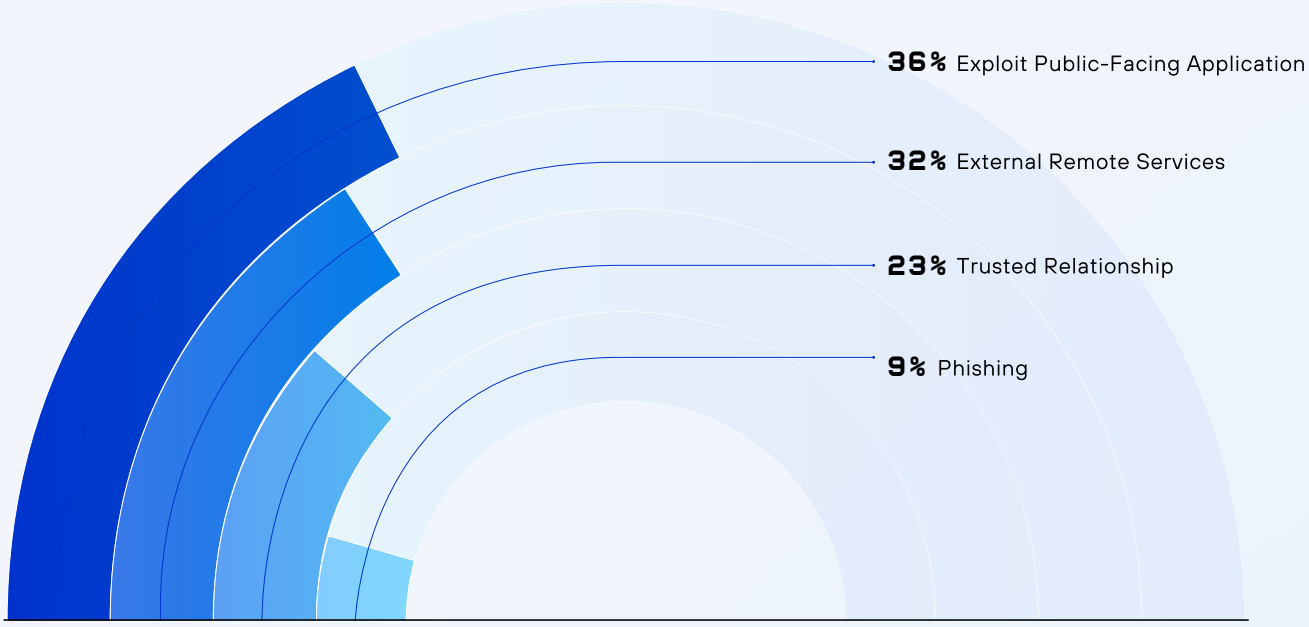
Чаще всего мы наблюдали следующие семейства шифровальщиков:



Наиболее типичные примеры вредоносных программ-шифровальщиков в рамках расследований

Как правило, основной причиной компрометации с последующим заражением стали уязвимости в общедоступных веб-приложениях, а также эксплуатация недостатков во внешних сервисах удаленного администрирования (RDP, VNC, SSH и другие). Рейтинг замыкают атаки на подрядчиков и фишинг, который уже много лет является надежным инструментом для получения первоначального доступа.

ТОП техник, чаще всего используемых для компрометации инфраструктур[5]



Получив доступ в инфраструктуру, злоумышленники стараются вести себя как можно тише. Наблюдается отход от использования шумных вредоносных программ в сторону полной мимикрии под легитимную активность. Атакующие активно совершенствуются в использовании техник LOTL: встроенные в ОС утилиты (powershell, bitsadmin или wmic) широко используются для мимикрии под легитимную активность. Такая активность сливается с фоном других легитимных действий системных администраторов и пользователей, что позволяет злоумышленникам достигать своих целей и избегать обнаружения.

Руслан Амиров,

руководитель экспертных сервисов мониторинга и реагирования Jet CSIRT

В 2025 году мы чаще фиксируем инциденты с атакой на подрядные организации. Взлом одного небольшого ИТ-сервисного провайдера де-факто предоставлял злоумышленникам «ключи от всех дверей» к его клиентам. Через доверенные каналы связи и доступы подрядчика атака беспрепятственно распространялась на другие компании, где в конечном итоге и происходило шифрование данных. При этом сам «нулевой пациент» зашифрован не был и получал только косвенный ущерб от разрыва отношений с клиентами.

[5] По результатам расследования инцидентов командой Jet CSIRT

КЕЙС

Заход через подрядчика

Крупный промышленный холдинг в сфере переработки пришел к нам, когда инфраструктура уже была зашифрована. Мы провели оперативное расследование инцидента и помогли в восстановлении инфраструктуры.

Вектором проникновения злоумышленников стала компрометация подрядной организации. В ходе анализа подключений к терминальному серверу мы поняли, что с использованием учетной записи подрядчика, оказывающего услуги в сфере ИТ, было установлено нелегитимное подключение с зарубежных IP-адресов. Получив доступ, злоумышленники скомпрометировали УЗ администратора посредством проведения атаки типа PetitPotam, после чего закрепились в инфраструктуре и регулярно продолжали подключаться с зарубежных адресов. С помощью учетной записи администратора злоумышленники завладели сервером управления AVZ Kaspersky и распространили на хостах организации задачу на запуск вредоносного ПО (шифровальщик LockBit 3.0).

Ущерб — неделя простоя для реанимации организации, восстановление ключевых бизнес-систем и долгий процесс восстановления и перестройки инфраструктуры под руководством наших специалистов.

КЕЙС

Дважды повезло

ИТ-организация обратилась к нам во время активного инцидента: с сервера, где было установлено ПО для автоматизации ИТ-процессов, под непривилегированной учетной записью были попытки извлечь учетные данные с других серверов. Быстрое реагирование (изоляция хостов, блокировка учетной записи) и расследование позволили обнаружить скрипты, управляющие серверы и самое главное — еще два скомпрометированных сервера. Анализ показал, что атака велась через эксплуатацию уязвимости в компоненте отчетности. Запросы шли в том числе с адреса другой, предположительно уже скомпрометированной организации.

Выяснилось, что злоумышленники дважды использовали двухлетнюю уязвимость: сначала скомпрометировали внешний хост, а через него — внутренний. Также произошла утечка учетных данных пользователей, связанных с этим ПО. Однако тот факт, что атака перекинулась на другие серверы, указывал, что привилегий для развития атаки у злоумышленников всё ещё было недостаточно. Наши действия позволили эффективно остановить атаку до нанесения существенного ущерба.

