

CODE RED 2026



Актуальные киберугрозы
для российских организаций



ОГЛАВЛЕНИЕ

ОБ ИССЛЕДОВАНИИ	3
КЛЮЧЕВЫЕ ВЫВОДЫ И ПРОГНОЗЫ	4
ОСНОВНЫЕ ЦИФРЫ	10
ВВЕДЕНИЕ	12
ХОДЫ ПО ТЕМНЫМ КЛЕТКАМ	14
ОСОБЕННОСТИ КИБЕРАТАК НА РОССИЮ	
Ключевые драйверы кибератак в России	16
Методы кибератак	19
Последствия кибератак	24
Выводы и прогнозы	30
ГРОССМЕЙСТЕРЫ ТЕНИ: КТО АТАКУЕТ	33
ОРГАНИЗАЦИИ В РОССИИ	
Финансово мотивированные атакующие	35
Кибершпионаж	48
Хактивизм	66
Выводы и прогнозы	78
В ЦЕНТРЕ ШАХМАТНОЙ ПАРТИИ: КАКИЕ	83
ОТРАСЛИ ПОД ОСОБЫМ ПРИЦЕЛОМ	
Промышленность	85
Госучреждения	90
IT-компании	95
Телекоммуникации	99
Выводы и прогнозы	103
ТАЙНЫЕ ХОДЫ: ПРОБЛЕМЫ В СИСТЕМАХ	107
КИБЕРБЕЗОПАСНОСТИ РОССИЙСКИХ КАМПАНИЙ	
Чувствительные данные в открытом доступе	110
Извечная проблема паролей	113
Проникновение к корпоративную инфраструктуру	115
Проблемы внутри инфраструктуры	128
Выводы и прогнозы	139
РЕКОМЕНДАЦИИ	141
Рекомендации для государства	142
Рекомендации для бизнеса	145

ОБ ИССЛЕДОВАНИИ

В отчете представлены результаты анализа ландшафта киберугроз для российских организаций и даны прогнозы по актуальным киберугрозам на 2026 год. Цель исследования — привлечь внимание компаний, заинтересованных в информационной безопасности, к текущему состоянию киберугроз в стране.

Представленные данные, выводы и прогнозы основаны на экспертизе компании Positive Technologies, исследованиях команд Threat Intelligence и Incident Response экспертного центра безопасности PT ESC, результатах проектов по анализу защищенности веб-приложений и тестированию на проникновение, выполненных специалистами PT SWARM, анализе объявлений на специализированных дарквеб-площадках, проведенном командой PT Cyber Analytics, а также на информации из авторитетных открытых источников.

Наша база инцидентов регулярно обновляется. Следует отметить, что информация о некоторых событиях может поступать значительно позже фактического времени кибератаки. В отчете представлены самые актуальные на момент публикации данные, охватывающие период с 1 июля 2024 года по 26 сентября 2025 года.

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков. В связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. В нашем отчете каждая массовая атака (например, фишинговая рассылка на множество адресатов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы использовали в исследовании, приведены в глоссарии на сайте Positive Technologies.

КЛЮЧЕВЫЕ ВЫВОДЫ И ПРОГНОЗЫ

1 На протяжении многих лет Россия входит в число наиболее приоритетных целей киберпреступников. По нашим данным, в период с июля 2024-го по сентябрь 2025 года на Россию пришлось от 14% до 16% всех успешных кибератак в мире и 72% атак, зафиксированных в СНГ. Мы прогнозируем, что по итогам 2025 года общее количество успешных кибератак вырастет на 20–45% по сравнению с предыдущим годом, а в 2026 году может увеличиться еще на 30–35%.

2 Мы выделили **пять ключевых драйверов кибератак** на российские организации

Рисунок 1. Ключевые драйверы кибератак на Россию



По нашим прогнозам, основное влияние на ландшафт киберугроз в 2026 году будут оказывать два драйвера - темпы цифровизации и геополитическая обстановка

Новые технологии порождают новые уязвимости, которые сложно выявить на ранних этапах внедрения. При этом защита зачастую не успевает за технологиями, особенно в условиях нехватки квалифицированных специалистов и зрелых решений.

Импортозамещение усиливает риски: переход на отечественные IT-решения часто происходит в сжатые сроки, без должного внимания к анализу их защищенности, что упрощает задачу злоумышленникам — особенно при наличии уязвимостей нулевого дня или утечек исходного кода.

Геополитика будет играть не менее важную роль. При снижении напряженности активность хактивистов тоже снизится, а основную угрозу будут представлять киберпреступники, ориентированные на вымогательство и кражу данных. В случае же усугубления геополитической ситуации возрастет число целевых атак на критическую инфраструктуру, усилится деструктивная активность хактивистов.

3

Методы кибератак. Социальная инженерия и вредоносное ПО останутся ключевыми методами кибератак в 2026 году, однако их формы станут более сложными. Уже сегодня наблюдаются многоступенчатые фишинговые кампании, а в будущем злоумышленники все чаще будут использовать искусственный интеллект для создания персонализированных писем и дипфейков, усиливая эффект психологического давления.

В киберпреступном сообществе будет расти востребованность многофункциональных троянов, совмещающих функции инфостилеров, вайперов и шифровальщиков. Популярность сохраняют «тихие» техники, использование легитимных программ, системных утилит и инструментов из категории *living off the land* для сбора данных и подготовки к целевым ударам.

4

Последствия кибератак. Кибератаки в 2026 году чаще будут приводить к комбинированным последствиям — одновременным утечкам данных и нарушениям бизнес-процессов. Это связано с тем, что злоумышленники не ограничиваются шифрованием информации, но также похищают ее для вымогательства или шантажа.

На фоне импортозамещения возрастают риски утечек исходного кода отечественного ПО и персональных данных пользователей. В условиях усиления контроля за обращением с персональными данными организациям, ставшим жертвами утечек, грозят существенные штрафы, а в отдельных случаях — уголовная ответственность должностных лиц.

По мере цифровизации в зону риска попадут системы промышленной автоматизации и IoT-устройства. Их вывод из строя может привести к остановке производственных процессов и срыву операций на объектах критической инфраструктуры.

Кроме того, ожидается рост атак на цепочки поставок: через подрядчиков и поставщиков услуг злоумышленники могут проникать в крупные бизнес-системы, что в случае успешности кибератаки будет приводить к наиболее масштабным последствиям.

