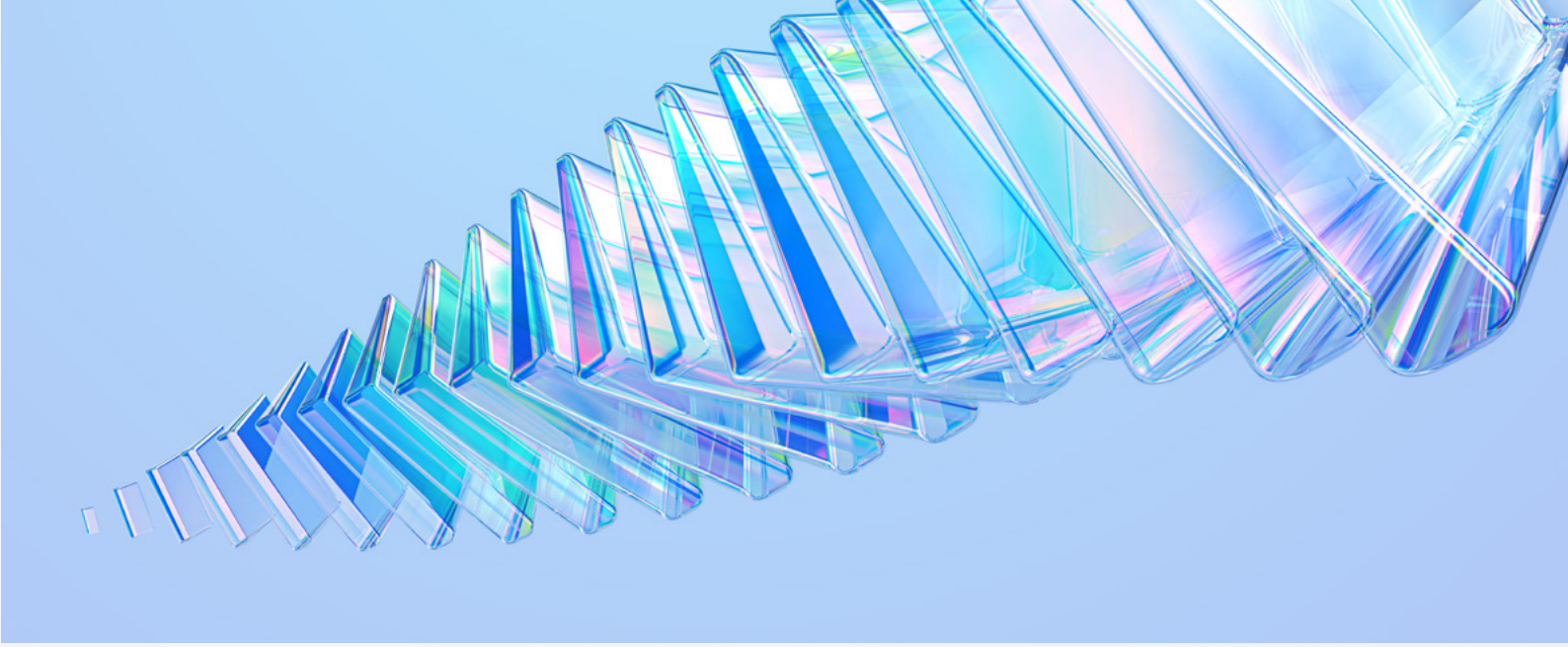
JET SECURITY TEAM

ИССЛЕДОВАНИЕ

АНАЛИЗ ЛАНДШАФТА УГРОЗ КИБЕРБЕЗОПАСНОСТИ 2024

Инфосистемы Джет
JET.SU



2024 ГОД: КРАТКИЕ ИТОГИ

- Пик напряженности по количеству инцидентов ИБ пришелся на середину весны — начало лета. Чаще всего **причиной взломов становились эксплуатация уязвимостей публичных веб-сервисов, сервисов удаленного доступа, атаки через поставщиков услуг, а также фишинг.**

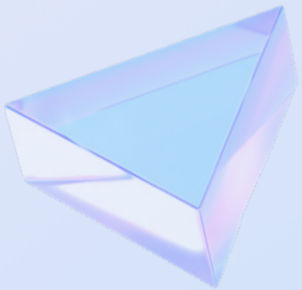
- **В 17%** расследованных нами инцидентов мы фиксировали **подозрение на компрометацию поставщиков услуг:** в основном атакующие использовали взломанные учетные записи компаний малого и среднего бизнеса, оказывающих сервис жертве. Около трети компаний-подрядчиков наших клиентов уже упоминаются на DarkNet-форумах и в Telegram-каналах хакерской или мошеннической тематики.

- **Финансовые организации, компании в сфере недвижимости, а также ИТ-компании вошли в топ-3 наиболее атакуемых отраслей** среди клиентов Jet CSIRT в 2024 году.

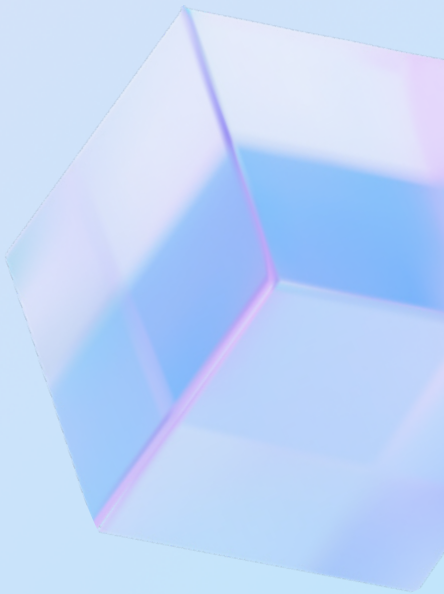
- **59%** компаний, которым «Инфосистемы Джет» оказывала услугу мониторинга внешних угроз, **упоминаются на DarkNet-форумах и в Telegram-каналах** хакерской или мошеннической тематики.

- Работники чаще всего регистрируются на внешних сервисах, используя корпоративный аккаунт, в онлайн-маркетах, сервисах страхования и медицинских услуг. **В 27% случаев среди «слитых» учетных записей** мы обнаруживали связку корпоративный логин-пароль, то есть пользователи регистрировались на различных ресурсах с использованием своей рабочей почты. При этом практика использования «любимого одного универсального» пароля значительно упрощала последующий взлом корпоративных сервисов. **В 35% случаев учетная запись упоминалась в связке с хэшем** пароля.

- Потенциально **вредоносные фишинговые веб-ресурсы**, на которых в любой момент может быть размещен опасный контент, **обнаруживаются почти для каждого нашего клиента** (92% компаний). При этом **треть таких ресурсов** (29%) **уже имела готовое веб-содержимое** и использовалась в мошеннических схемах.



- Наибольший **интерес к проведению киберучений мы фиксировали в промышленной и финансовой отраслях,** при этом компании стали увеличивать количество тренировок в год, уходя от «разовых» практик. Наиболее востребованным остается проведение киберучений для специалистов SOC (Security Operations Center): аналитиков первой линии (90% запросов) и второй линии (80% запросов) реагирования на инциденты ИБ.



- Мы отмечаем **рост спроса на услуги тестирования DRP- и BCP-планов более чем на 30%.** Самый тестируемый сценарий — сценарий успешной атаки вируса-шифровальщика.

- С конца 2023 — начала 2024 года мы фиксируем смещение интереса компаний с классического «инфраструктурного» пентеста в сторону целевых пентестов: вместо запроса «получить доступ, куда получится» компании начали более зрело подходить к постановке целей и выбирать проверку реализации катастрофических гипотез. Топ-3 типов уязвимостей, которые позволили быстрее всего реализовать цели в рамках тестирований на проникновение:

Некорректные (избыточные) права доступа в AD или ИС

Неустановленные критичные обновления безопасности

SQL-инъекции

АННОТАЦИЯ

Настоящий отчет представляет собой анализ ландшафта угроз кибербезопасности, в котором освещаются наиболее частые кибератаки, а также рассматриваются ключевые тенденции и эволюция угроз в различных секторах, выявленные Jet CSIRT и экспертными подразделениями «Инфосистемы Джет» в 2024 году.

В 2024 году ландшафт угроз кибербезопасности продолжает развиваться: на фоне усложнения угроз происходит смещение фокуса с защиты инфраструктуры на обеспечение непрерывности операционной деятельности, проактивное обнаружение потенциальных атак с использованием средств анализа внешних цифровых рисков, сверхоперативную адаптацию к новым угрозам и восстановление после инцидентов ИБ. Тренды 2024 года отражают этот сдвиг: после всплеска атак шифровальщиков в начале года компании активно инвестировали в инструменты кризис-менеджмента (актуализация и тестирование планов непрерывности/планов коммуникации), усиливали контроль за рисками цепочек поставок, обеспечивали защиту и развивали систему резервного копирования.

Сохраняющийся дефицит навыков в области кибербезопасности, недостаток навыков команд реагирования и «киберусталость» рядовых пользователей продолжают быть одними из ключевых проблем для сохранения устойчивости организаций к кибератакам, стимулируя компании концентрироваться на обучении команд реагирования и повышении общей культуры информационной безопасности.