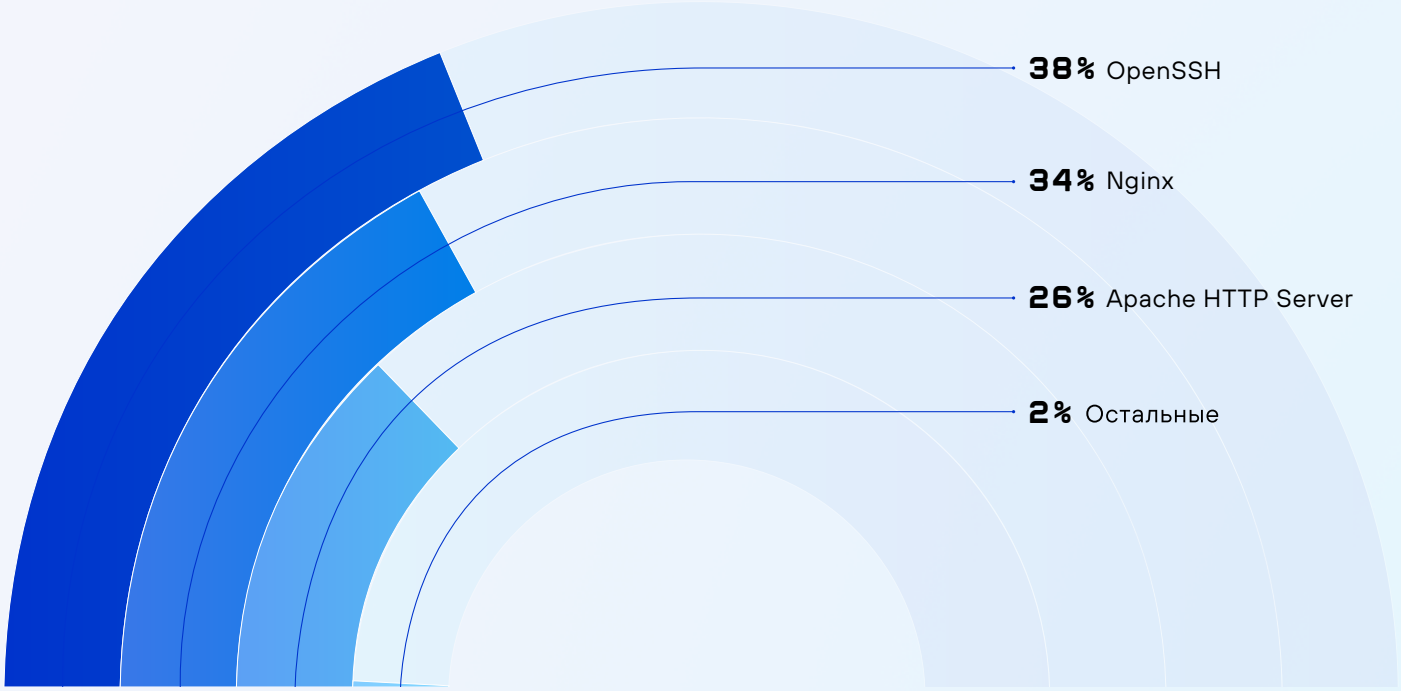
ПОДГОТОВКА И ПРОГНОЗИРОВАНИЕ

Управление поверхностью атак

Управление внешней поверхностью атак помогает компании увидеть свои слабые места глазами злоумышленника и устранить их до атаки.

В 2025 году **основным вектором атак остаются базовые уязвимости на внешнем периметре.** 65% всех инцидентов связаны с проблемами в трех ключевых компонентах инфраструктуры: OpenSSH, Nginx и Apache HTTP Server. Это напрямую вызвано использованием критически устаревших версий данного ПО, таких как OpenSSH 7.4 (2016 г.), Apache 2.2.3 (2005 г.) и PHP 5.6.36 (2018 г.), что формирует устойчивую и легко эксплуатируемую поверхность атаки даже в периметре крупных организаций.

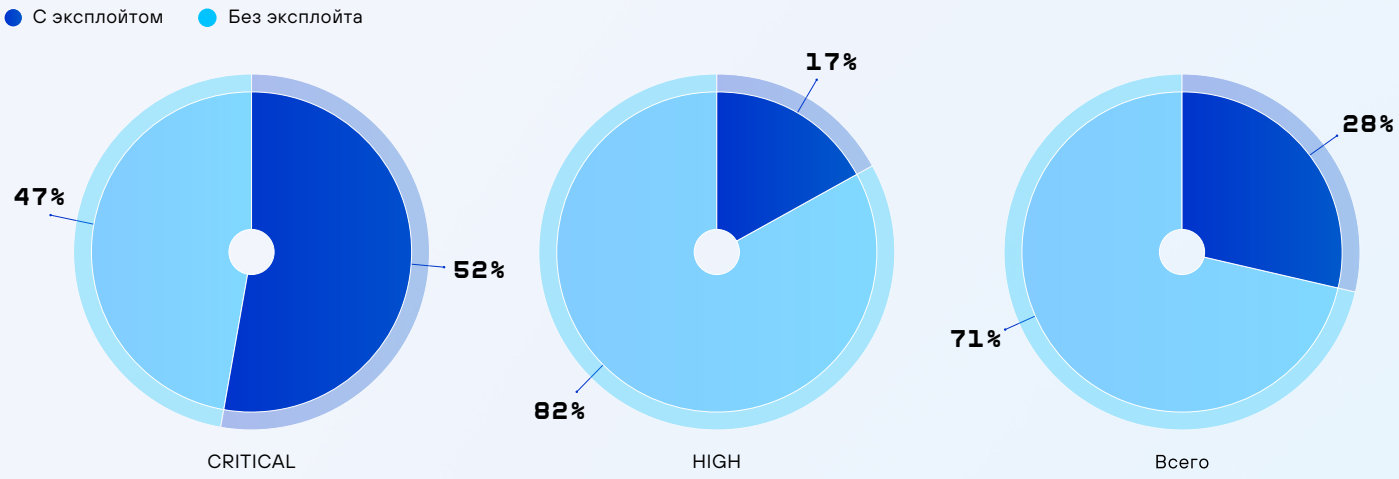
ТОП-3 уязвимых сервисов на внешнем периметре (доля от общего числа уязвимостей)



Каждая вторая (53%) критическая уязвимость просканированных нами компаний уже имеет публичный эксплойт и может быть использована для немедленной атаки. В среднем по всем уязвимостям этот показатель составляет 29%. Особое внимание требуют следующие уязвимости:

- CVE-2024-6387 (OpenSSH RCE) — CRITICAL, эксплойт доступен. Обнаружена у 75% исследуемых компаний. Затрагивает все версии OpenSSH <9.8, включая актуальные на начало 2025 года.
- CVE-2023-44487 (HTTP/2 Rapid Reset) — HIGH, эксплоит доступен. Встречается у 75% исследуемых компаний. Активное использование этой уязвимости коррелирует с пиком DDoS-активности в январе 2025 года (79 тысяч атакованных хостов).

Доля уязвимостей с публичным эксплойтом по уровню критичности



Вот что мы выяснили в рамках работ по сканированию внешнего периметра.

- В 83% компаний выявлены доступные из внешней сети административные интерфейсы. Из них **19% использовали учетные данные по умолчанию**. Вместе это даёт мгновенный и полный доступ к внутренней инфраструктуре без взлома.
- У 21% компаний были обнаружены API Key, хранящиеся в открытом виде, что повышает риск эксплуатации внешних интеграций.
- В 28% компаний выявлены Auth-token, размещенные в открытом виде, что потенциально предоставляет злоумышленнику полноценный доступ к соответствующим системам.
- В 80% компаний-пользователей системы «1С Предприятие» на внешнем контуре обнаруживались уязвимости, связанные с небезопасным дизайном публикации системы, при котором выпадающие списки пользователей отображали логины с ФИО (фамилия, имя, отчество). Это упрощает такие атаки как фишинг (легко угадать цель по имени), брутфорс (ограниченный словарь имен) и социальная инженерия, повышая вероятность несанкционированного доступа к данным.

Большинство организаций сталкиваются с типовыми и повторяющимися проблемами внешнего периметра: отсутствие ограничения доступа к административным интерфейсам и мультифакторной аутентификации, использование дефолтных учетных данных, хранение ключей и токенов в открытом виде, а также использование устаревшего уязвимого ПО.

КЕЙС

Мониторинг открытых кодовых платформ, используемых злоумышленниками для подготовки к sophisticated-атакам

При мониторинге github была обнаружена подготовка к атаке с помощью поддельного сайта государственной организации. В репозитории хранились файлы: HTML-код для фишингового сайта, PDF-файлы документов для создания легенды наполненности сайта. APK-файлы: Ros********or.apk и Rus*******fety.apk, которые злоумышленники замаскировали на сайте под приложение «Рус******* ***** безопасности» и Антивирус государственной организации.

При проведении анализа APK-файлов мы выявили встроенные вредоносные программы, которые получают несанкционированный доступ к компьютерным системам и размещенным в них данным или содержат нагрузку, намеренно причиняющую вред компьютерной системе. Благодаря раннему обнаружению на этапе подготовки атаки удалось предотвратить ее реализацию.