5

Финансово мотивированные атаки. Переориентация в мотивах ряда группировок и согласие жертв платить выкупы вымогателям — основные факторы, способствующие эскалации финансово мотивированных атак. Появились так называемые гибридные группы: часть хактивистов начала внедрять тактику вымогательства, характерную для классических финансово мотивированных группировок. Продолжая сопровождать атаки политической риторикой, они шифруют и похищают данные, после чего требуют выкуп за ее восстановление или неразглашение.

Этот тренд особенно опасен, потому что организации демонстрируют готовность идти на уступки злоумышленникам. Выплата выкупа воспринимается как быстрый способ решить проблему, но на практике лишь подпитывает интерес атакующих к подобным схемам.

С начала всплеска хактивизма в 2022 году множество малоквалифицированных, но восприимчивых к идеологическому влиянию новичков было вовлечено в киберпреступную деятельность. Под руководством более опытных кураторов за несколько лет они приобрели практические навыки проведения атак. По мере снижения геополитической напряженности возрастает риск, что эти участники начнут проводить атаки с требованием выкупа ради получения прямой финансовой выгоды, в первую очередь — на российские организации, уже знакомые им по прежней активности.

В 2026 году ожидается рост шантажа с использованием утечек персональных данных. С 30 мая 2025 года в России значительно увеличены штрафы за нарушения в этой сфере — теперь они могут достигать миллионов рублей. Злоумышленники начнут оказывать давление на жертву, ссылаясь на возможные санкции. В первую очередь под удар попадает малый и средний бизнес: недостатки в системе защиты в сочетании с высокой чувствительностью к репутационным потерям могут повышать вероятность уступок вымогателям, стремящимся монетизировать новые регуляторные риски.

6

Кибершпионаж. Один из ключевых факторов эскалации кибершпионажа — экономическая и технологическая трансформация, вызванная санкциями и уходом иностранных компаний с российского рынка. В ответ Россия активно развивает высокотехнологичные сферы, включая искусственный интеллект, квантовые технологии, энергетику, медицину и биотехнологии. Эти разработки вызывают интерес у зарубежных государств, поскольку могут изменить расстановку сил в глобальной конкуренции.

Второй важный фактор — модернизация оборонно-промышленного комплекса (ОПК). Разработка новых вооружений, цифровизация и привлечение множества подрядчиков создают дополнительный объем чувствительной информации. В условиях кризиса и геополитической напряженности технологическое усиление России воспринимается как угроза, что стимулирует иностранную киберразведку. Дополнительным уязвимым звеном становятся подрядчики, подключаемые к проектам в сфере ОПК: их защита может оказаться недостаточной для противостояния высокоуровневым угрозам. Все это делает российские высокотехнологичные и оборонные предприятия приоритетными целями для кибершпионских кампаний.

В 2026 году активность и цели кибершпионов будут напрямую зависеть от геополитической ситуации. При ее обострении основное внимание будет сосредоточено на объектах, критически важных для национальной безопасности: ОПК, госучреждения, топливно-энергетический комплекс. При нормализации внешнеполитических отношений фокус кибершпионов сместится на научно-исследовательские организации, университеты, коммерческие компании с уникальными технологиями.

7

Хактивизм. Сложная геополитическая ситуация остается главным фактором эскалации хактивизма в России. Наибольший интерес для хактивистов представляют государственные сервисы, топливно-энергетический комплекс, транспортная инфраструктура, телекоммуникации, финансовый сектор. Нарушение деятельности организаций и вмешательство в их бизнес-процессы рассматриваются хактивистами прежде всего как инструмент стратегического давления на отрасли и государство в целом.

Однако с течением времени формы оказания этого давления меняются. Несмотря на то что организации в отдельных регионах и отраслях России продолжают регулярно сталкиваться с DDoS-атаками, они перестали быть основным методом в хактивистских кампаниях. На первый план вышли деструктивные атаки с использованием шифровальщиков и вайперов. Большинство хактивистов используют в атаках общедоступные инструменты и ВПО, распространяемое по модели *malware as a service*. Однако в арсенале некоторых группировок все чаще стали появляться собственные разработки, что ранее в атаках хактивистов отмечалось крайне редко.

Еще один фактор, который способствует росту хактивистской активности в России, — низкий порог входа в киберпреступную деятельность, в первую очередь в части DDoS-атак. Этому способствует широкая доступность инструментов для проведения атак в открытых источниках.

8

Отраслевой срез. Промышленность и госучреждения лидируют по количеству атак, и в 2026 году ситуация не изменится. Высокая интенсивность кибератак на эти отрасли сохранится даже в случае урегулирования острых геополитических вопросов. Доступ к информации госучреждений и промышленных предприятий по-прежнему будет рассматриваться как важный инструмент политического и экономического влияния. В ближайшие годы активная цифровизация, внедрение IoT и систем на базе ИИ, а также переход на решения российских разработчиков будут расширять поверхность атак на промышленность и госсектор, что может привести к еще большему количеству успешных кибератак на эти отрасли.

Российские IT- и телеком-компании остаются не только одними из самых частых мишеней, но и наиболее уязвимыми к последствиям атак. Для IT-компаний особой опасностью будут представлять атаки на цепочки поставок и доверительные отношения. В случае спада геополитической напряженности и восстановления международных деловых связей возникнут новые цепочки поставок и партнерства, в которых подрядчики могут стать «узловыми точками» с доступом к данным и системам сразу нескольких организаций. Важно отметить, что в случае затишья злоумышленники будут реже использовать этот доступ для немедленного разрушения IT-инфраструктуры. Вместо этого они смогут затаиться и готовить почву для будущих атак, закладывая бэкдоры на случай обострения ситуации.

В 2026 году интенсивность и характер атак на телеком также будут варьироваться в зависимости от геополитической обстановки. DDoS-атаки в 2026 году полностью не исчезнут: они останутся актуальным инструментом давления, но будут чаще использоваться с целью получения выкупа за их прекращение. При росте напряженности стоит ожидать как увеличения числа атак, так и их большей агрессивности. Прежде всего под удар будут попадать региональные провайдеры, не обладающие достаточными ресурсами для эффективной защиты.

9

Основные проблемы кибербезопасности российских компаний и что можно сделать уже сегодня. Многолетняя практика проведения тестов на проникновение показывает, что типичные проблемы — слабые парольные политики, отсутствие многофакторной аутентификации, небезопасное хранение данных, использование устаревшего ПО с известными уязвимостями, ошибки в разграничении доступа и недостаточная подготовка сотрудников к распознаванию атак методами социальной инженерии — останутся актуальными для большинства компаний и в 2026 году.

Уже сегодня базовые уязвимости можно выявить при помощи сканеров в составе VM-решений и автопентестов. Это поможет снизить риски массовых атак со стороны киберпреступников, выбирающих наименее защищенные цели. Формат подписки делает такие инструменты доступными для компаний с любым бюджетом.