В этом отчете мы рассматриваем ключевые тренды кибербезопасности 2024 года, а также прогнозы развития кибериндустрии на 2025 год.

Jet CSIRT — коммерческий центр мониторинга и реагирования на инциденты информационной безопасности, оказывающий услуги мониторинга и оперативного реагирования на инциденты, проактивного поиска угроз, защиты бренда, цифровой криминалистики, поиска следов компрометации и другие экспертные сервисы. Среди клиентов Jet CSIRT как крупные коммерческие компании из сферы ИТ, финансового сектора, ритейла, недвижимости, так и государственные организации.

ЧТО МЫ НАБЛЮДАЛИ В 2024 ГОДУ

1. МОНИТОРИНГ И РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ

В 2024 году, за период с января по конец ноября, центр мониторинга и реагирования на инциденты Jet CSIRT зафиксировал более 10 тысяч инцидентов[1] ИБ, что соизмеримо с результатами 2023 года (напомним, что в 2023 году прирост составил 11% против трехкратного роста в 2022-м). При этом количество инцидентов заметно переросло в качество: на замену довольно простым, но массовым атакам прошлых лет пришли сложные атаки на цепочку поставок и сложные схемы заражения инфраструктур.

Ниже представлено распределение внешних атак по самым популярным категориям инцидентов Jet CSIRT, отражающее картину за год. Пик напряженности пришелся на середину весны — начало лета.

Атака на отказ в обслуживании

Инциденты, связанные с недоступностью внешнего узла или системы, значительное увеличение потребляемых ресурсов на внешних узлах, а также выявление сетевых атак типа «отказ в обслуживании».

Атака с использованием вредоносного ПО

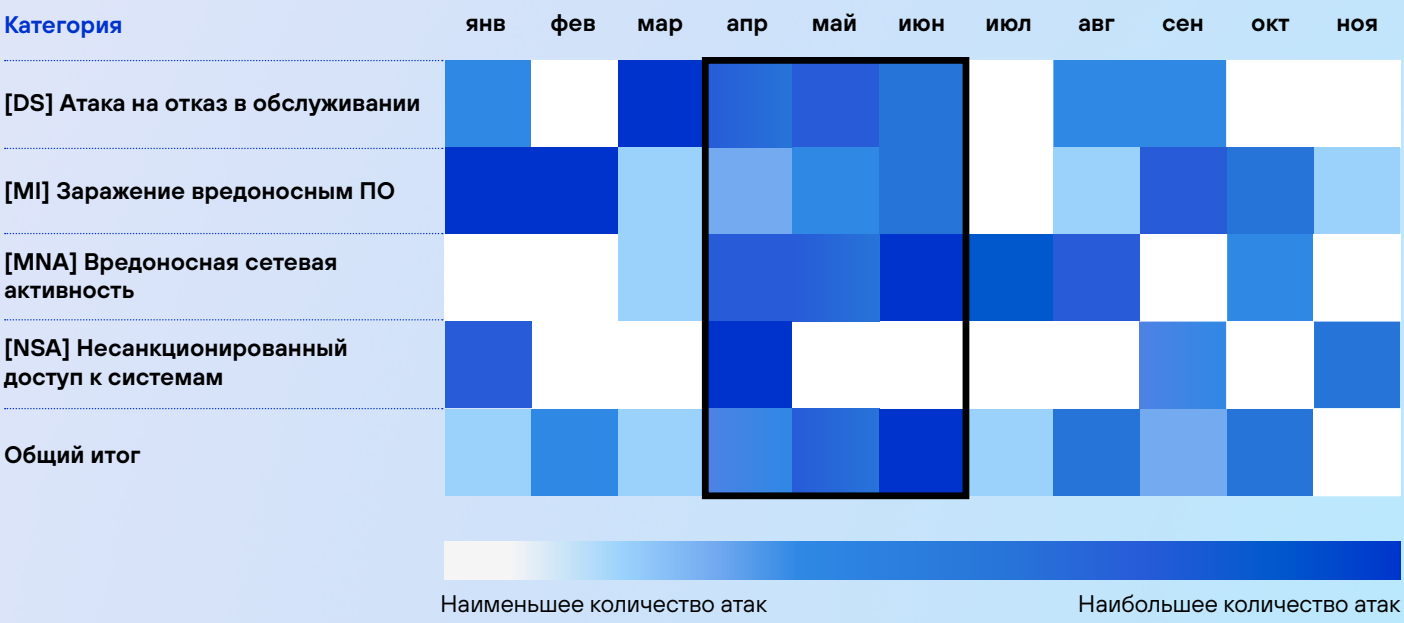
Случаи заражения хостов в защищаемом периметре в результате внешних атак (например, фишинга), а также обнаружение индикаторов компрометации в защищаемом периметре.

Вредоносная сетевая активность

Потенциально опасные внешние 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 успешной аутентификацией после брутфорса на УЗ, и нетипичная активность внешних пользователей.



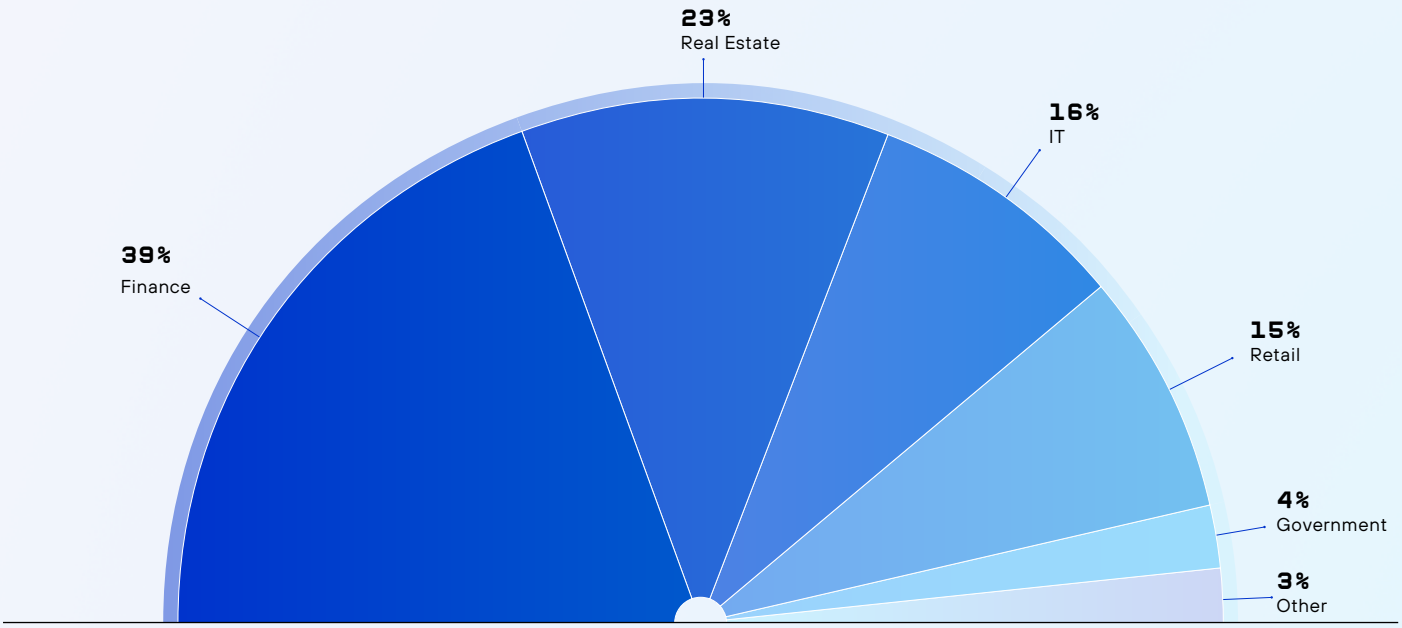
[1] Речь идет об инцидентах, которые мы фиксировали среди компаний, находящихся на мониторинге Jet CSIRT. Мы классифицируем событие как «Инцидент», когда фиксируем подтвержденную нелегитимную активность, исключая ложноположительные срабатывания.

Наиболее атакуемой отраслью за период наблюдения по нашим данным среди клиентов сервиса Jet CSIRT стали финансовые организации. Банки, страховые, кредитные и микрофинансовые организации управляют активами, представляющими наибольший интерес для злоумышленников, — деньгами, и с большей вероятностью заплатят за расшифровку данных, чтобы бизнес не простаивал. Количество инцидентов, зафиксированных в этих организациях, не выходит из нашего топ-3 уже третий год. Скорее всего, не выйдет и в дальнейшем.

На втором месте расположились организации, оказывающие услуги в сфере недвижимости. За год в инфополе не раз появлялась информация об атаках застройщиков и компании из сферы Real estate.