КЕЙС

Анонимный доступ к GraphQL API в GitLab EE

В ходе тестирования on-premise-инсталляции GitLab Enterprise Edition мы выявили критически важную уязвимость: GraphQL API был доступен анонимно, то есть без какой-либо аутентификации. Это позволило внешнему субъекту:

- получить полную схему GraphQL API (более 60 чувствительных полей, включая, например, auditEventsInstanceAmazonS3Configurations и aiChatContextPresets);
- получить доступ к публичным сниппетам, содержащим конфиденциальные фрагменты конфигураций: Nginx, SSH, ESLint, а также логи мобильного приложения;
- собрать данные о технологическом стеке приложения;
- потенциально реализовать DoS-атаку через техники вроде Alias/Field Overloading, эксплуатируя отсутствие лимитов и защиты на уровне API.

После оперативного уведомления компания:

- немедленно ограничила публикацию публичных сниппетов, переведя все существующие в статус Internal;
- внесла в конфигурацию GitLab корректное значение: (graphql_authentication_required = true), полностью закрыв доступ к GraphQL API для неавторизованных пользователей;
- дополнительно настроила защиту на уровне Nginx, добавив ограничения, предотвращающие эксплуатацию GraphQL в целях DoS.

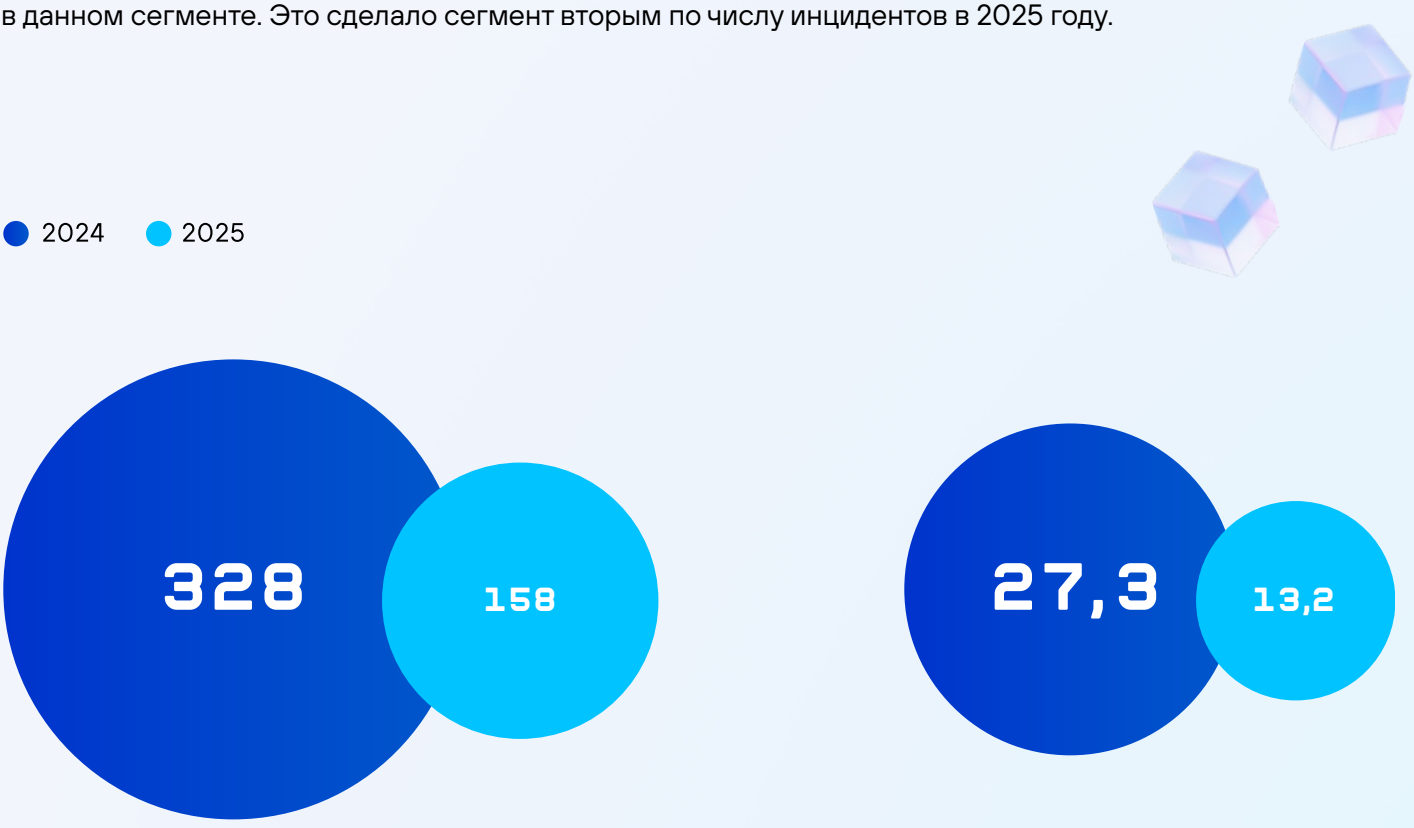
Киберразведка

Мониторинг публикаций «слитых» данных и паролей в открытых источниках и даркнете, анализ фишинговых сайтов и инфраструктуры злоумышленников помогают перейти от реактивной защиты к проактивной, упреждая действия злоумышленников.

За наблюдаемый период 2025 года мы зафиксировали **снижение количества публикаций скомпрометированных данных более чем в два раза по сравнению с 2024 годом.** Основное сокращение произошло в следующих отраслях: финансовый сектор, медицина, государственные организации.

Сектор электронной коммерции сохранил доминирующее положение и даже незначительно увеличил относительную долю, оставаясь главным источником компрометации клиентских данных (доля выросла с 35,7% до 37,3% при снижении абсолютного количества инцидентов на 49,6%).

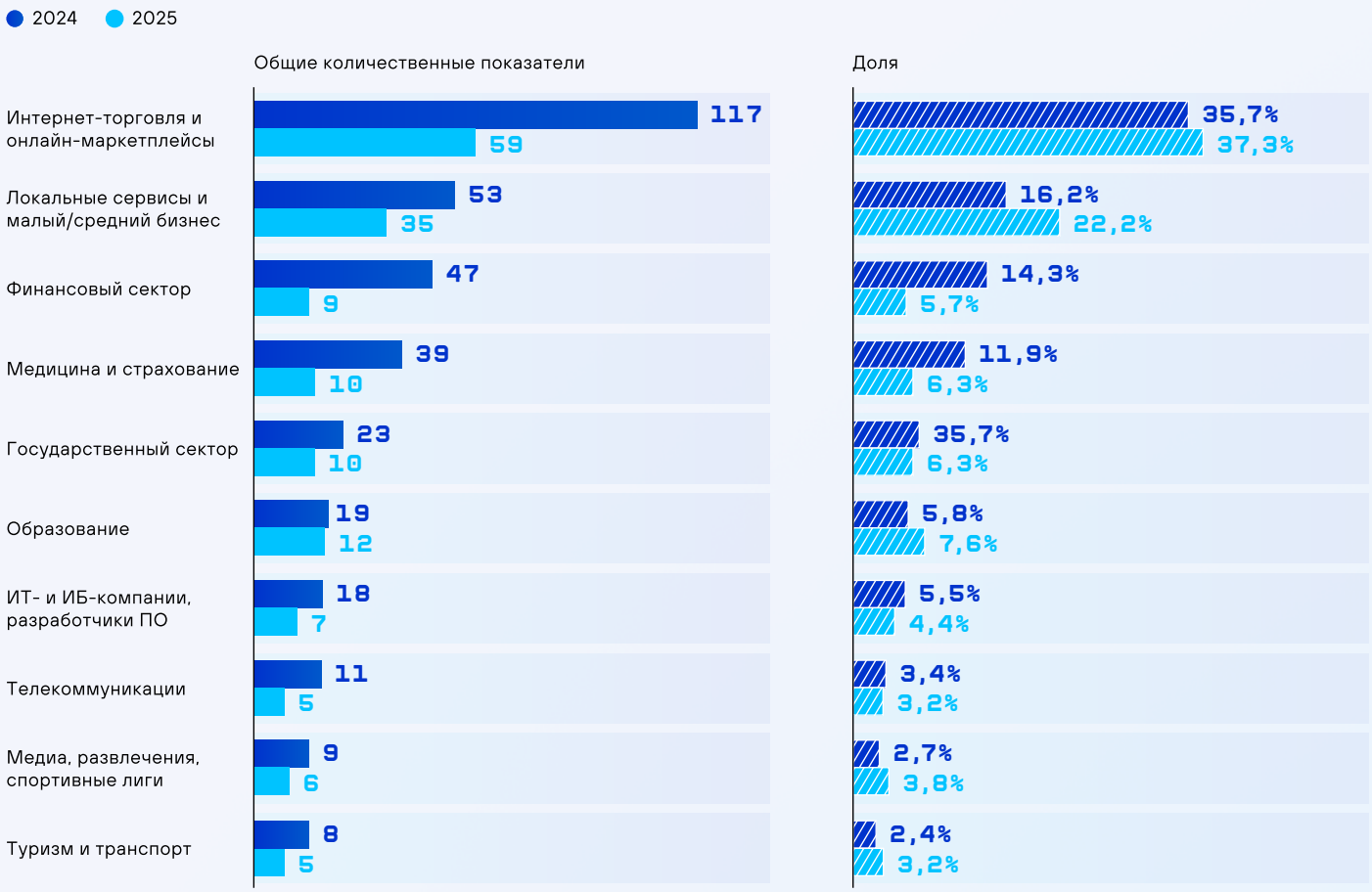
Мы отмечаем относительный рост доли локальных сервисов и малого/среднего бизнеса (с 16,2% до 22,2%) с сохраняющейся низкой зрелостью процессов защиты информации в данном сегменте. Это сделало сегмент вторым по числу инцидентов в 2025 году.