Роль крупных игроков на рынке сервисов по анализу защищенности будет постепенно смещаться в сторону комплексных проектов. По мере того как базовые проблемы безопасности в инфраструктуре все чаще будут выявляться с помощью автоматизированных инструментов, задачи экспертных команд выйдут за рамки стандартных тестов на проникновение. Они будут сосредоточены на проверке реализуемости недопустимых событий, проведении киберучений и оценке эффективности MDR-сервисов.

Для организаций со зрелыми процессами ИБ ежегодный внешний red teaming должен оставаться обязательной практикой, даже если инфраструктура компании проходит кибериспытания на платформах багбаунти.

Автоматизированные средства поиска уязвимостей не обеспечивают всестороннюю оценку защищенности приложений, поэтому перед их запуском или размещением на платформе багбаунти необходимо проводить ручное экспертное тестирование. Это особенно актуально в условиях растущего использования ИИ-ассистентов, которые ускоряют разработку, но повышают риск ошибок в бизнес-логике и появления недекларированных возможностей.

ОСНОВНЫЕ ЦИФРЫ

- С июля 2024-го по сентябрь 2025 года на Россию пришлось **14–16% всех успешных кибератак в мире**. Учитывая ожидаемый рост активности злоумышленников во втором полугодии, мы прогнозируем, что по итогам 2025 года общее количество успешных кибератак превысит показатель прошлого года на 20–45%. **В 2026 году их количество может вырасти еще на 30–35%** по сравнению с 2025 годом.
- Основными методами кибератак на организации в России остаются **использование вредоносного ПО и социальная инженерия**. По сравнению с 2023 годом и первой половиной 2024-го доля успешных атак с применением ВПО выросла с **56% до 71%**, а доля атак с использованием социальной инженерии — с **49% до 60%**.
- Промышленные предприятия стали основной целью киберпреступников**. На промышленность пришлось 17% всех успешных кибератак на организации, что на 6 п. п. больше, чем в 2023 году и первой половине 2024-го. Доля успешных атак на государственный сектор составила 11%. На третьем и четвертом месте — ИТ-компании (9%) и телекоммуникации (7%).
- Финансово мотивированные группировки являются самой активной категорией злоумышленников в России**. Во втором полугодии 2024-го и первых трех кварталах 2025 года они совершили **33% всех успешных кибератак**, при этом было зафиксировано **не менее 28 группировок** с финансовой мотивацией. Чаще всего их жертвами становились промышленные предприятия (16%), организации торговли (10%) и финансовые организации (9%). При этом 28% успешных атак были совершены без привязки к отрасли.
- С июля 2024-го по сентябрь 2025 года на организации в России совершали атаки **не менее 22 кибершпионских групп**. На их долю пришлось **22% всех успешных кибератак**. Чаще всего жертвами становились промышленные предприятия (21%), государственные учреждения (16%) и организации оборонного комплекса (13%).

-  Во второй половине 2024-го и в первых трех кварталах 2025-го российские организации стали объектами атак как **минимум 18 хактивистских группировок**, на долю которых пришлось **19% всех успешных кибератак**. Лидируют по количеству успешных атак со стороны хактивистов промышленность (15%), госучреждения (13%) и телекоммуникации (13%) — отрасли стратегического значения. В то же время доля успешных хактивистских кибератак на телеком сократилась вдвое по сравнению с 2023 годом и первой половиной 2024-го.
-  Наиболее распространенными последствиями кибератак на организации в России остаются **утечки конфиденциальных данных и сбои в работе компаний**. По сравнению с 2023 годом и первой половиной 2024-го доля успешных атак с утечкой информации увеличилась **с 44% до 56%**, а доля успешных атак, приводивших к нарушению деятельности компаний, увеличилась **с 37% до 40%**. Чаще всего похищались служебные документы, содержащие коммерческую тайну (30%), учетные записи (24%), а также персональные данные клиентов и сотрудников (17%).
-  На темных площадках более половины (55%) публикаций об утечках связаны **с бесплатной раздачей** украденных данных. Еще 27% объявлений нацелены на их продажу, при этом в большинстве случаев (81%) цена **не превышает 1 тыс. долларов**.
-  Половина объявлений о продаже или раздаче данных связана с утечками небольшого размера — до 100 тыс. записей. Однако на темных площадках встречаются и **крупные утечки**: каждое восьмое (12%) объявление содержало базы **объемом свыше 5 млн записей**. В 6% случаев предлагались архивы размером **более 100 ГБ**.
-  Специалисты PT SWARM при проведении внешних тестов на проникновение смогли получить доступ к корпоративной сети в **89% проектов**, а в рамках внутренних пентестов — добиться **максимальных привилегий в домене в 100% случаев**. Удалось реализовать **79% обозначенных недопустимых событий** с минимальным временем достижения цели — **4 часа после получения контроля над доменом**. Ключевые проблемы, выявленные в инфраструктурах компаний, включают раскрытие конфиденциальных данных в открытых источниках, использование слабых и словарных паролей, применение устаревшего ПО с известными уязвимостями, небезопасную настройку веб-приложений и сервисов.

ВВЕДЕНИЕ

Киберпространство на протяжении долгого времени формируется под воздействием множества факторов — технологических, правовых, экономических, социально-культурных и других. Среди них в последние годы для России особое значение приобрели геополитические процессы, которые напрямую влияют на характер киберугроз.

В условиях растущей напряженности киберпространство все чаще напоминает шахматную доску: здесь важны не только тактические ходы, но и стратегическое планирование на несколько шагов вперед. Каждая атака становится проверкой прочности систем, а допущенные ошибки или неустраненные уязвимости способны привести к тяжелым последствиям. В отличие от классической шахматной партии эта «игра» не имеет финала: противостояние между киберпреступниками и защитниками продолжается непрерывно, требуя постоянного обновления подходов и ресурсов.

В течение последних лет наблюдается тенденция к снижению доли атак со стороны отдельных лиц. Вместо них все чаще на первый план выходят устойчивые киберпреступные группировки, обладающие собственной инфраструктурой, финансированием и системой распределения ролей. Такие структуры действуют в рамках долгосрочной стратегии, преследуя конкретные цели: от прямой финансовой выгоды и промышленного шпионажа до дестабилизации политической обстановки.