На третьем месте в 2024 году оказались ИТ-компании. Злоумышленники используют их в качестве «трамплина» для доступа в инфраструктуры более крупных организаций. Такие атаки на эксплуатацию доверия — один из самых экономически эффективных способов компрометации. Высокая окупаемость инвестиций (ROI), когда взлом одной компании открывает доступ к сотням или тысячам других, делает ИТ-компании привлекательной целью для хакеров.

Распределение инцидентов по отраслям среди клиентов сервиса Jet CSIRT[2]



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

Мы составили 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 2024 (%)
T1204	User Execution	**44,19%**
T1190	Exploit Public-Facing Application	**18,26%**
T1219	Remote Access Software	**9,85%**
T1021	Remote Services	**7,93%**
T1562.001	Impair Defenses: Disable or Modify Tools	**6,50%**
T1071	Application Layer Protocol	**4,56%**
T1110.001	Brute Force: Password Guessing	**4,18%**
T1133	External Remote Services	**1,81%**
T1046	Network Service Discovery	**1,71%**
T1090.003	Proxy: Multi-hop Proxy	**1,01%**

Сам рейтинг техник претерпел значительные изменения по сравнению с 2023 годом. На первом месте по-прежнему остаются инциденты, связанные с заражением узлов вредоносным ПО, вторыми по частоте стали случаи атак на публично-доступные веб-приложения, а на третье место поднялись инциденты, связанные с использованием ПО для удаленного администрирования, хотя в прошлом году этот тип был на последнем месте.

Mitre_ID		Название техники	2024	Mitre_ID	Название техники	2023
T1204		User Execution		T1204	User Execution	
T1190	+ 1	Exploit Public-Facing Application		T1562.001	Impair Defenses, Disable or Modify Tools	
T1219	+ 7	Remote Access Software		T1190	Exploit Public-Facing Application	
T1021	+ 5	Remote Services		T1110.001	Brute Force, Password Guessing	
T1562.001	- 3	Impair Defenses: Disable or Modify Tools		T1133	External Remote Services	
T1071	new	Application Layer Protocol		T1110.003	Password Spraying	
T1110.001	- 3	Brute Force: Password Guessing		T1071.004	Application Layer Protocol, DNS	
T1133	- 3	External Remote Services		T1090.003	Proxy: Multi-hop Proxy	
T1046	new	Network Service Discovery		T1021	Remote Services	
T1090.003	- 2	Proxy: Multi-hop Proxy		T1219	Remote Access Software	

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.

Большинство инцидентов в данной категории связано с действиями пользователя: посещение сомнительных сайтов, установка недоверенных браузерных расширений, открытие ссылок. В большинстве случаев инцидент нивелируется автоматической работой средств АВЗ либо ручной очисткой пораженного хоста и разъяснительной беседой с пользователем. Львиную долю таких заражений составляют надоедливые варианты AdWare. Реже мы отмечаем случаи целенаправленного заражения (Spear Phishing[3]), являющиеся элементами цепочки APT-атак.

[3] Spear Phishing (целевой фишинг) — подготовленная атака, направленная на то, чтобы обмануть конкретного человека или сотрудников конкретной компании.

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 эксплойтов, что также может представлять интерес для расследования.

Уязвимости в CMS Bitrix, в частности, стали в 2024 году причиной многих взломов, и специалисты нашего отдела киберкриминалистики (форензики) не раз помогали в расследовании инцидентов у наших клиентов. В результате успешной эксплуатации уязвимости BDU:2022-01141 (CVE-2022-27228) CMS Bitrix нашего подрядчика, сайт-визитка Jet CSIRT подверглась дефейсу.

Этот кейс мы подробно расследовали и опубликовали результаты на Habr[1].

[1]

3. **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.

В этом году мы отмечаем существенный рост инцидентов, связанных с программным обеспечением для удаленного доступа. Данное ПО является инструментом №1 в целенаправленных атаках для закрепления на скомпрометированном хосте, откуда злоумышленник может развивать атаку. Часто реализация этой техники связана с нарушением политик безопасности, когда пользователи устанавливают себе подобные программы для удаленного администрирования корпоративных ресурсов.

4. **T1021** — Remote Services. Техника заключается в обнаружении и эксплуатации внутри атакуемой сети легитимных сетевых сервисов удаленного доступа: SSH, RDP, VNC и WinRM сервисы.

Зачастую злоумышленнику необходимо сначала украсть или сбрутить легитимную учетную запись для сервиса в рамках данной атаки. Такая категория техник является классическим примером горизонтального перемещения в атакуемой инфраструктуре.

5. **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.

В рамках расследования инцидентов чаще всего мы фиксируем отключения Windows Defender и изменение правил встроенного Firewall на Windows-узлах. Такое поведение характерно для вирусов шифровальщиков, например LockBit 3.0. При этом основная масса зафиксированных в 2024 году подозрений на инцидент по данной технике носит ложноположительный характер.

6. **T1071** — Application Layer Protocol. Категория вредоносной сетевой активности, которая включает в себя атаки с применением протоколов прикладного уровня.

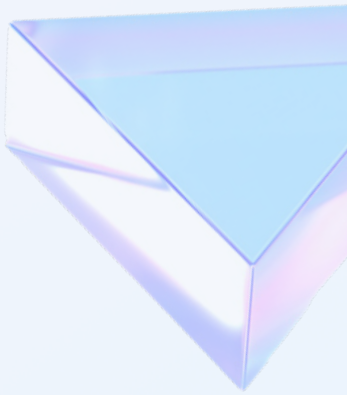
Протоколы прикладного уровня используются злоумышленниками для взаимодействия с командными серверами (C2), туннелирования и маскирования вредоносного трафика. Чаще всего такая нелегитимная активность определяется правилами использующих базы Threat Intelligence. Однако зачастую в эту категорию попадают инциденты нарушения политики безопасности, связанные с использованием программного обеспечения для P2P-обмена. Самым популярным представителем является BitTorrent.

7. **T1110.001** — Brute Force, Password Guessing. К этой технике относятся инциденты, связанные с методами угадывания паролей: внутренние и внешние попытки подбора паролей, нетипичные действия с учетными данными.

В основном данный тип инцидентов был связан с попытками внешнего брутфорса: большинство внешних форм аутентификации, опубликованных в сети Интернет, будут подвержены такой атаке. В этом году мы отмечаем рост популярности данной техники в качестве первичного вектора (Initial Access) проникновения в инфраструктуру.

8. **T1133** — External Remote Services. Сюда относятся инциденты, связанные с атаками на внешние сервисы, такие как VPN, VNC и другие. Зачастую после этих 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. Банальный пример — забытый тестовый сервер с открытым портом удаленного доступа с дефолтными учетными данными.



9. **T1046** — Network Service Discovery. Данная категория содержит инциденты внешнего и внутреннего сканирования, а также другие приемы исследования защищенности.

Стоит отметить, что сканирование происходит в интернете постоянно, поэтому отслеживать каждый случай зачастую неэффективно, так как при должной настройке средства периметральной защиты успешно блокируют попытки сканирования. В большинстве случаев проверка выведет на различные краулеры сервисов поиска общедоступных устройств в интернете, например, таких как Shodan. Поэтому в логику правил выявления инцидентов этой категории интегрированы данные систем Threat Intelligence и фиды угроз, которые добавляют контекст к событиям и позволяют реагировать только на потенциально серьезные попытки атак.

10. **T1090.003** — Proxy: Multi-hop Proxy. Инциденты, связанные с использованием прокси с множественными прыжками (например, сети Tor и i2p).

Tor и другие многоуровневые анонимные сети нередко используются злоумышленниками для скрытия истинного источника атак или организации обратной связи (backdoor) со скомпрометированными активами. При применении таких сетей данные проходят через цепочку промежуточных узлов, а на выходе отображается только адрес так называемого выходного узла. Это позволяет злоумышленникам маскировать свои реальные адреса и избегать их блокировки. Даже если удастся заблокировать конкретный выходной узел, последующие атаки могут идти через другой. При этом

Tor может применяться не только внешними злоумышленниками, но и обычными пользователями внутри корпоративных сетей, что может быть признаком работы инсайдеров в организации или же грубым нарушением корпоративных политик безопасности.

Ринат Сагиров,

руководитель департамента мониторинга и реагирования,
«Инфосистемы Джет»

Сравнение частоты используемых техник за два прошлых года и результаты расследования инцидентов показывают незначительные изменения в привычках атакующих. Злоумышленники чаще предпочитают эксплуатировать уязвимости на сетевом периметре для получения первоначального доступа, так называемые «низко висящие фрукты». В этом году наиболее часто эксплуатируются уязвимости 1C Bitrix и атаки типа брутфорс на RDP/SSH опубликованных серверов. Ключевое изменение — злоумышленники стали работать более скрытно, мимикрируют под поведение администраторов инфраструктуры, используя легитимные инструменты и протоколы администрирования.

КЕЙС

Целенаправленный фишинг с целью кражи данных

Консалтинговая компания обратилась к нам за расследованием инцидента.

В один из дней пользователи заметили ухудшение производительности на узлах под управлением Windows при выполнении повседневных задач, а после обнаружили факт шифрования рабочих файлов. Файлы стали недоступны и получили странное расширение .lock.