Количество уникальных инцидентов

Среднемесячное количество новых уникальных инцидентов

Главные источники компрометации клиентских данных за 2024–2025 годы



Наиболее частыми причинами компрометации данных в 2025 году стали:

- уязвимости веб-приложений и CMS, особенно в интернет-торговле и онлайн-сервисах;
- ошибки конфигурации облачных хранилищ (открытые базы, неверные права доступа);
- избыточные или некорректно настроенные права доступа в бизнес-приложениях;
- компрометация подрядчиков и сторонних сервисов, имеющих доступ к данным.

В ходе мониторинга фишинговой активности за 2025 год нам удалось выявить ключевые тенденции, отражающие развитие методов злоумышленников и организацию их инфраструктуры.

- У 40% фишинговых доменов, проиндексированных в 2025 году, обнаружена MX-запись, что говорит о наличии настроенной почтовой инфраструктуры. Такие домены могут использоваться не только для размещения поддельных веб-страниц, но и для рассылки фишинговых писем — в том числе писем, стилизованных под корпоративные уведомления и сообщения от имени компаний.

- Большинство (60%) доменных имен, относящихся к категории тайпсквоттинга, регистрируются у абузоустойчивых регуляторов, что заметно усложняет процесс пресечения активности. Для скрытия инфраструктуры злоумышленники активно используют:
  - маскирование реального IP-адреса через Cloudflare и аналогичные сервисы;
  - геоблокировки (ограничение доступа для отдельных стран или регионов);
  - фильтрацию по User-Agent;
  - динамическое поведение домена и периодическую смену контента (fast-flux).

  Эти меры значительно повышают устойчивость фишинговых ресурсов к обнаружению и блокировкам, а также требуют более глубокого анализа при расследовании. Остальные 40% доменов размещены в национальных доменных зонах .ru, .su и .рф.

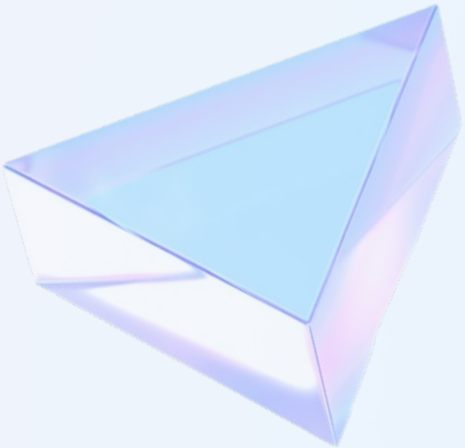
- Вырос объем регистрации доменных имен, схожих с официальным названием компаний, на которых располагаются магазины с продажей нелегальной продукции. Указанные домены находятся на абузоустойчивых регуляторах, которые не попадают в юрисдикцию РФ. Исходя из этого присутствует проблема по полной блокировке. Как правило, истинные DNS-записи скрыты Cloudflare, а регистраторами являются Namecheap, Namesilo.

КЕЙС

Теневой двойник

В ходе мониторинга сети Интернет был выявлен вредоносный интернет-ресурс, который незаконно использовал в своем доменном имени название компании и ее зарегистрированный товарный знак. Сайт предназначался для реализации запрещенных препаратов.

Действия злоумышленников представляли прямую угрозу репутации компании, поскольку у посетителей ресурса могло сложиться ложное впечатление о причастности организации к незаконной деятельности, что потенциально вело к утрате доверия со стороны клиентов и партнеров.



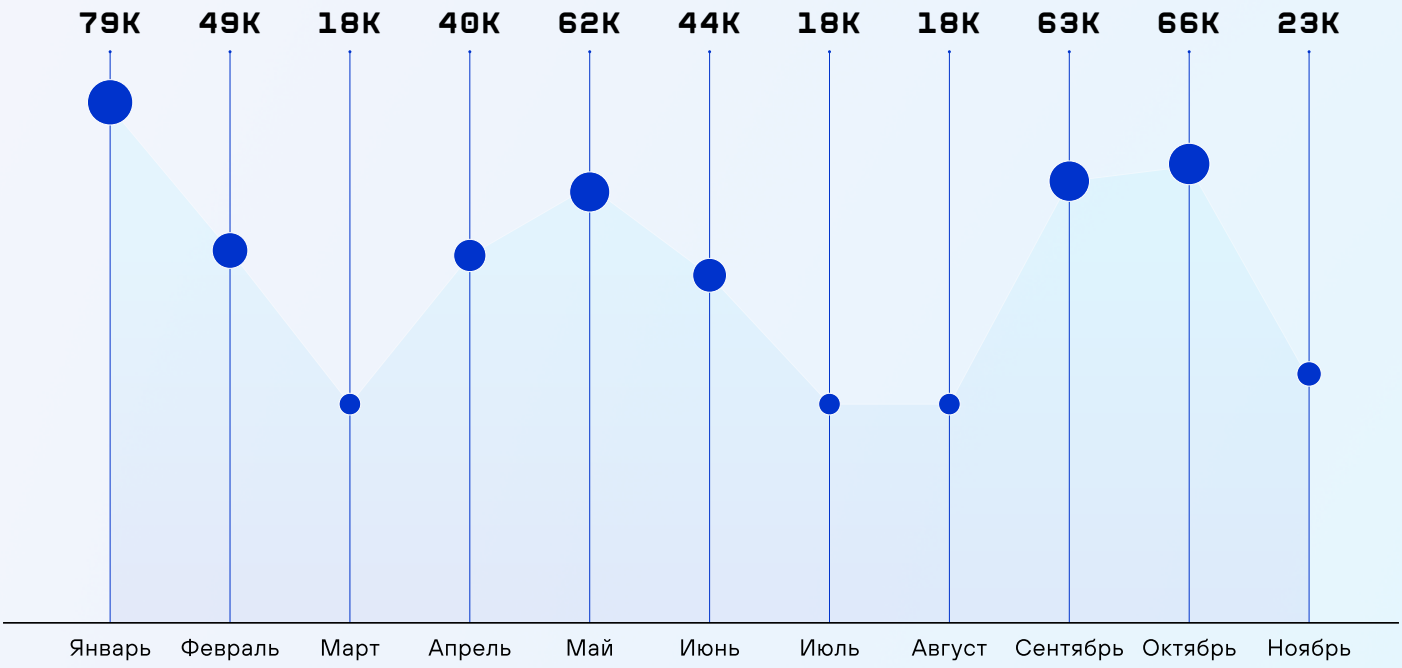
ЗАЩИТА, ЗАМЕДЛЕНИЕ, СДЕРЖИВАНИЕ

В 2025 году продолжается высокая активность DDoS-атак:

- в среднем ежедневно атакуется около 1 466 хостов, а в пиковые дни — до 8 532 хостов за сутки;
- общее число уникальных атакованных хостов за год превысило 483,9 тысячи;
- самая продолжительная атака длилась 10 дней, что указывает на растущую сложность и настойчивость злоумышленников.