Кроме того, десятки группировок перешли от массовых атак без отраслевой направленности к крупномасштабным кампаниям, демонстрируя высокий уровень скоординированности и технологической подготовки, ранее не свойственный подобным структурам. Именно поэтому сегодня российским организациям следует воспринимать кибератаки не как гипотетическую угрозу, а как практически неизбежную реальность. Вопрос уже не в том, столкнется ли компания с кибератакой, а в том, насколько она будет к ней готова.

При таких условиях критически важно умение ориентироваться в динамично меняющемся ландшафте киберугроз. Только четкое понимание потенциальных рисков позволяет выстраивать эффективные превентивные меры, грамотно расставлять приоритеты при формировании стратегий кибербезопасности и обеспечивать своевременное реагирование на инциденты.

Это исследование призвано стать важным ресурсом для руководителей в сфере информационной безопасности (CISO), IT-директоров (CIO), а также для других лидеров компаний в России, заинтересованных в надежной защите своих организаций от киберугроз.

В отчете вы найдете ответы на ключевые вопросы:

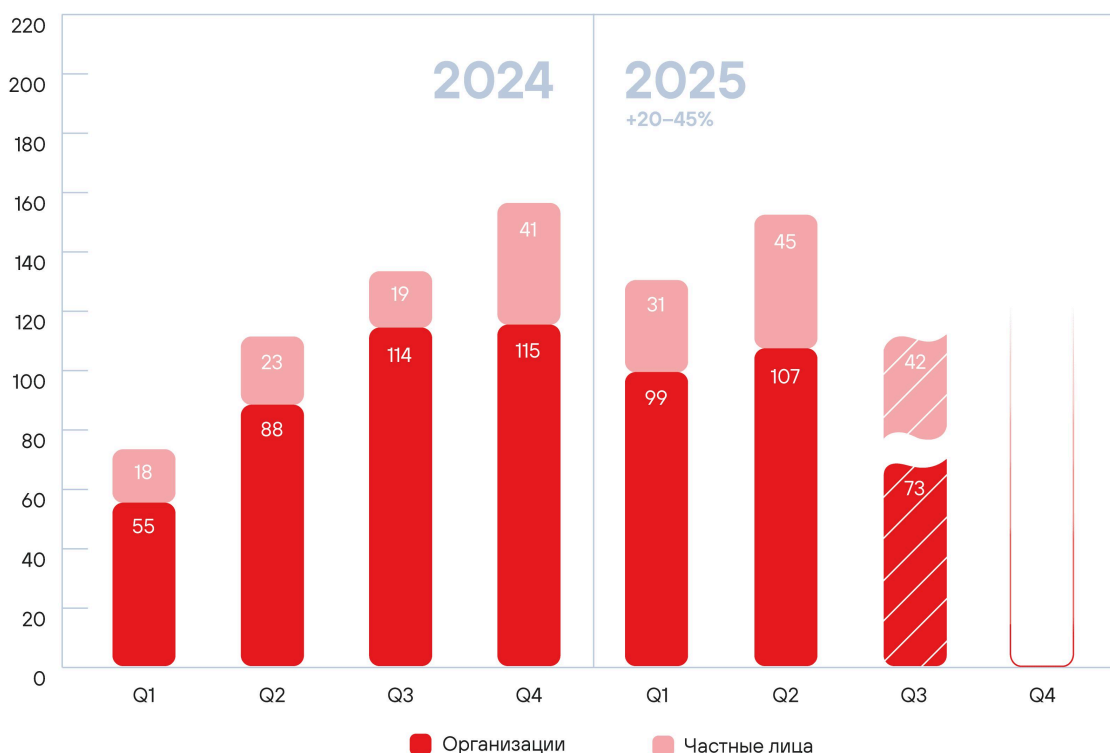
- каковы цели злоумышленников, атакующих организации в России;
- какие факторы стимулируют рост числа атак и определяют их интенсивность;
- какие компании находятся в зоне повышенного риска;
- какие методы и инструменты используют киберпреступники в атаках на российские организации;
- какие меры необходимо предпринять уже сегодня, чтобы снизить риски и предотвратить недопустимые для компании последствия.

Ходы по темным клеткам: особенности кибератак на Россию



Россия на протяжении многих лет остается одной из наиболее приоритетных целей для киберпреступников. По нашим данным, в период с июля 2024-го по сентябрь 2025 года на долю России приходилось от 14% до 16% всех успешных кибератак в мире и 72% атак, зафиксированных в СНГ. Для сравнения: на втором и третьем местах по количеству кибератак в регионе находятся Белоруссия (9%) и Казахстан (7%).

Рисунок 2. Динамика успешных кибератак на организации и частных лиц в России



Из года в год во втором полугодии фиксируется больше атак, чем в первом. В этот период у компаний наблюдается пик деловой активности: завершаются проекты, заключаются крупные сделки, распределяются бюджеты на следующий год и формируется отчетность. Все это повышает интерес злоумышленников, нацеленных на кражу данных или шантаж. Осенью и зимой также усиливается фишинговая активность, связанная с налоговыми уведомлениями, праздничными продажами и сезонными акциями.

Дополнительный рост числа атак обусловлен политико-экономическими факторами — обсуждением и утверждением бюджетов, выборами, подведением итогов социально-экономического развития. Кроме того, во многих компаниях именно к концу года накапливаются отложенные обновления, а высокая нагрузка на IT-службы снижает их способность оперативно реагировать на угрозы.

КЛЮЧЕВЫЕ ДРАЙВЕРЫ КИБЕРАТАК В РОССИИ

В мировой картине киберугроз Россия занимает особое место из-за совокупности факторов. Ключевым из них является роль страны **на мировой политической арене**. Россия формирует альянсы, участвует в международных инициативах и нередко занимает самостоятельную позицию по важнейшим глобальным вопросам. Это делает ее приоритетной целью как для небольших кибергруппировок, так и для иностранных разведывательных структур и аффилированных с ними АРТ-групп, стремящихся получить доступ к информации о планах и решениях, чтобы предугадать или скорректировать действия страны.

Дополнительный интерес вызывает участие России в международных объединениях, таких как БРИКС и ШОС, где вырабатываются новые форматы сотрудничества. Данные о переговорах, позициях российских представителей и будущих инициативах обладают высокой ценностью для конкурентов, стремящихся повлиять на баланс сил.

Значимым фактором, формирующим ландшафт киберугроз, является **продолжительная геополитическая напряженность**. На ее фоне сохраняется высокая активность хактивистов, которые применяют деструктивные кибератаки как инструмент политического и идеологического давления. Их действия направлены не только на подрыв доверия к государственным институтам, но и на дестабилизацию экономики, провокацию социальной напряженности и формирование атмосферы неопределенности в обществе. Особенно опасны атаки, направленные на государственные органы, промышленность, транспортную инфраструктуру, телекоммуникации и средства массовой информации, поскольку они способны привести к недопустимым событиям, оказать каскадное воздействие на национальную безопасность, экономику и повседневную жизнь общества.