Приняв экстренные меры по изоляции зараженной инфраструктуры, мы приступили к оперативному расследованию и установили:

- точкой входа стал целенаправленный фишинг;

- предполагаемые злоумышленники — одна из азиатских APT-группировок;

- пребывание в инфраструктуре — более полугода;

- основная цель взлома — хищение данных, шифрование запущено для отвода глаз.

С учетом результатов расследования инцидента ИБ осуществлялось восстановление инфраструктуры с соблюдением необходимых мер повышения уровня защищенности. После восстановления основных информационных систем и работоспособности бизнес-процессов мы продолжали осуществлять непрерывный мониторинг.

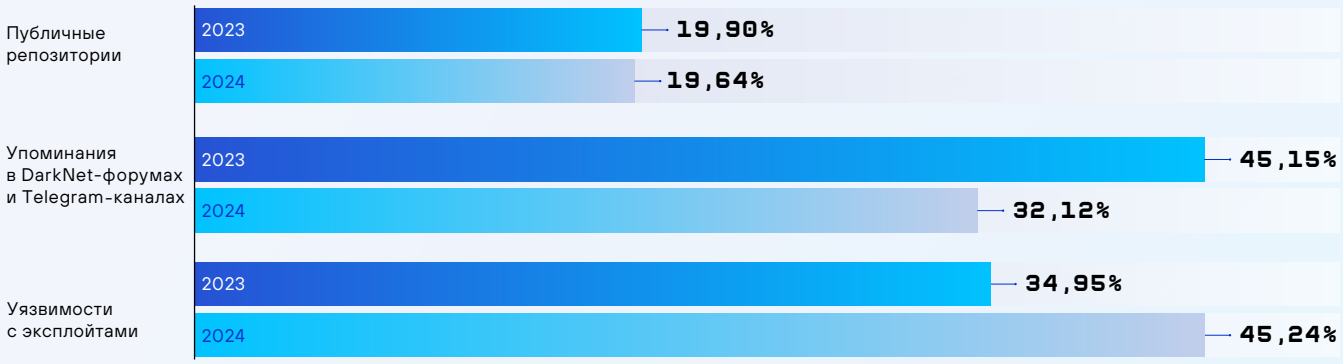
2. УПРАВЛЕНИЕ ПОВЕРХНОСТЬЮ АТАКИ

По данным сервиса анализа внешних цифровых угроз Jet Nautilus, при оценке потенциальных векторов атак для наших клиентов определено:

1. В **33%** случаев были обнаружены учетные данные или исходный код в публичных репозиториях;
2. **59%** компаний упоминается на DarkNet-форумах и в Telegram-каналах хакерской или мошеннической тематики;
3. **76%** компаний используют на внешнем периметре версии ПО (определяемые даже пассивными методами), имеющие критические (Critical) уязвимости с публичными эксплойтами.

Эти данные в целом сопоставимы с результатами, наблюдаемыми нами годом ранее. Сравнение данных 2023 и 2024 годов представлено на диаграмме:

Сравнение числа потенциальных векторов атак в 2023 и 2024 годах



Руслан Амиров,

руководитель экспертных сервисов мониторинга и реагирования Jet CSIRT, «Инфосистемы Джет»

Несмотря на кратное увеличение интереса рынка к направлениям управления поверхностью атаки и управлению уязвимостями, в 2024 году зафиксирован рост количества уязвимостей в корпоративных сервисах, доступных из Всемирной паутины. Подобными уязвимостями может воспользоваться человек с базовыми навыками поиска информации и возможностью задать непонятные вопросы популярной LLM. Своевременное обновление ПО и/или корректировка настроек средств защиты позволяют снизить риск реализации такого вектора проникновения, но не исключают необходимости контроля за угрозами, присущими компаниям в киберпространстве.

КЕЙС

Незащищенный удаленный доступ

Компания из финансового сектора обратилась к нам после взлома инфраструктуры.

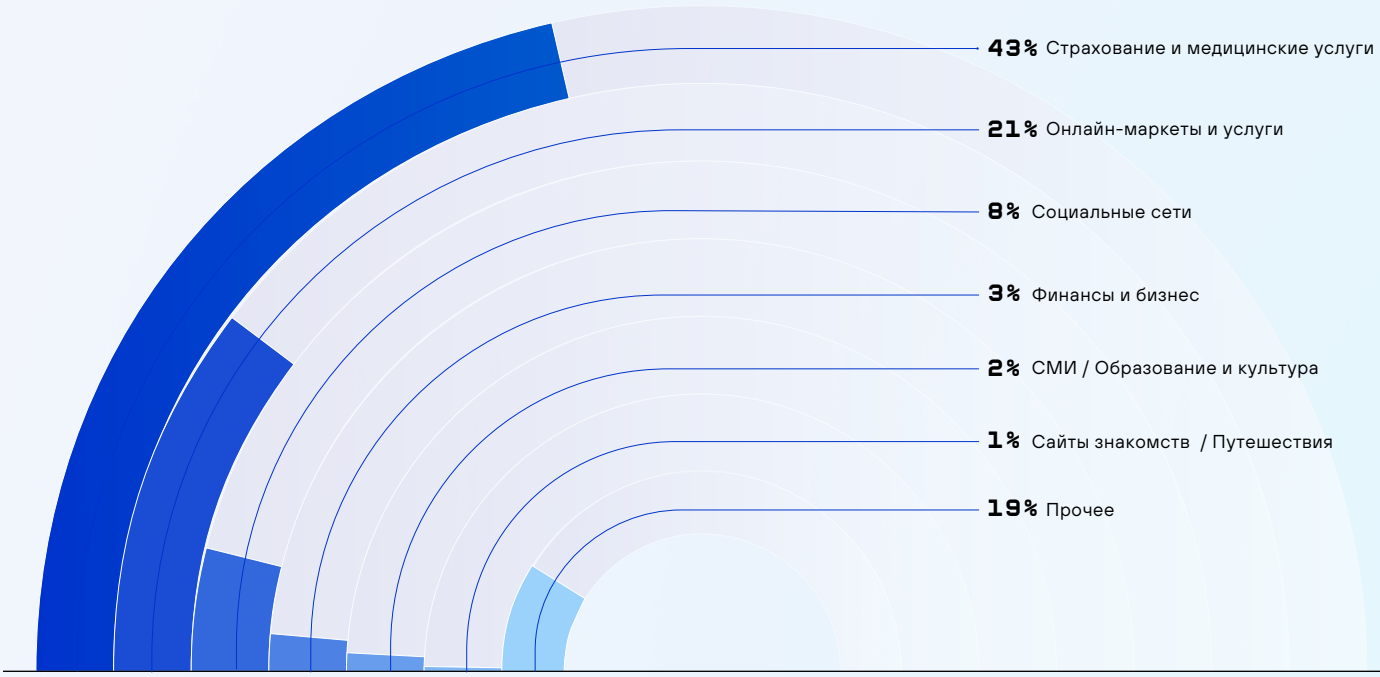
Мы провели работы по поиску и анализу доменов, поддоменов и внешних уязвимых сервисов компании, утечек данных, открытых форм авторизаций, а также мониторинг упоминаний в Telegram и DarkNet. В ходе пассивного сканирования внешних ресурсов компании были обнаружены сведения о наличии на одном из серверов открытого RDP-порта на протяжении длительного времени вплоть до даты инцидента. Дальнейшее расследование подтвердило, что злоумышленники обнаружили этот сервер и провели успешную атаку именно посредством уязвимого сервиса удаленного доступа. Взлом можно было предотвратить, если поиск уязвимых сервисов проводился бы на систематической основе.

3. МОНИТОРИНГ ВНЕШНИХ ЦИФРОВЫХ УГРОЗ ДЛЯ КОНТРОЛЯ ЗА ЧУВСТВИТЕЛЬНЫМИ ДАННЫМИ

С помощью сервиса защиты от внешних цифровых угроз Jet Nautilus мы системно анализируем DarkNet для поиска «слитых» учетных записей, относящихся к инфраструктуре наших клиентов, которые могут быть использованы атакующими.