Наиболее атакуемыми секторами остаются промышленность, телекоммуникации и банковская сфера — отрасли, критически зависимые от стабильности цифровой инфраструктуры. Атаки на них не только наносят прямой ущерб, но и могут вызывать масштабные каскадные сбои.

Пик напряженности по количеству DDoS-атак имеет сезонный характер: максимумы приходятся на январь (79 тыс.), май (62 тыс.), сентябрь (63 тыс.) и октябрь (66 тыс.), тогда как в марте, июле и августе наблюдается спад (по 18 тыс.). Возможные причины — киберпреступные кампании, приуроченные к финансовым отчетам, праздникам или началу/окончанию отчетных периодов, а также более низкая активность в летние месяцы.



Статистика DDoS-атак за 2025 год по данным исследуемых нами источников

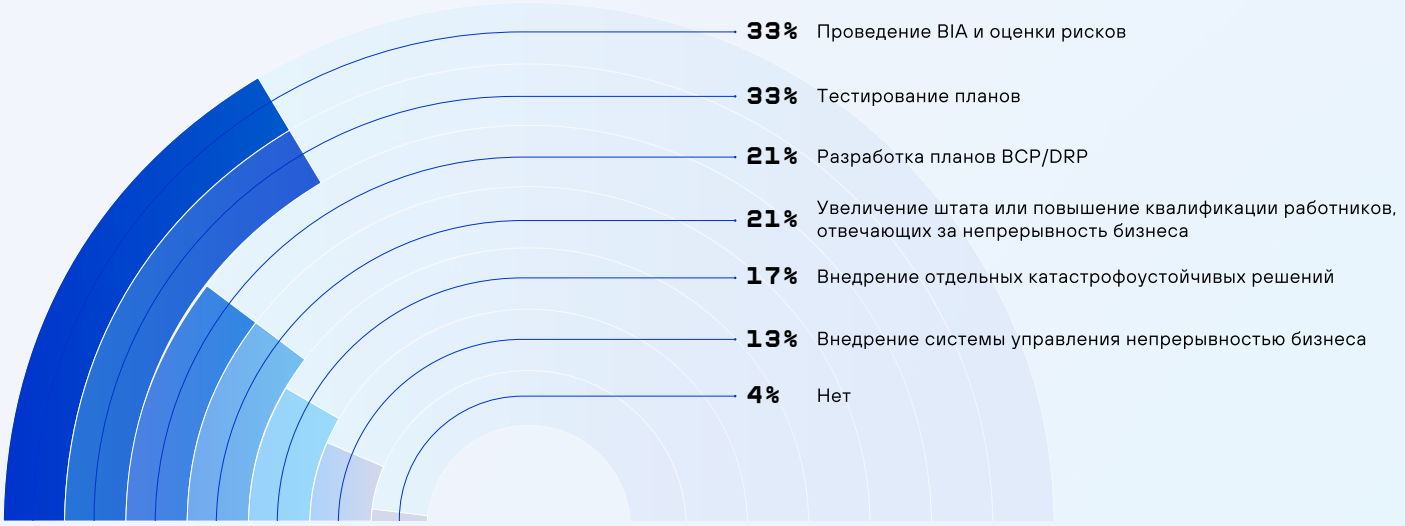
ВОССТАНОВЛЕНИЕ

Планирование и поддержка кризисных процессов, управление жизнестойкостью

Значительный рост кибератак с использованием шифровальщиков и вайперов в 2025 году напрямую подрывает устойчивость бизнеса. Длительные простои в результате таких инцидентов заставляют компании возвращаться к стандартам обеспечения непрерывности бизнеса и применять практики, используемые раньше исключительно при различных катастрофах «на земле», к кризисам в цифровой реальности.

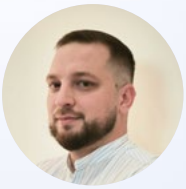
В 2025 году компании продолжили наращивать финансирование систем непрерывности бизнеса и отработки действий при сбоях. К таким практикам в первую очередь можно отнести тестирование планов реагирования и восстановления, а также проведение анализа воздействия на бизнес (BIA).

Планы по развитию системы управления непрерывностью бизнеса на ближайшие 2–3 года*



Мы фиксируем более чем двукратное увеличение спроса на услуги по тестированию кризисного реагирования на кибератаки и разработке на основе результатов такого тестирования планов реагирования. Внедрение процесса кризис-менеджмента позволяет компаниям уменьшить возможный простой от масштабного инцидента ИБ. Распространенным и наиболее эффективным видом такого тестирования остается настольное тестирование или table-top, позволяющее без больших вложений оценить готовность компании к катастрофе, а также отработать реагирование на инцидент, включая коммуникации и принятие решений топ-менеджментом.

* Респонденты могли выбрать несколько вариантов ответа



Аскар Мусаев,

эксперт по непрерывности бизнеса

На каждом настольном тестировании с участием ТОП-менеджмента мы видим, как быстро все вовлекаются в обсуждение реагирования и восстановления на инцидент. Участие в table-top представителей HR, PR, бизнеса позволяет командам из ИТ и ИБ по-другому взглянуть на знакомый процесс, отработать взаимодействие с коллегами и подсветить руководству насущные проблемы. Иногда прямо во время тестирования принимаются решения о запуске какого-либо проекта, направленного на повышение устойчивости, например, пентест контура резервного копирования, разработка плана кризисной коммуникации.

Параллельно с этим компании озадачились формализацией процесса резервного копирования — разработкой детальных регламентов по частоте создания резервных копий для разных классов систем и обновлению результатов BIA. 2025 год еще раз подчеркнул проблему расхождения ожиданий по восстановлению ИТ-инфраструктуры между ее владельцами и пользователями. 21% компаний не выделяют классы критичности ИТ-систем, что увеличивает риски ошибок при определении порядка восстановления, но при этом компании начали более осознанно подходить к классификации BIA, что позволяет подкрепить принятую внутри ИТ классификацию ущербами от простоя.

КЕЙС

Классификация критичности web-приложений

Методология анализа воздействия на бизнес (BIA) была применена для решения конкретной задачи ИБ-подразделения — приоритизации защиты веб-приложений. Оценивая важность каждого приложения для бизнеса и возможные последствия его взлома, компания смогла распределить их по уровням критичности. Это, в свою очередь, позволило перейти от универсальных мер к точечному и обоснованному планированию усилий по защите.

Резервное копирование в архитектуре киберустойчивости

Резервное копирование является ключевым фактором устойчивости, позволяя компании гарантировать клиентам и партнерам выполнение обязательств даже в условиях кризиса.

Доля компаний, которые остаются в зоне риска, поскольку не обладают полноценной СРК или резервируют не все данные, снижается: в 2025 году их число составило всего 19%. При этом только 25% компаний действительно обеспечивают высокий уровень доступности и соблюдают стратегию «3-2-1».

Доля компаний, в которых есть СРК

Доля компаний, использующих стратегию «3-2-1»

Под влиянием эпидемии шифровальщиков подходы к резервному копированию претерпели значительные изменения: из технической функции они превратилась в элемент управления киберрисками. Создание изолированных, защищенных от компрометации копий данных постепенно становится базовым элементом ИТ-архитектуры компании, а независимые аудиты систем резервного копирования — системной практикой для многих отраслей.

В рамках 2025 года в два раза выросло количество запросов на:

- проверку архитектуры СРК на соответствие лучшим отечественным и мировым практикам;
- оценку устойчивости компонентов СРК к действиям злоумышленников и вредоносного ПО;
- анализ вероятности потери резервных копий в результате целевых атак,
- аудит механизмов защиты данных, репозиториев и каналов передачи копий,
- оценку текущих мер по изоляции копий и резервных площадок.