Существенным фактором выступает **стремительная цифровизация**. Процесс цифровизации в России получил системную основу вместе с запуском национального проекта «Цифровая экономика», реализованного в 2019–2024 годах. Его целью было создание условий для развития цифровых технологий и их применения в экономике, социальной сфере и государственном управлении. С 1 января 2025 года на смену «Цифровой экономике» пришел новый национальный проект «Экономика данных и цифровая трансформация государства». Он продолжает и расширяет начатые инициативы, делая акцент на внедрении цифровых решений, повышении доступности онлайн-госуслуг, развитии интернета в удаленных регионах, поддержке российских разработчиков и защите от киберугроз.

Массовое внедрение онлайн-сервисов, электронных госуслуг, финтеха и электронной коммерции заметно расширяет поверхность атак. Во-первых, растет количество уязвимых точек входа. Во-вторых, увеличивается объем обрабатываемых и хранящихся данных: персональные данные, финансовые транзакции, государственные реестры становятся ценными целями для киберпреступников. Дополнительную угрозу несет ускоренное внедрение инновационных технологий без должного уровня зрелости кибербезопасности. Когда организации стремятся как можно быстрее вывести новые продукты на рынок, вопросы защиты информации и устойчивости инфраструктуры иногда отходят на второй план. В условиях политических и экономических сложностей, а также внешнего давления это создает благоприятную среду для атак с минимальными рисками для злоумышленников.

Не менее важным фактором, влияющим на ландшафт киберугроз, является стратегическая **роль России как энергетической державы**. Нефть, природный газ и уголь экспортируются в десятки стран и служат инструментом влияния на мировой рынок. В последнее время все большее значение приобретает и атомная энергетика: Россия выводит на внешние рынки проекты АЭС и развивает эту сферу как одно из ключевых направлений энергетического присутствия. В 2025 году были подписаны соглашения о строительстве АЭС в Иране и Эфиопии, ведется подготовка проектов в Узбекистане и Казахстане, продолжается строительство флагманской АЭС «Аккую» в Турции.

Контроль над промышленным сектором и понимание его будущих направлений развития представляют особую ценность для государств-конкурентов. Поэтому киберпреступники активно атакуют промышленные и производственные предприятия, стремясь получить данные о контрактах, инфраструктуре и технологических процессах. Промышленность остается самой атакуемой отраслью в России: на ее долю приходится 17% всех успешных кибератак, направленных на российские организации.

Помимо энергетики и промышленности, Россия активно развивает высокотехнологичные отрасли — оборонно-промышленный комплекс, ядерные технологии, космос и IT. Эти сферы традиционно находятся под прицелом иностранных государств, поскольку доступ к наработкам и разведывательная информация могут обеспечить серьезное стратегическое преимущество.

Таким образом, геополитическая роль России, ее ресурсы и технологический потенциал делают страну крайне привлекательной целью для киберпреступников. Причем атаки направлены не только на госструктуры, но и на крупный бизнес и его подрядчиков, что создает сложную и многоуровневую картину угроз.

МЕТОДЫ КИБЕРАТАК

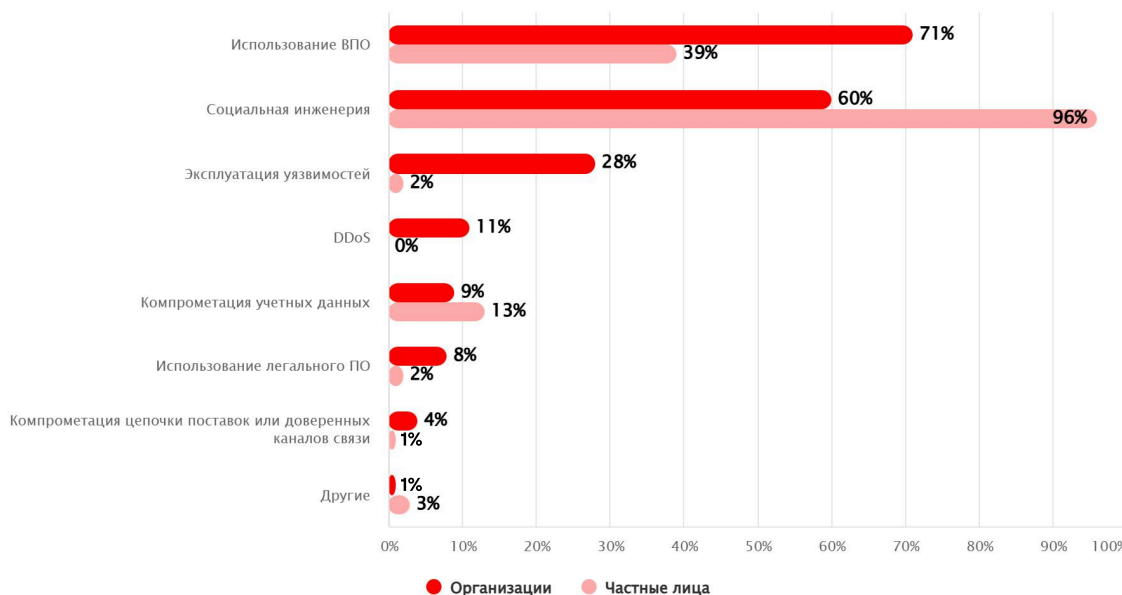
Основными методами кибератак в России, как и во всем мире, по-прежнему остаются использование вредоносного ПО и социальная инженерия. По сравнению с 2023 годом и первой половиной 2024-го их распространенность заметно возросла: доля успешных атак на организации с применением ВПО увеличилась с 56% до 71%, а доля атак с использованием социальной инженерии — с 49% до 60%. Такой рост объясняется активной деятельностью финансово мотивированных и кибершпионских группировок, кампании которых, как правило, начинаются с фишинговых рассылок с целью заражения систем жертв вредоносным ПО и дальнейшего развития атаки.

Иногда злоумышленники маскируются под представителей компаний из той же или смежной отрасли, чтобы вызвать доверие у потенциальной жертвы, и только после вступления с ней в диалог отправляют вредоносные вложения. Для таких атак они регистрируют фишинговые домены, максимально похожие на адреса реально существующих организаций, за которые себя выдают. Ниже перечислены два случая из практики экспертов PT ESC.