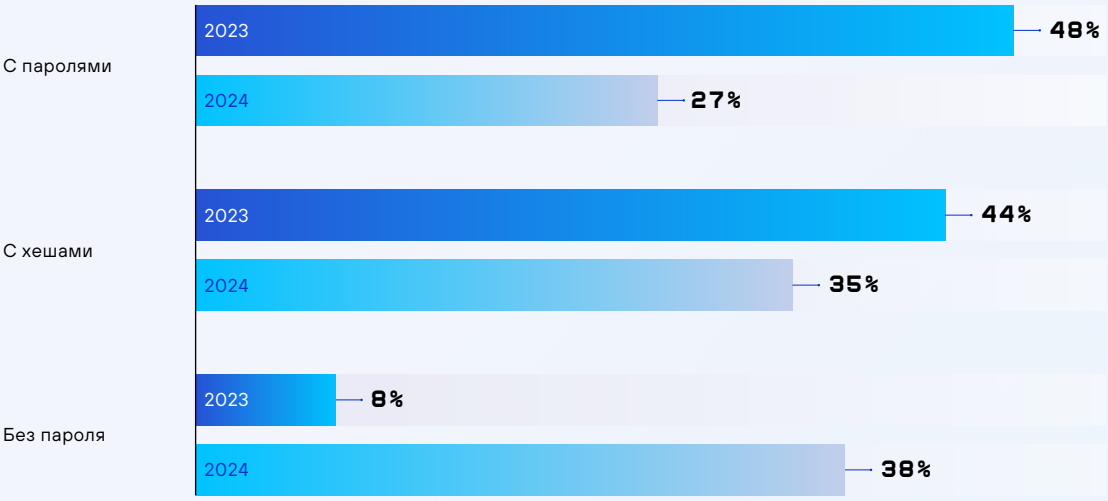
По сравнению с 2023 годом количество утечек анализируемых компаний возросло на 60%. Распределение утечек по сервисам, где сотрудники оставляли УЗ, не изменилось: лидируют сервисы страхования и онлайн-маркеты, где работники чаще всего регистрируются с корпоративными учетными данными.

В каких сервисах работники чаще всего регистрируются, используя корпоративный аккаунт



В 27% случаев среди «слитых» учетных записей мы обнаруживали связку корпоративный логин-пароль, то есть пользователи регистрировались на различных ресурсах с использованием своей рабочей почты. При этом практика использования «любимого одного универсального» пароля значительно упрощала последующий взлом корпоративных сервисов. В 35% случаев учетная запись упоминалась в связке с хэшем пароля.

Сравнение данных по утечкам 2023 и 2024 годов



В 2024 году количество утечек, содержащих аутентификационные данные пользователей, относительно 2023 года заметно снизилось, что может свидетельствовать об изменениях как в системах хранения парольной информации (например, отказ от хранения паролей в открытом виде, использование хеш-функций «с солью»), так и в ориентации злоумышленников на публикацию другой чувствительной внутренней информации компаний, в том числе файлов с компьютеров пользователей. Об этом также свидетельствует характер утечек в публичных кейсах.

- В июле 2024 года хакерская группировка C.A.S. выложила в открытый доступ дамп ИТ-компании Avanpost. Утечка содержала внутренние документы, исходные данные систем аутентификации программ, исходный код программ, базы знаний, парольную информацию для удаленного доступа к сервисам клиентов. Злоумышленники зашифровали 405 виртуальных машин и большинство рабочих станций работников. Было уничтожено более 60 ТБ данных. Также в открытый доступ попала клиентская база.
- В октябре 2024 года на Dark-форуме пользователь выложил дамп с ПК одного из сотрудников ООО МНПП «АНТРАКС» (АСУ ТП). Утечка содержала внутренние доку-

менты, исходный код программ, базы знаний, парольную информацию для удаленного доступа к сервисам, почтовые переписки и парольную информацию клиентов.

- В октябре 2024 года хакерская группировка DumpForums заявила о предполагаемом взломе инфраструктуры компании «Доктор Веб» (Dr.Web) (компания не признала инцидент). Злоумышленники выгрузили сервер корпоративного GitLab, где хранились внутренние разработки и проекты, сервер корпоративный почты, Confluence, Redmine, Jenkins, Mantis, RocketChat — системы, где велась разработка и обсуждались задачи. Также злоумышленники выгрузили клиентскую базу и заполучили доступ к домен-контроллеру (в открытый доступ выложили только почты сотрудников информационной безопасности Dr.Web).

Путем анализа доменных имен мы также отслеживаем регистрацию новых доменов, изменение уже существующих ресурсов, которые потенциально могут использоваться злоумышленниками для проведения атак на инфраструктуру, мошеннической деятельности, сбора контактных данных целевой аудитории клиента, нанесения ущерба бренду.

Потенциально вредоносные веб-ресурсы, которые «ждали своего часа» и на которых в любой момент может быть размещен опасный контент, — «фишинговый» веб-ресурс или вредоносное ПО — были обнаружены почти для каждого нашего клиента (92% компаний). При этом треть таких ресурсов (29%) уже имела готовое веб-содержимое и использовалась в мошеннических схемах.

Анастасия Кисько,

руководитель сервиса проактивного мониторинга внешних цифровых угроз Jet CSIRT, «Инфосистемы Джет»

Для проведения фишинговых атак злоумышленники все чаще используют готовые боты, которые автоматизируют процесс создания и распространения вредоносных ссылок и поддельных веб-страниц. Эти боты могут имитировать действия реальных пользователей, отправляя фишинговые сообщения через электронную почту, социальные сети или мессенджеры. Использование таких ботов значительно упрощает процесс и автоматизирует процесс.

Также отмечается тенденция на отслеживание метаданных потенциальных жертв фишинга. Это означает, что фишинговые сайты могут быть настроены так, чтобы открываться только для пользователей из определенных стран или регионов, где злоумышленники ожидают, что жертвы будут более восприимчивы к их уловкам. В остальных случаях происходит перенаправление на официальные сайты.

КЕЙС

Фишинговые страницы маркетплейсов

В последние месяцы 2024 года злоумышленники сделали упор на подделку страниц популярных российских маркетплейсов. Так, в преддверии сезона распродаж и предновогодних праздников нами было обнаружено значительное количество фишинговых ресурсов, нацеленных на пользователей «Яндекс Маркет», как схожих по написанию (yandexmar.com, yandexmar.top, yandexmar.vip, yandexmars.top, yandexmar.cc, yandexmarkets.com и т.д.), так и нет (например, mercadoliprs.com и mercadoliprs.vip). Эти сайты используют доменные имена, схожие с официальными, а также имитируют товарный знак «Яндекс Маркет» и содержат форму для авторизации.

4. УПРАВЛЕНИЕ РИСКАМИ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ И КИБЕРРАЗВЕДКА

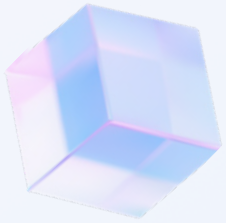
Тренд «атаки через доверенных поставщиков» (Trusted Relationship) продолжил свое устойчивое развитие в 2024 году.

- В **17%** киберкриминалистических расследований мы фиксировали подозрение на компрометацию поставщиков. В основном атакующие использовали взломанные учетные записи компаний малого и среднего бизнеса, оказывающих сервис жертве. Используя сервисы удаленного доступа (как правило, клиентский VPN без второго фактора), злоумышленники доставляли в более защищенную инфраструктуру инструменты и шифровали данные.
- **83%** подрядных организаций, оказывающих услуги клиентам сервиса Jet Nautilus, используют на внешнем периметре версии программного обеспечения, имеющие уязвимости уровня Critical и High с публичными эксплойтами. В среднем у одного подрядчика насчитывается 93 уязвимости с возможностью использования эксплойтов.
- Более **30%** компаний — подрядчиков наших клиентов упоминаются на DarkNet-форумах и в Telegram-каналах хакерской или мошеннической тематики.

В ответ на популярную угрозу компании продолжают усиливать меры по безопасному взаимодействию с подрядчиками. Мы провели сравнительный анализ данных, полученных в ходе исследования риска эксплуатации доверия (2022–2023 годы), с данными аудитов и опросов российских компаний текущего года[4].

[4] Сравнение проведено на аналогичной выборке из 50 российских компаний среднего и крупного бизнеса.

Компании начали проводить более глубокий анализ безопасности подрядчиков на этапе заключения договоров и регулярно пересматривать их статус. При этом все большую популярность набирают сервисы анализа поверхности атак своих подрядчиков. Это позволяет выявлять уязвимые места еще до того, как они станут целями злоумышленников.



Оцениваете ли вы уровень риска ИБ поставщиков до начала взаимодействия?	**2024 год**	**2022-2023 годы**
Проводим свой/независимый аудит для критичных поставщиков	**36%**	**17%**
Проводим только проверку по линии СБ	**48%**	**68%**
Третьи лица заполняют анкету с вопросами по ИБ	**16%**	**15%**

Кроме того, компании внедряют политики взаимодействия с подрядчиками, закрепляющие процедуры по минимизации рисков, уходя от «размазанных» по документам общих правил передачи информации.

Формализован ли процесс безопасного взаимодействия с поставщиками?	**2024 год**	**2022-2023 годы**
Есть отдельный документ, детализирующий меры безопасности при работе с поставщиками	**48%**	**19%**
Есть требования только по безопасной передаче информации поставщикам	**42%**	**71%**
Нет или в процессе разработки	**10%**	**10%**

Компани стали чаще включать в свои планы реагирования на инциденты сценарии атак через поставщиков, а также ставить критичные учетные записи на мониторинг, чтобы сократить время на обнаружение и ликвидацию последствий атаки.