Создание защищенных хранилищ становится стандартным требованием при внедрении или модернизации СРК. При этом наиболее распространенными практиками в 2025 году стали следующие:

- использование ленточных библиотек для размещения изолированных копий, с обязательным регламентом ротации носителей;
- физическое изъятие лент из библиотеки и хранение их в местах с ограниченным доступом;
- формализованная процедура обмена, транспортировки и учета носителей;
- применение уровневой хранения, где часть копий хранится в оперативных репозиториях, а критичные и долгосрочные — в более защищенных.

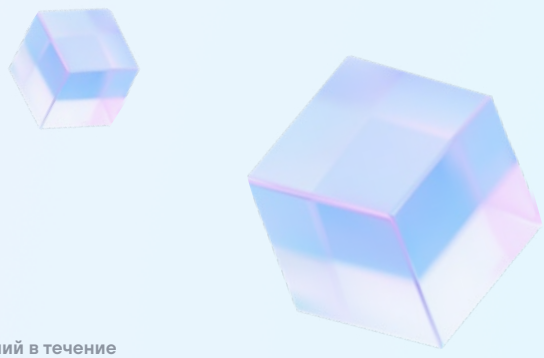
Игорь Шконда,

руководитель отдела систем хранения данных

Тренд 2025 и следующего года — слияние процессов резервного копирования и аварийного восстановления в единую, формализованную и регулярно тестируемую дисциплину. Бизнес больше не будет спрашивать «Есть ли у нас бэкапы?», а будет спрашивать «Сможем ли мы восстановить работу с учетом наших RTO и RPO после инцидента?». Ответ «Да» возможен только при наличии не просто данных резервных копий на полке, а работающего DR-плана, который был проверен на практике.

Тренд на защищенный бэкап способствовал увеличению спроса на объектные системы хранения (поддерживающие неизменяемость данных Object Lock[6]) — за 2025 год он вырос более чем в два раза.

Еще одной яркой тенденцией 2025 года стал переход крупных компаний к регулярным тестовым восстановлениям данных в изолированных контурах. Эта практика, которую уже внедрили 74% организаций, особенно активно развивается в банковском секторе, ритейле и других отраслях с повышенными требованиями к доступности информации.



[6] Позволяет блокировать возможность логического удаления или изменения сохраненных копий в течение заданного периода, независимо от внешних действий (администраторов или вредоносного ПО).

Распространенность практики регулярных тестовых восстановлений данных

74%

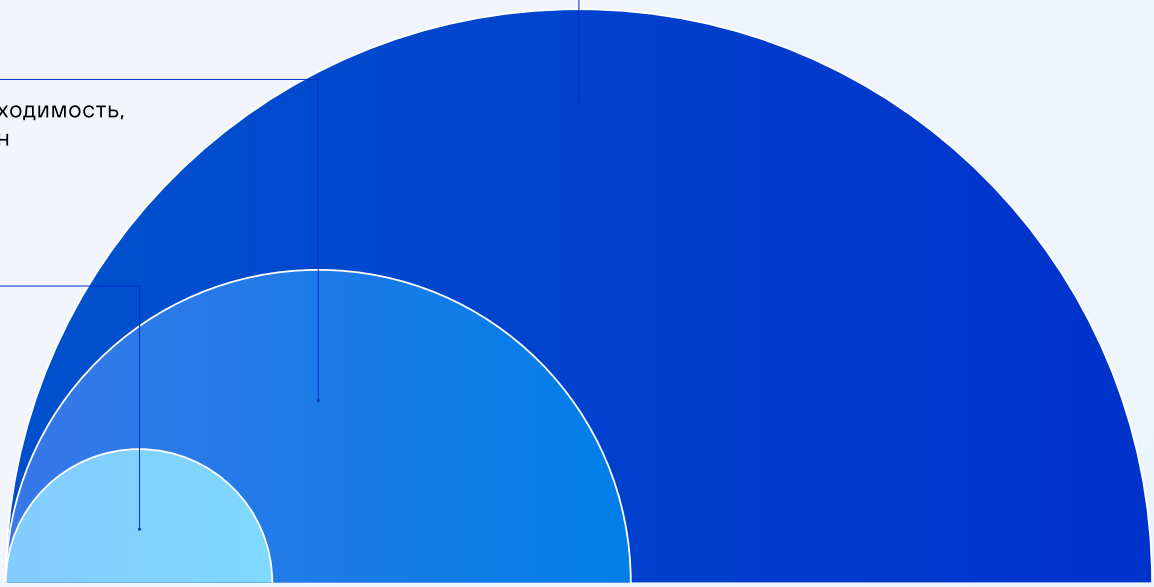
Да, периодически делаем тестовые восстановления

22%

Нет, понимаем необходимость, процесс не выстроен или нет ресурсов

4%

Нет



КЕЙС

Полная потеря данных из-за игнорирования базовых принципов резервного копирования

В результате успешной атаки компания столкнулась с полной потерей данных, включая первичные системы и все резервные копии. Причиной катастрофы стало фундаментальное пренебрежение базовыми принципами безопасности: резервные копии хранились в той же сети, что и основные системы, не были защищены от удаления и никогда не проверялись на возможность восстановления. Восстановить часть информационных систем удалось лишь из устаревших копий баз данных, которые по случайности сохранились в изолированной тестовой среде разработки, которую атака не задела.

Резервная копия, которую можно удалить тем же доступом, что и оригинал, — это не резервная копия. Надежда на везение и случайно уцелевший тестовый контур — это не стратегия.