Летом 2024 года специалисты PT ESC обнаружили нетипичную схему атаки. Злоумышленники вступали в переписку с жертвой, представляясь потенциальным заказчиком, и таким образом снижали уровень ее бдительности. После получения ответа они отправляли архив с вредоносным содержанием — якобы с техническим заданием. Киберпреступники представились компанией «Промышленная автоматизация» и использовали домен promautomatic.ru, который отличался от реального всего одной буквой и был зарегистрирован незадолго до атаки.

В конце октября 2024 года группа киберразведки PT ESC обнаружила еще одну фишинговую кампанию, в которой атакующие сначала пытались завоевать доверие и лишь затем переходили к доставке полезной нагрузки. Письмо было отправлено якобы от имени управления ФСТЭК по СЗФО. Использовался домен fstec.info, не связанный с официальными ресурсами ФСТЭК и зарегистрированный 16 октября 2024 года. Во вложении был скан документа низкого качества, непригодный для полноценного визуального ознакомления. По предположению наших экспертов, это мог быть этап многоступенчатой социальной инженерии: сначала жертве отправляли неопасное, но трудночитаемое вложение, чтобы спровоцировать ответ и вовлечь в переписку, а вредоносный файл отправляли уже после установления доверия.

Рисунок 3. Методы атак на российские организации и частных лиц (доля успешных атак)

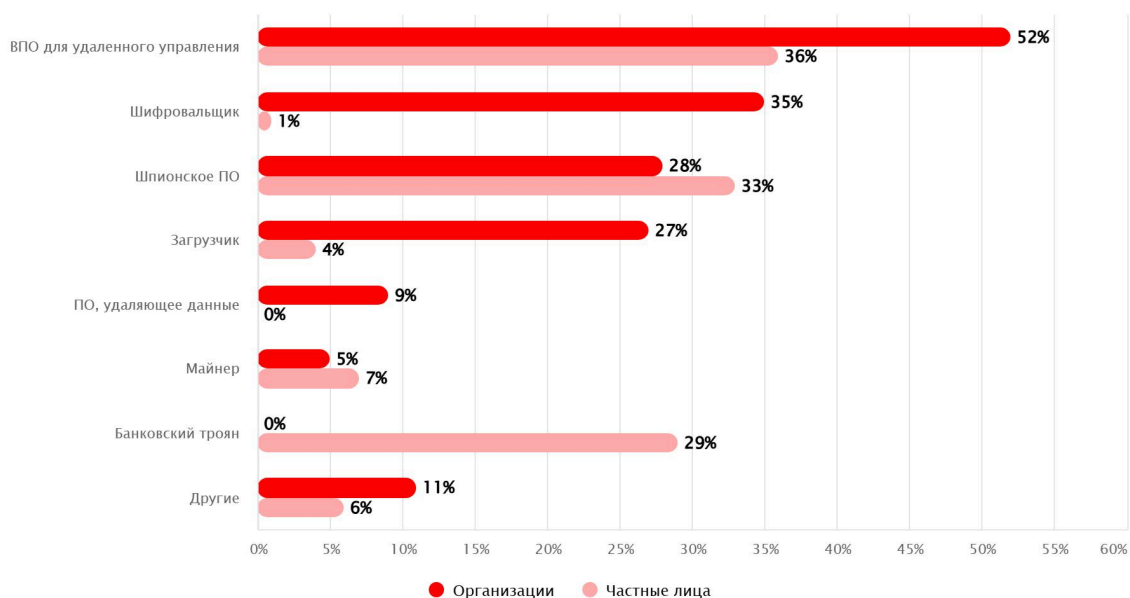


Наиболее часто (в 52% случаев заражений вредоносным ПО) использовались трояны для удаленного управления (RAT). Они есть в арсенале практически всех киберпреступных группировок. Некоторые специализированные RAT могут выполнять дополнительные задачи — извлекать пароли из браузеров, записывать нажатия клавиш, загружать дополнительные модули и т. д. Пример такого многофункционального трояна — STRRAT, использовавшийся группировкой Bloody Wolf.

Кроме того, ряд группировок для управления скомпрометированными узлами использует легитимные средства. Такие программы обычно не классифицируются антивирусными средствами защиты как вредоносные, и злоумышленники могут применять их для управления скомпрометированными системами, избегая использования легко детектируемых RAT. Уже долгое время самым популярным инструментом в этой категории остается AnyDesk. Это подтверждают результаты расследований инцидентов, проведенных командой PT ESC Incident Response. Например, AnyDesk фиксировался в кампаниях Rare Werewolf, Crypt Ghouls, Blackjack, Werewolves и других группировок, атаковавших организации в России в течение последнего года. Среди аналогов AnyDesk, часто используемых злоумышленниками в атаках на российские компании, также отмечаются UltraVNC, TightVNC, Radmin и NetSupport.

Значительно (с 25% до 35%) выросла доля успешных атак на организации с использованием шифровальщиков. Прежде всего это связано с учащением их использования хактивистскими группировками. Наиболее часто используются шифровальщики LockBit Black (3.0), Babuk и Conti, которые оказались в свободном доступе в 2021–2022 годах и с тех пор применяются в вымогательских кампаниях различными группировками.

Рисунок 4. Типы вредоносного ПО
(доля успешных атак с использованием ВПО)



© Positive Technologies

Во второй половине 2024 года и в течение 2025-го доля DDoS-атак на российские организации оставалась на уровне 11%. Невысокая доля DDoS-атак на российские организации обусловлена рядом причин:

- публикация украденных данных вызывает большой общественный резонанс, чем временная недоступность сайта вследствие DDoS-атаки;
- атаки, направленные на компрометацию данных, их шифрование или уничтожение, приводят к более серьезным последствиям (вывод из строя критически важных систем, нарушение бизнес-процессов, ущерб репутации) и позволяют получить выгоду через вымогательство или продажу украденной информации;
- за последние годы российские компании, столкнувшиеся с интенсивными DDoS-атаками, усилили защиту, что снизило их эффективность и привлекательность для киберпреступников.

Киберпреступники все чаще проникают в крупные организации через подрядчиков — доверенные VPN-каналы и скомпрометированные служебные учетные данные. Такая стратегия основана на том, что подрядчики зачастую имеют доступ к инфраструктуре и части данных своих клиентов, но уровень их киберзащиты нередко ниже, чем у крупных организаций. Компрометация даже одного поставщика открывает злоумышленникам путь к атакам сразу на несколько компаний.

Если в 2023 году и первой половине 2024-го доля атак через цепочку поставок и доверенные каналы связи в российском ландшафте киберугроз составляла лишь 2%, то сегодня этот показатель вырос до 4%. Хотя показатель остается сравнительно небольшим, подобные инциденты особенно опасны, поскольку IT-подрядчики обычно обслуживают десятки клиентов одновременно, предоставляя программные решения и техническую поддержку.