Какие меры по мониторингу событий ИБ, связанных с поставщиками, реализованы?	2024 год	2022-2023 годы
Есть отдельные правила на учетки поставщиков, СЗИ или критичную инфраструктуру, к которой поставщики имеют доступ	48%	18%
Осуществляем мониторинг событий ИБ в целом, фокус на поставщиков не делаем	48%	77%
Иное	4%	5%

Александр Морковчин,

руководитель отдела развития консалтинга по информационной безопасности, «Инфосистемы Джет»

Данные наших аудитов, расследований и опросов показывают, что компании начали делать стратегические шаги для предотвращения угроз, чтобы обеспечить надежность всей цепочки поставок, вместо реагирования на инциденты и «пожаротушения».

КЕЙС

Шифровальщик через ИТ-подрядчика

Компания из финансового сектора обратилась к нам за помощью, когда SOC заметил нетипичные подключения к ИТ-системам от имени сервисных учетных записей.

При расследовании мы поняли, что инфраструктура скомпрометирована:

- злоумышленники проникли в инфраструктуру в ночное время;
- подключение производилось с использованием УЗ подрядчика;
- использовался VPN без многофакторной аутентификации.

Подрядчик занимался разработкой и поддержкой специализированного ПО и имел повышенные привилегии на серверах разработки. От имени скомпрометированных УЗ проводилось исследование инфраструктуры, атака на контроллер домена. Далее злоумышленники проводили множественные RDP-подключения к доступным серверам — изучали инфраструктуру. На одном из серверов были обнаружены скрипты, где в открытом виде хранятся логины и пароли сервисных УЗ для БД. При попытке подключений к одной из БД злоумышленники были обнаружены.

Был запущен процесс оперативного реагирования:

- блокировка IP-адресов, с которых осуществлялось подключение злоумышленников;

- сброс VPN-сессий;

- блокировка УЗ;

- смена паролей в AD.

А также запущены процессы по детальному исследованию скомпрометированных узлов и срочное внедрение сервиса многофакторной аутентификации.

Стоит отметить, что в нашем кейсе реагирование было проведено вовремя и неожиданно для атакующих. В это же время как минимум две крупные компании из энергетического сектора и одна компания из финансового сектора были атакованы с использованием той же самой УЗ подрядчика, которая использовалась злоумышленниками в данном инциденте.

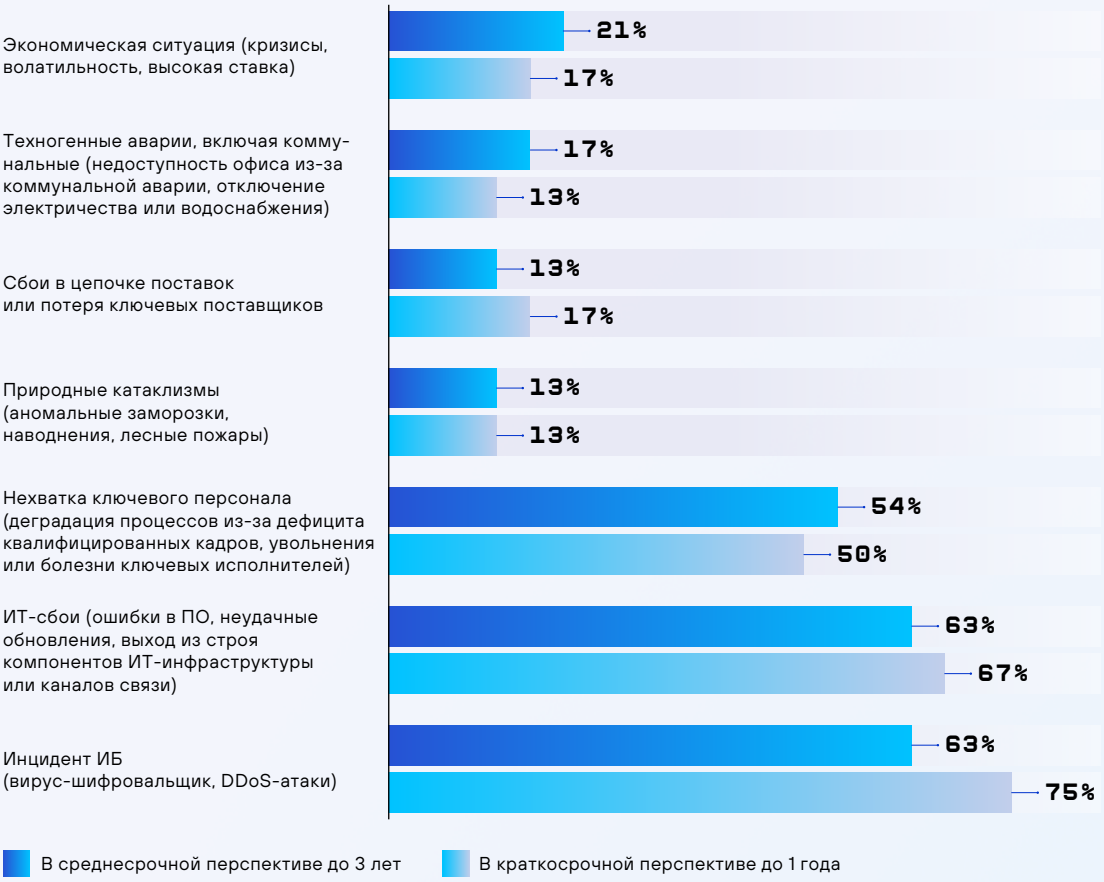
Хакеры стали действовать быстрее, без длительного исследования инфраструктуры. Как итог — зашифрованные данные и требование выкупа.

5. НЕПРЕРЫВНОСТЬ БИЗНЕСА

Серия громких инцидентов, связанных с вирусами-шифровальщиками в российских компаниях, заставляет бизнес все чаще задаваться вопросом: «Если это случится у нас, за какое время мы сможем восстановиться?» Соблюдение целевых сроков восстановления критически важных информационных систем в случае успешной атаки напрямую влияет на устойчивость компании и размер потенциального ущерба. При этом и в краткосрочной, и в более отдаленной перспективе киберугрозы рассматриваются компаниями в качестве ключевого риска нарушения деятельности.

Какие наиболее вероятные угрозы прерывания деятельности вы видите для своей организации? Мультивыбор	**В краткосрочной (до 12 месяцев) перспективе**	**В среднесрочной (до 3 лет) перспективе**
Инцидент ИБ (вирус-шифровальщик, DDoS-атаки)	**75%**	**63%**
ИТ-сбои (ошибки в ПО, неудачные обновления, выход из строя компонентов ИТ-инфраструктуры или каналов связи)	**67%**	**63%**
Нехватка ключевого персонала (деградация процессов из-за дефицита квалифицированных кадров, увольнения или болезни ключевых исполнителей)	**50%**	**54%**
Природные катаклизмы (аномальные заморозки, наводнения, лесные пожары)	**13%**	**13%**
Сбои в цепочке поставок или потеря ключевых поставщиков	**17%**	**13%**
Техногенные аварии, включая коммунальные (недоступность офиса из-за коммунальной аварии, отключение электричества или водоснабжения)	**13%**	**17%**
Экономическая ситуация (кризисы, волатильность, высокая ставка)	**17%**	**21%**

Какие наиболее вероятные угрозы прерывания деятельности вы видите для своей организации?