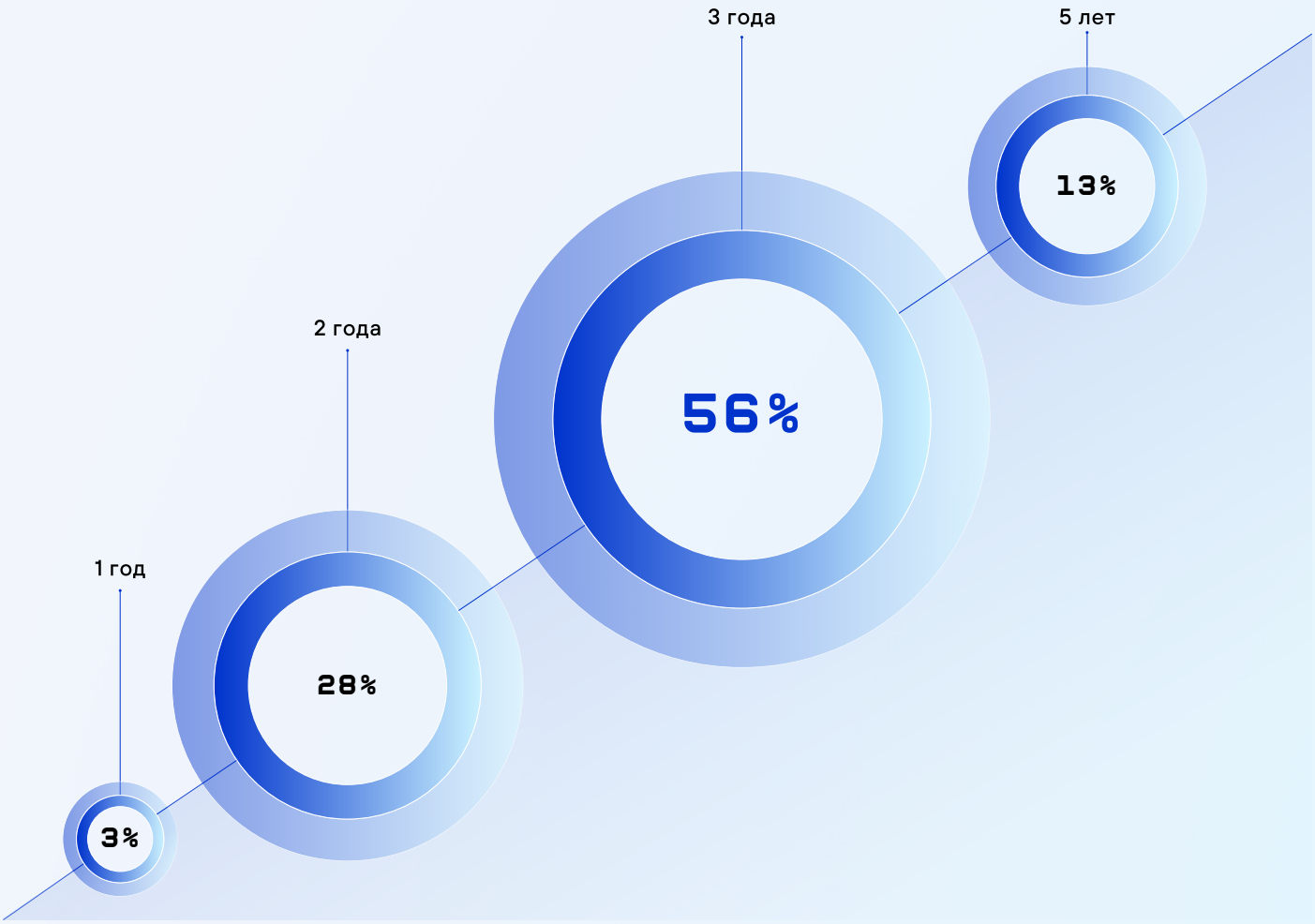
СИСТЕМНОЕ РАЗВИТИЕ И КОНТРОЛЬ

Стратегическое управление киберустойчивостью

2025 год продолжил эпоху нарастающей нестабильности в мире и РФ, требуя от руководителей служб ИБ не только технической экспертизы, но и лидерских качеств кризис-менеджера. Ключевым трендом становится «гибкая стратегия» — отказ от пяти-трехлетних горизонтов в пользу динамичных среднесрочных циклов (1–2 года), сохраняющих общее видение, но допускающих оперативную корректировку.

К 2024 практика пятилетнего планирования сократилась до 15%, а в 2025 году составила уже 13%, тогда как горизонт в 2 года выбрали уже 28% руководителей ИБ. Ускоряющаяся цифровизация, волатильность экономики и необходимость быстрого реагирования на угрозы делают классические долгосрочные стратегии менее релевантными.

Горизонт стратегического планирования в 2025 году



Александр Морковчин,

руководитель отдела развития консалтинга по информационной безопасности

Руководители ИБ продолжают выбирать «осторожный» метод стратегического планирования, отдавая предпочтение стратегии постепенного улучшения[7] (60% компаний). Использование инновационных стратегий продолжает снижаться и актуально для 4% компаний.

Продолжающаяся масштабная цифровизация делает бизнес не только эффективнее, но и уязвимее, поэтому в 2025 году мы наблюдали смещение фокуса многих CISO с превентивных мер в организацию непрерывности бизнес-процессов и ИТ-инфраструктуры и кризис-менеджмент.

Противодействие киберусталости и совершенствование готовности к реагированию на инциденты ИБ

Формирование и поддержание культуры кибербезопасности обеспечивает осознанное выполнение сотрудниками требований ИБ и снижает влияние человеческого фактора на состояние безопасности.

Мы наблюдаем устойчивую тенденцию к систематизации киберучений — их планируют заранее и проводят несколькими циклами в течение года. Растет реалистичность учений — упражнения разрабатываются с адаптацией под имеющуюся ИТ-инфраструктуру и средства защиты (моделирование атак под конкретные продукты, работа с ошибками конфигураций и т.д.) и отработкой реальных инцидентов (атаки шифровальщиков, компрометация инфраструктуры через почту, использование уязвимостей в корпоративных продуктах и т.д.).

В 2025 году наибольший интерес к киберучениям мы зафиксировали в финансовом секторе, государственных структурах и промышленных компаниях. Высокий уровень заинтересованности злоумышленников и растущее количество угроз, нацеленных на объекты критической информационной инфраструктуры, формируют осознанный спрос на практические инструменты подготовки к атакам.

[7] Согласно ГОСТ Р 54147-2010. Стратегический и инновационный менеджмент. Термины и определения:

- Инновационная стратегия строится вокруг новых, «прорывных» продуктов или решений. Новизна стратегии охватывает все основные составляющие: масштаб, облик и цели.
- Стратегия обновления является промежуточной между инновационной стратегией и стратегией постоянного совершенствования.
- Стратегия постепенного совершенствования предполагает постепенные небольшие изменения масштаба, облика и цели: выполнение в основном прежних операций, но в больших объемах и с незначительными изменениями используемых процессов

Как и в прошлом году, чаще всего учения проводятся в небольших группах — от 5 до 15 человек. Наиболее востребованной остается отработка навыков для специалистов 1 и 2 линий SOC и ИБ-специалистов широкого профиля, однако все чаще в обучении участвуют ключевые ИТ-специалисты, работающие с критичными сервисами, что связано с необходимостью синхронизировать реагирование на инциденты между двумя подразделениями. Происходит адаптация под более гибкие форматы — индивидуальное прохождение тренировки для минимального отрыва от рабочего времени без влияния на работу ИБ.

В 2025 году мы фиксируем устойчивый рост интереса к корпоративному обучению кибербезопасности рядовых сотрудников. Компании стремятся выстроить целостный подход: укрепляют компетенции ИБ и ИТ-команд и одновременно повышают цифровую грамотность сотрудников.

Обучение сотрудников перестаёт быть формальной «галочкой» — компании ищут форматы, которые действительно вовлекают людей и меняют их поведение. Растёт интерес к очным встречам, где живое общение и разбор кейсов дают больший результат, чем стандартные онлайн-курсы. Программы становятся масштабнее: организации стремятся обучить весь штат, не ограничиваясь отдельными группами риска. При этом чаще используются сегментация аудитории и подход с формированием практик ожидаемого безопасного поведения.

Кира Шиянова,

менеджер продукта Jet CyberCamp

Критически важными для киберучений и повышения осведомленности в 2025 году стали:

- реалистичные сценарии, моделирующие именно те угрозы, с которыми организация может столкнуться;
- индивидуальная гибкость программ, подстраивающихся под специфику компании и организацию рабочего времени сотрудников;
- целостный охват работников, от рядовых сотрудников до топ-менеджмента, который способствует формированию единой культуры кибербезопасности.

Так, 2025 год стал важным рубежом, обозначившим четкий отказ бизнеса от формальных подходов. Компании перестали рассматривать киберучения как абстрактную «галочку» и перешли к требованию реальных результатов.

Оценка и тестирование киберустойчивости

Систематическая и независимая проверка уровня киберустойчивости является ключевым элементом реальной готовности к кибератакам.

Как и в 2024 году, в 2025-м подчеркивается преемственность и развитие трендов, обозначившихся в сфере тестирования на проникновение ранее, а не их кардинальное изменение. Так, классические инфраструктурные пентесты постепенно уступают место проверке целевых сценариев. Компании научились формулировать более точные гипотезы, фокусируясь на проверке реализации катастрофических для бизнеса сценариев атак. Это позволяет точечно выстраивать защиту и минимизировать ключевые риски, оставаясь в рамках требований регуляторов, включая положения Указа Президента Российской Федерации от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Продолжает набирать обороты и тренд на комплексный анализ безопасности, который интегрирует разрозненные требования в единую картину. В скоуп таких проектов начали включать не только «классические» сегменты сети, но и расширенный круг информационных систем — как внешних, так и внутренних, включая критичные для функционирования бизнес-процессов и новые цифровые направления, например, безопасность инфраструктуры цифрового рубля.

Развитием прошлогодней тенденции стал растущий фокус на проверку безопасности цепочек поставок. Такие проекты все чаще нацелены либо на моделирование атаки от лица подрядчика, либо на прямую оценку защищенности партнеров, что является прямым ответом на учащающиеся инциденты в этой сфере.

В сфере уязвимостей сохраняются устойчивые тренды: во внутренней сети основные риски связаны с неактуальными обновлениями и несвоевременным патчингом, что позволяет злоумышленникам получать критичные права доступа. Кроме того, сохраняется проблема избыточных привилегий у пользователей и сервисных аккаунтов, отсутствие надлежащего контроля аутентификации и неисправности в настройках Active Directory и инфраструктуры сертификатов.