Показательный случай произошел в сентябре 2025 года. По данным СМИ, жертвой атаки стала американская компания Collins Aerospace — поставщик системы регистрации пассажиров, багажа и выполнения операционных процессов MUSE. Эта единая платформа позволяла авиакомпаниям снижать издержки и гибко управлять пассажиропотоками за счет совместного использования стоек регистрации и выходов. Взлом одной системы обернулся масштабными последствиями сразу для нескольких европейских аэропортов и авиакомпаний, часть операций пришлось выполнять вручную.

В России к атакам через подрядчиков чаще всего прибегают хактивистские и кибершпионские группировки, такие как Blackjack, Crypt Ghouls, Silent Crow, Hellhounds, ExCobalt и IAmTheKing. Для хактивистов основная цель заключается в максимизации деструктивного эффекта от кибератаки. Компрометация подрядчика позволяет им парализовать работу сразу нескольких компаний или даже целой отрасли. Например, если под удар попадает IT-компания, предоставляющая сервисы для государственных порталов или банков, это может привести к массовым сбоям в привычных цифровых услугах и сформировать недоверие к ним.

Для кибершпионских группировок атаки через подрядчиков представляют интерес как скрытый канал разведки и получения данных. Подрядчики нередко имеют прямой доступ к инфраструктуре и внутренней информации десятков клиентов, что делает их удобным узлом для сбора разведанных. Кроме того, доступ через доверенные каналы выглядит легитимным, что позволяет злоумышленникам оставаться незамеченными месяцами и даже годами и перехватывать переписку, документы и планы сразу нескольких организаций без необходимости взламывать каждую из них отдельно. В зоне повышенного риска находятся подрядчики, работающие с государственными структурами и объектами критической инфраструктуры — энергетикой, транспортом, телекомом.

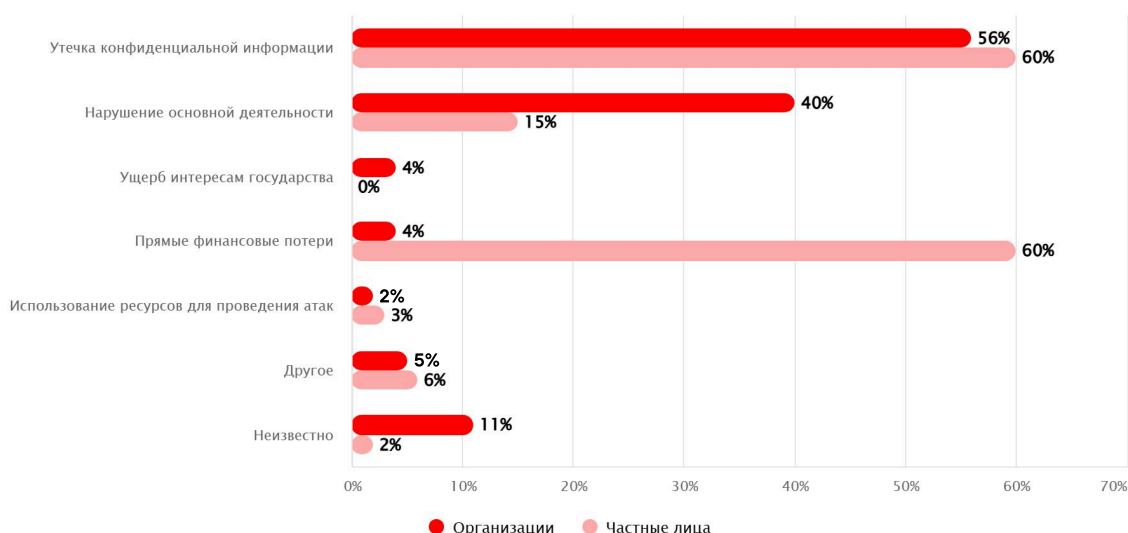


ПОСЛЕДСТВИЯ КИБЕРАТАК

Наиболее распространенные последствия кибератак на организации в России — это утечка конфиденциальной информации и нарушение основной деятельности компаний. Эти два последствия часто взаимосвязаны. Например, злоумышленники могут сначала получить доступ к внутренним системам компании и незаметно извлечь ценные данные, после чего запустить шифровальщик, который парализует ключевые бизнес-процессы — от документооборота до работы сервисов, производственных систем и клиентских платформ.

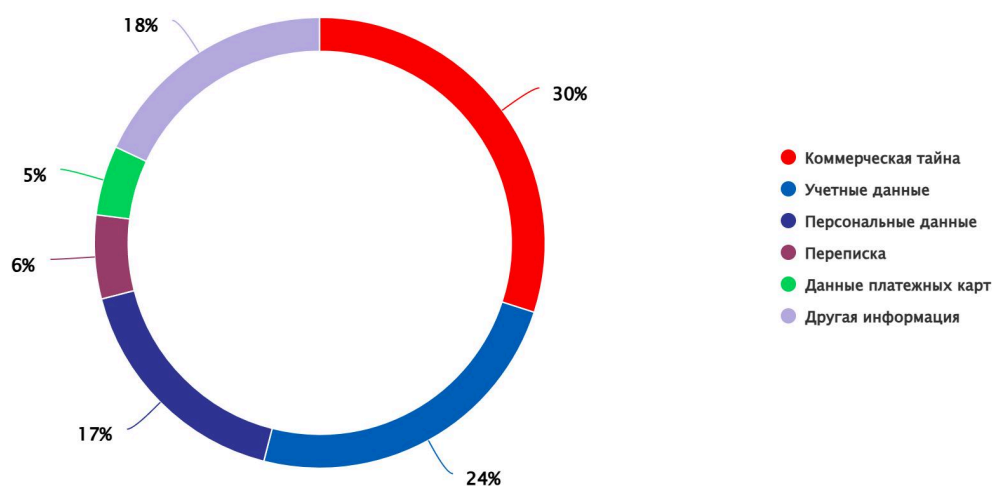
Подобная тактика позволяет киберпреступникам добиться двойного эффекта: шантажировать организацию угрозой публикации или продажи украденных данных (так называемый double extortion) и одновременно требовать выкуп за восстановление доступа к системам. Подобные инциденты приводят не только к финансовым потерям, но и существенно подрывают доверие со стороны партнеров и клиентов. В условиях ужесточающегося регулирования в области защиты персональных данных такие утечки становятся особенно опасными, поскольку влекут за собой крупные штрафы и серьезные репутационные риски.