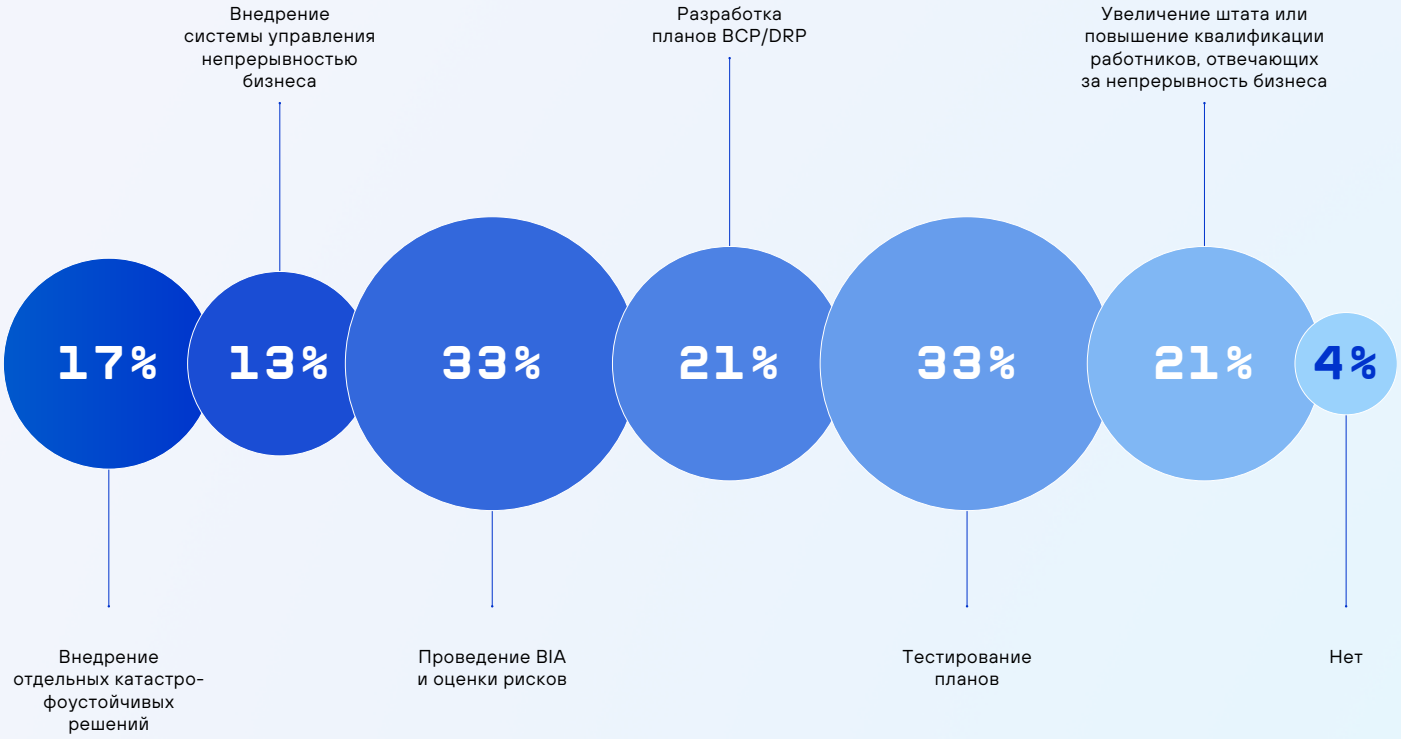


Такие ожидания, а также серии громких инцидентов с компаниями СДЭК, «Верный» и прочими формируют среди руководителей крупных компаний устойчивый тренд независимого подтверждения собственной киберустойчивости. Мы отмечаем, что спрос на услуги тестирования Disaster recovery и Business continuity планов увеличился более чем на 30%, где самым частым тестируемым сценарием был выбран сценарий успешной атаки вируса-шифровальщика.

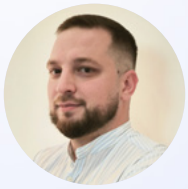
В 2025 году мы ожидаем рост интереса к направлению непрерывности бизнеса, увеличение спроса на выстраивание процессов и стратегий устойчивости, что подтверждают данные нашего опроса российских компаний по планам на ближайшие 2–3 года и запросы клиентов. В настоящий момент сам процесс управления непрерывностью бизнеса почти в 40% компаний до сих пор находится на уровне «у нас есть система резервного копирования, в случае сбоя восстановимся как-нибудь».

Планы развития системы управления непрерывностью в ближайшие 2–3 года Мультивыбор	**Итог**
Внедрение отдельных катастрофоустойчивых решений	17%
Внедрение системы управления непрерывностью бизнеса	13%
Нет	4%
Проведение BIA и оценки рисков	33%
Разработка планов BCP/DRP	21%
Тестирование планов	33%
Увеличение штата или повышение квалификации работников, отвечающих за непрерывность бизнеса	21%

Планы развития системы управления непрерывностью в ближайшие 2–3 года



Вместе с тем внедрение процесса управления непрерывностью бизнеса несет и ряд неочевидных выгод. Так, более 38% респондентов отмечают, что результаты Business impact analysis используются для обоснования бюджетов служб ИТ и ИБ, показывая стоимость простоя бизнеса.



Аскар Мусаев,

эксперт по непрерывности бизнеса, «Инфосистемы Джет»

Бизнес чаще всего не готов к полноценным симуляциям инцидентов в ходе тестирований, и, на наш взгляд, это связано не только с высокими трудозатрами при таком формате учений, но и с недостаточно детализированными планами реагирования и восстановления. Более предпочтительным вариантом тестирований в таких случаях становится настольное (tabletop) тестирование, в рамках которого не только оценивается корректность базовых планов и стратегий восстановления, но и проверяется способность к ситуативному реагированию на не учтенное в планах развитие инцидента.

КЕЙС

Настольное тестирование киберустойчивости

Компания пыталась ответить на вопрос «Как мы будем реагировать и как быстро мы восстановимся, если нас зашифруют?». Лучшим ответом стало настольное тестирование готовности компании к инциденту-шифровальщику.

Для проведения тестирования нами были заранее определены участники: представители ИТ и ИБ, ответственные за внешние и внутренние коммуникации, представители бизнеса. Была разработана подробная легенда, включающая в себя предполагаемое заражение и развитие атаки, а затем уже и непосредственное шифрование. Помимо этого, была определена методология оценки реагирования и восстановления. На каждом из шагов участникам тестирования задавались вопросы об их действиях, которые оценивались наблюдателями по различным критериям. Тестирование прошло в две итерации и заняло суммарно более шести часов.

По итогу у команд реагирования повысилась слаженность и улучшилось взаимодействие, что подтвердил реальный инцидент (дефейс сайта), случившийся на следующий день. Помимо этого, нами был подготовлен ряд технических предложений — например, практический анализ защищенности контура резервного копирования, а также рекомендации по улучшению процесса восстановления и реагирования.

6. ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

С конца 2023 — начала 2024 года мы фиксируем смещение интереса с классического «инфраструктурного» пентеста в сторону целевых тестирований на проникновение: так, вместо запроса «получить доступ, куда сможете» компании начали более зрело подходить к постановке целей и выбирать проверку реализации катастрофических гипотез.

Компании стали объединять работы с учетом различных нормативных требований с целью проведения единого комплексного тестирования, в рамках которого также можно оценить защищенность сегментов сети, неподпадающих под область действия регуляторных требований.

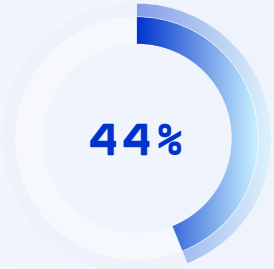
В 2024 году продолжился тренд на комплексные проекты по тестированию на проникновение, когда компании хотят проверить свой уровень защищенности сразу на нескольких уровнях. Внешнее тестирование на проникновение не заканчивается на получении привилегированного доступа на компонентах внешнего периметра, а подразумевает развитие атаки во внутренней ЛВС с целью проверки защищенности критичных для непрерывности бизнеса информационных систем и систем резервного копирования, а также мест хранения конфиденциальных данных. С точки зрения векторов получения доступа во внутреннюю ЛВС также рассматриваются различные беспроводные технологии и социотехническое тестирование.

Также продолжился тренд на проверку своих подрядных организаций, вызванный ростом числа реальных инцидентов, происходящих с подрядными организациями. При этом данные проекты условно можно разделить на две составляющие. Это либо проверка защищенности нашего клиента при сценарии, когда мы осуществляем тестирование от лица его подрядчика (с легитимным VPN-доступом и аутентификационными данными ИС), либо проверка защищенности самой подрядной организации.

С точки зрения уязвимостей, которые наиболее часто встречались в ходе наших проектов на периметре компаний, стоит отметить классические уязвимости веб-приложений, такие как XSS, SQLi и IDOR. Они встречались либо в самописных приложениях, либо в приложениях, написанных на заказ подрядными организациями.

Что касается внутренней сети, то ключевые угрозы, позволяющие получить привилегированный доступ к критичным ИС, по-прежнему связаны с несвоевременным устранением уязвимостей, для которых производители выпустили обновления безопасности, но которые не были своевременно установлены, либо связаны с избыточными правами доступа, выдаваемыми сотрудникам или сервисным учетным записям.

По нашей внутренней статистике, в 2024 году к топ-3 уязвимостей, позволяющих реализовать цели работ, можно отнести:



Некорректные (избыточные) права доступа в AD или ИС

Неустановленные критичные обновления безопасности

SQL-инъекции

Алексей Куприянов,

руководитель группы практического анализа защищенности,
«Инфосистемы Джет»

В 2024 году можно отметить существенное увеличение количества запросов на проверку эффективности работы ИБ-подрядчиков. Это как оценка эффективности существующих сервисов AntiDDoS, так и запросы на проведение RedTeam-упражнений с целью оценки услуг, предоставляемых коммерческими SOC.

КЕЙС

Flipper Zero: захват ПК через мышку, или Нестандартный подход проникновения в домен

В рамках проведения работ по внутреннему тестированию был получен доступ к ПК заместителя директора по ИТ через беспроводную мышку, позволяющий обойти стандартные меры безопасности. Это стало возможным благодаря маленькому устройству Flipper Zero, которое было использовано для имитации клавиатуры. Flipper перехватил сигнал от беспроводной мышки, ввел команды запуска в командной строке и запустил PowerShell-скрипт. Скрипт запустил замаскированный файл, который позволил установить соединение с сервером команд и контроля (command & control, C2) через редиректоры. С учетом того, что зараженный пользователь имел права администратора домена, стало возможным удаленно управлять захваченным хостом и использовать данный хост как плацдарм для дальнейшего продвижения по сети.