Алексей Куприянов,

руководитель группы практического анализа защищенности

Мы отмечаем рост интереса к Red-Team-проектам: компании проверяют не только инфраструктуру, но и физическую защиту, а также эффективность как своих, так и коммерческих SOC. Также отмечается увеличенный спрос на глубокий анализ внутренних и внешних приложений с расширением используемых ролей.

Частыми нарушениями в области раскрытия информации и веб-безопасности являются перечисление пользователей и внутренних IP-адресов. Также регулярно выявляются уязвимости в веб-приложениях, такие как XSS и SSRF, плюс использование устаревших версий серверного программного обеспечения (например, Apache). Кроме того, отмечается отсутствие надлежащей аутентификации в API-интерфейсах (Swagger, Redis) и IoT-устройствах, включая камеры Hikvision и принтеры Kyocera, что создает дополнительные точки входа для атак.

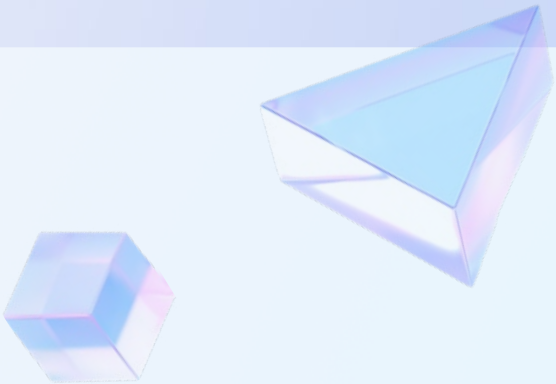
Если смотреть на статистику по успешно выполненным kill-chain нашей командой тестирования на проникновение, можно отметить топ-3 техник, которые оказали наибольшее влияние на достижение целей работ:

- извлечение NTDS.dit и выгрузка LSASS[8] были ключевыми шагами, обеспечившими полную компрометацию домена (62%);
- эксплуатация MS17-010[9], которая уже более 8 лет успешно используется для компрометации (20%);
- Relay-атаки (NTLM / LDAPS)[10] позволили повысить привилегии в домене (16%).

КЕЙС

От фишинга к внедрению вредоносного кода: угрозы слабой защиты процесса разработки и распространения ПО

В рамках проведения работ по формату Red-Team была скомпрометирована учетная запись пользователя через фишинговую атаку, что позволило злоумышленникам перехватить контроль над двухфакторной аутентификацией и получить доступ к корпоративной сети под легитимными учетными данными. В ходе дальнейшего анализа безопасности конвейера разработки и распространения ПО мы обнаружили неограниченный доступ к внутреннему хранилищу программных артефактов через учетную запись с избыточными правами. Это дало возможность внедрять модифицированные версии приложений с вредоносным кодом, создавая реальную угрозу распространения программных закладок и обхода систем защиты.



[8] Файл NTDS.dit содержит базу данных доменных учетных записей, а процесс LSASS отвечает за управление их сессиями и хранение временных копий паролей в памяти. Получение из них данных предоставляет возможность получить контроль над всеми учетными записями в домене, включая администраторов сети.

[9] MS17-010 — критическая уязвимость в Windows, позволяющая удаленно выполнить код без авторизации. В пентестах наличие этой уязвимости становится «точкой входа» для закрепления в сети жертвы

[10] Relay-атака — тип атаки, при котором перехватываются аутентификационные данные, использующие протокол NTLM / LDAPS, и далее перенаправляются на легитимный сервис для выполнения действий от имени жертвы без знания ее пароля. В результате пентестер может получить доступ к ресурсам, изменить настройки или повысить привилегии в домене

АДАПТАЦИЯ И ПЕРЕСТРОЙКА

Непрерывное улучшение и оценка эффективности ИБ

Ключевым инструментом оценки эффективности ИБ, позволяющим «держать руку на пульсе», в 2025 году остается применение измеряемых показателей — метрик, KPI, KRI и других.

Метрики позволяют превратить разрозненные сигналы о состоянии защиты в понятную картину и делают принятие решений более прозрачным. Доля компаний, у которых метрики ИБ отсутствуют, существенно сократилась в сравнении с 2024 годом — с 73% до 57%. Компании начинают активно внедрять количественные показатели, интегрируя их в регулярную отчётность и используя как инструмент для коммуникации с топ-менеджментом.

В большинстве организаций набор метрик все еще фрагментарный: как правило, используются единичные метрики, входящие в область интереса руководства компании (24%). При этом доля компаний, которые используют полноценный набор метрик для принятия решений о функционировании ИБ, все еще растет медленно (с 3% в 2024 году до 4% в 2025 году).

Ручной сбор метрик и их анализ ведет к быстрому устареванию собранных данных и расходованию большого количества ресурсов на их поддержку, ограничивая оперативность и глубину анализа. Однако доля компаний, которые автоматизировали сбор, обработку и визуализацию метрик, также выросла незначительно (с 2% в 2024 году до 3% в 2025 году).

Несмотря на растущую популярность использования метрик ИБ, большинство из них по-прежнему фокусируются на операционных и количественных показателях, а не на измеримом фактическом уровне киберустойчивости (например, времени атаки, времени реагирования и вероятности компрометации). Приоритет традиционно отдается закрытию тактических задач. В результате развитие эффективных показателей, напрямую коррелирующих со снижением бизнес-рисков, остается второстепенной задачей в условиях постоянной ресурсной нагрузки.

Наличие в компаниях метрик для отслеживания эффективности ИБ

ПРОГНОЗЫ НА 2026 ГОД

Жизнь в условиях постоянных кибератак — новая реальность. В 2026 году стратегической целью станет создание «антихрупкой» архитектуры бизнеса, способной к непрерывной адаптации, восстановлению и сохранению операционной жизнеспособности. Такие меры как защищенные, изолированные системы резервного копирования и аварийного восстановления, инструменты кризисного реагирования, платформы киберразведки и упреждающего обнаружения угроз, защита цепочек поставок станут фокусом российских компаний.

От абстрактных оценок рисков к защите на основе техник противника

Мы ожидаем, что в 2026 году концепция Threat Profiling — переход от абстрактных оценок рисков к моделированию поведения конкретных противников, ориентируясь на их точные тактики и техники (TTPs), — начнет активно использоваться российскими компаниям.

Конкретный вопрос — «Какие методы (TTPs) используют противники, которые целенаправленно охотятся на нас или наш сектор, и насколько мы к ним готовы?» — станет основой для прагматичной защиты. Ключевым инструментом этой трансформации будет практическое моделирование на основе фреймворка MITRE ATT&CK.

Перераспределение бюджетов на кризис-менеджмент и симуляцию атак / кризисов

Инциденты кибербезопасности в крупных компаниях заставляют задуматься — «Сможем ли мы сами восстановиться?» и «Как мы будем действовать в кризис?». Мы ожидаем увеличение интереса к проверке кризисного реагирования и вовлеченности ключевых лиц, принимающих решения в форматах настольного тестирования (tabletop exercise) и штабных киберучений, а также выстраиванию процессов кризисного реагирования.

Переход к threat-led-пентестингу

Мы прогнозируем развитие тренда по смещению фокуса тестирований на проникновение на цели, соотносящиеся с реальными угрозами, которые видит перед собой бизнес, а именно:

- возможность уничтожения резервных копий;
- вывод из строя ключевых бизнес-систем;
- демонстрация массовой утечки критичных для бизнеса данных;
- дефейс критичных бизнес-витрин и подобное.

Тренд на быстрый чек-ап киберустойчивости

Это ответ на бюджетные ограничения и геополитическую турбулентность. Проверка критичных областей — внешний периметр, готовность к фишингу, работоспособность резервных копий — нужна не для того, чтобы получить формальный отчет, а для того, чтобы получить краткий список конкретных приоритетных действий.

JET

SECURITY
TEAM

security@jet.su
jetcsirt.su