7. КИБЕРУЧЕНИЯ

Недостаток квалификации ИБ-команд снижает способность эффективно реагировать на угрозы. Мы наблюдаем, что в компаниях растет понимание важности проведения киберучений на регулярной основе: если в 2023 году киберучения зачастую ограничивались разовыми тренировками, то в 2024-м компании стали увеличивать количество тренировок в год. Уменьшение времени, необходимого для адаптации новых сотрудников к особенностям процесса, а также сокращение времени реагирования на инциденты повышают общую киберустойчивость компании.

В 2024 году наибольший интерес к проведению киберучений мы отмечали в промышленной и финансовой отраслях. Количество атак на объекты критической информационной инфраструктуры остается стабильно высоким, что объясняет спрос на подобные тренировки в данных сферах.

Наибольший спрос мы фиксируем на проведение киберучений в небольших группах — от 5 до 15 человек. В части состава участников наиболее востребованным является проведение киберучений для специалистов SOC (Security Operations Center), а именно для аналитиков первой линии (90% запросов) и второй линии (80% запросов) реагирования на инциденты ИБ. Так, в киберучениях могут участвовать не только аналитики, но и специалисты по защите АСУ ТП и ИТ-специалисты. Однако мы отмечаем, что спрос на обучение именно для ИТ-специалистов пока еще остается невысоким.

Одним из самых эффективных подходов стало использование в обучающих сценариях реальных инцидентов безопасности, которые расследовали эксперты Jet CSIRT у наших клиентов. Среди них эксплуатация уязвимостей в Битрикс, сохраняющие актуальность атаки шифровальщиков, действия инсайдеров, компрометация инфраструктуры через вредоносные почтовые вложения и ошибки конфигурирования инфраструктуры.

Дмитрий Казмирчук,

руководитель группы сервиса киберучений, «Инфосистемы Джет»

Среди новых трендов киберучений — адаптация сценариев под инфраструктуру компании: практические задания модифицируются с учетом используемых и привычных для специалистов ИБ защитных средств. Помимо стабильного спроса на классические тренировки для профильных специалистов, в 2024 году заметно вырос интерес к интерактивному повышению осведомленности рядовых сотрудников.

КЕЙС

По следам CyberCamp 2024

В октябре 2024 года мы провели онлайн-кэмп по кибербезопасности CyberCamp 2024, посвященный цепочке атаки (Cyber Kill Chain). В течение трех дней свыше 6 тысяч участников выполняли задания индивидуально, а 138 команд приняли участие в киберучениях.

Киберучения проводились одновременно для корпоративной и студенческой лиг, причем задания для обеих групп были идентичными. Корпоративные команды традиционно показали высокие результаты в заданиях по эксплуатации средств защиты, поскольку это часть их повседневной работы. Однако некоторые студенческие команды добились успеха, набрав в ряде заданий максимальные баллы, чего не смогли достичь корпоративные участники. Это продемонстрировало способность студентов быстро адаптироваться и осваивать новое.

Лучшие результаты в навыках Offensive Security остались за корпоративной лигой: средний балл корпоративных команд составил 1052, тогда как студенческих — 686. При этом 13% студенческих команд по итогам всех заданий показали результаты, аналогичные лидерам корпоративной лиги.

ПРОГНОЗЫ НА 2025 ГОД

Сложные атаки на цепочки поставок, рост числа атак на критическую инфраструктуру, инвестиции в киберучения и инструменты кризис-менеджмента и многое другое — все это формировало развитие индустрии в 2024 году. Какие тренды и угрозы будут определять киберпространство в следующем году? Мы предлагаем вашему вниманию прогнозы и направления, которые, на наш взгляд, будут играть ведущую роль в формировании стратегий безопасности.

ОБЪЕДИНЕНИЕ КОНЦЕПЦИЙ КИБЕРБЕЗОПАСНОСТИ И НЕПРЕРЫВНОСТИ БИЗНЕСА В ЕДИНУЮ СТРАТЕГИЮ КИБЕРУСТОЙЧИВОСТИ

Кибербезопасность и непрерывность бизнеса — концепции, которые должны работать симбиотически вместе, но многие компании по-прежнему воспринимают их как отдельные направления, зачастую за счет сложившегося разделения обязанностей (например, когда за непрерывность и восстановление отвечает исключительно блок ИТ). В 2025 году ожидается усиление тренда на интеграцию этих концепций в единый подход киберустойчивости, признающий неизбежность инцидентов и фокусирующийся на способности организаций эффективно противостоять угрозам и быстро восстанавливаться.

ПЕРЕХОД ОТ ПЛАНОВОЙ К АДАПТИВНОЙ КИБЕРБЕЗОПАСНОСТИ

Фокус на статических оценках рисков, которые быстро устаревают, ограниченное использование данных киберразведки, формальное тестирование планов реагирования, статические правила вместо постоянного обучения и изменения не позволяют эффективно реагировать на стремительно меняющиеся инструменты и методы атакующих.

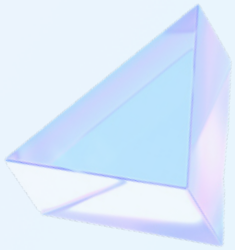
В 2025 году мы ожидаем трансформацию подходов к кибербезопасности организаций от традиционного планирования к более гибким и адаптивным моделям: непрерывная киберразведка и более интенсивный обмен данными об угрозах

между компаниями, развитие решений оркестрации, автоматизации и прогнозирования ИБ, технологий динамического управления доступом, решений SOAR, EDR ускорят этот переход. Несмотря на очевидные риски в случае сбоев, специалисты по ИБ вынуждены все больше доверять в реагировании на подозрительные события средствам автоматизации, потому что человек не способен обеспечить необходимую оперативность в принятии решений 24x7.

УВЕЛИЧЕНИЕ ЧИСЛА «ГЛУБОКИХ ФЕЙКОВ»

Атаки становятся более таргетированными благодаря анализу больших данных о человеке, включая его связи, привычки и интересы. Злоумышленники активно применяют общедоступные Deepfake-сервисы, сервисы создания синтезированного аудио или видео и данные из социальных сетей, чтобы сделать свои атаки более целевыми и труднораспознаваемыми. Если раньше эти механизмы использовались для направленных атак, то в 2024-м фиксировались даже в массовых атаках на физических лиц, например, в рамках фишинга Fake boss — популярнейшей атаки в Telegram. Мы ожидаем скачок популярности технологий для целей мошенничества и фишинга как точки входа в инфраструктуру.

НАКОПЛЕНИЕ «КИБЕРУСТАЛОСТИ»



Фишинговые предупреждения, постоянные напоминания о безопасности от систем ДБО, рассылки о правилах безопасности от привычных ресурсов, частые новости о крупных утечках и многое другое постепенно формируют утомление, которые люди испытывают из-за необходимости постоянно защищать себя в цифровой среде. Из-за усталости пользователи становятся мишенью для простых, но эффективных атак, читать предупреждения о которых становится просто лень. Поэтому информирование пользователей будет становиться менее формальным, содержать живые и близкие человеку примеры, приобретать элементы интерактива.

«ПЛОХИЕ ПАРНИ РАБОТАЮТ ПРОСТО»

Для атак на разные отрасли атакующие используют небольшой набор популярных техник, распространенные уязви-

мости и недостатки, которые закрываются базовой кибергигиеной и харденингом (настройкой встроенных политик безопасности) элементов ИТ-инфраструктуры. В 2025-м злоумышленники продолжат применять методы, которые легко масштабируются, не требуют сложной подготовки и легко автоматизируются для атак на малые и средние предприятия. Кроме того, использование общедоступных и популярных инструментов двойного назначения, например средств удаленного управления или ИТ-автоматизации, позволят злоумышленникам также маскироваться под легитимную активность и долго оставаться незамеченными в сети компании-жертвы.

СХЕМЫ «ДВОЙНОГО» И «ТРОЙНОГО» ВЫМОГАТЕЛЬСТВА СТАНУТ НОРМОЙ

С начала 2024 года мы фиксируем рост спроса компаний на услуги по расследованию киберинцидентов, связанных с программами-вымогателями. Вслед за распространением практики «тройного» вымогательства на зарубежном рынке, когда злоумышленники не только вымогают деньги за расшифровку и удаление похищенных данных (это «двойное» вымогательство), но и выдвигают требование выплат во избежание DDoS-атаки на их ресурсы (это «тройное» вымогательство), мы ожидаем, что такая практика закрепится и в российском киберпространстве.

SOC – ОРИЕНТАЦИЯ НА РЕЗУЛЬТАТ, А НЕ НА ПРОЦЕССЫ

С середины 2024 года мы наблюдаем тренд на повышение эффективности центров мониторинга и реагирования на кибератаки Security Operations Centers (SOC) за счет внедрения измеримых подходов к результативности. В дополнение к классическим операционным показателям эффективности (время реакции на инциденты, количество обработанных событий или скорость отклика на угрозы) на первый план выходят показатели, получаемые в результате совместной работы с Red Team, например в части обнаружения тестирований на проникновение. Это позволяет более точно определить, как SOC реагирует на сложные и адаптивные атаки, а также оценить качество взаимодействия SOC с другими подразделениями компании.

JET
SECURITY
TEAM

security@jet.su
jetcsirt.su