Рисунок 5. Последствия атак (доля успешных атак)



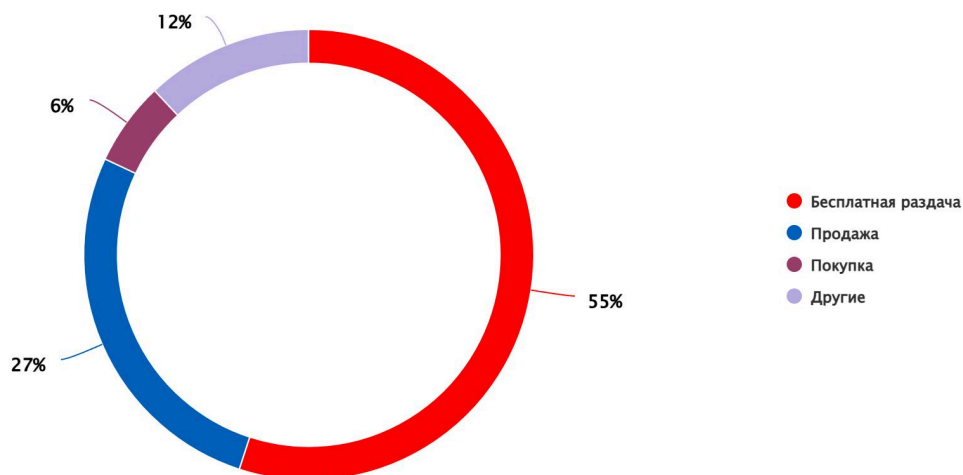
По сравнению с 2023 годом и первой половиной 2024-го доля атак на организации, закончившихся утечкой данных, выросла с 44% до 56%. Наиболее часто из организаций похищалась информация, относящаяся к коммерческой тайне (30%), учетные записи (24%), а также персональные данные клиентов и сотрудников (17%).

Рисунок 6. Типы украденных данных в успешных атаках на организации



Похищенные из организаций данные редко остаются исключительно в распоряжении злоумышленников. Чаще всего они становятся инструментом получения выгоды или давления на жертву. Наиболее распространенный сценарий — продажа данных на специализированных форумах и маркетплейсах дарквеба.

Рисунок 7. Типы объявлений, связанных с утечками данных, на теневых форумах



Каждое четвертое (27%) объявление связано именно с продажей украденных данных: баз данных клиентов, сканов документов, корпоративных учетных записей, коммерческой переписки, чертежей и технологической документации. В 81% таких объявлений стоимость данных не превышает 1 тыс. долларов. Чем ценнее и уникальнее информация, тем выше ее цена. Так, средняя стоимость простой базы с Ф. И. О., адресами электронной почты и телефонами составляет около 120 долларов. Более полные наборы с паспортными данными и ИНН оцениваются в среднем в 500–600 долларов, а при наличии фотографий или сканов паспортов цена может достигать нескольких тысяч долларов. Доступ к корпоративным системам или уникальные коммерческие сведения оцениваются значительно выше — в десятки и даже сотни тысяч долларов.

Рисунок 8. Диапазон цен в объявлениях о продаже данных на теневом рынке

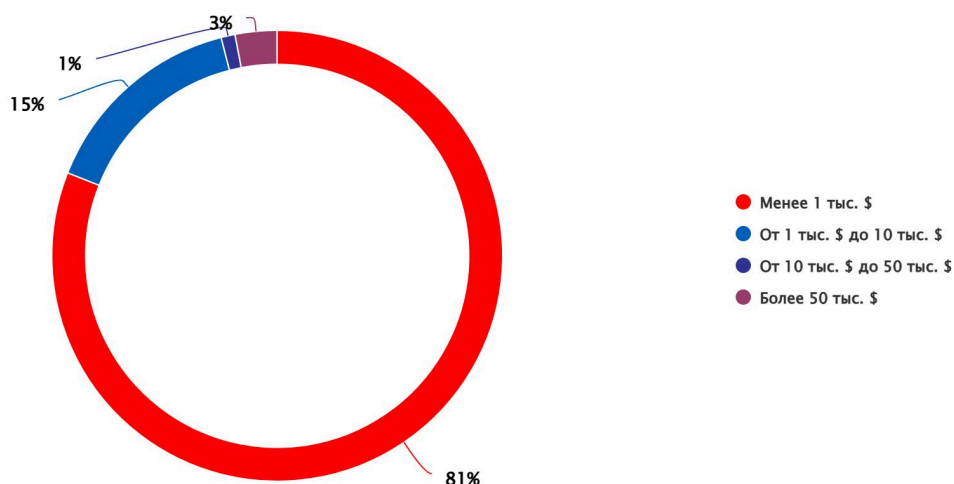


Рисунок 9. Объявление о продаже сканов паспортов

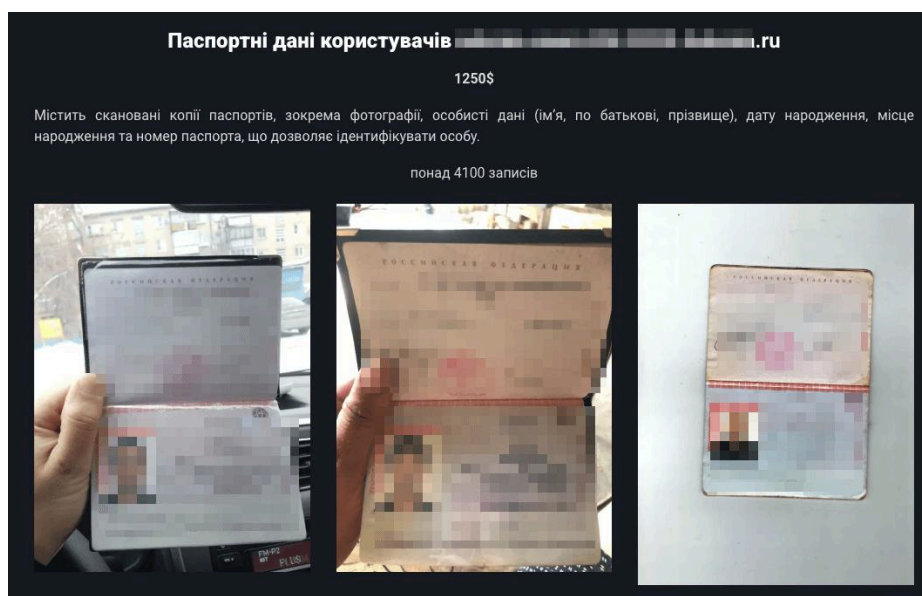
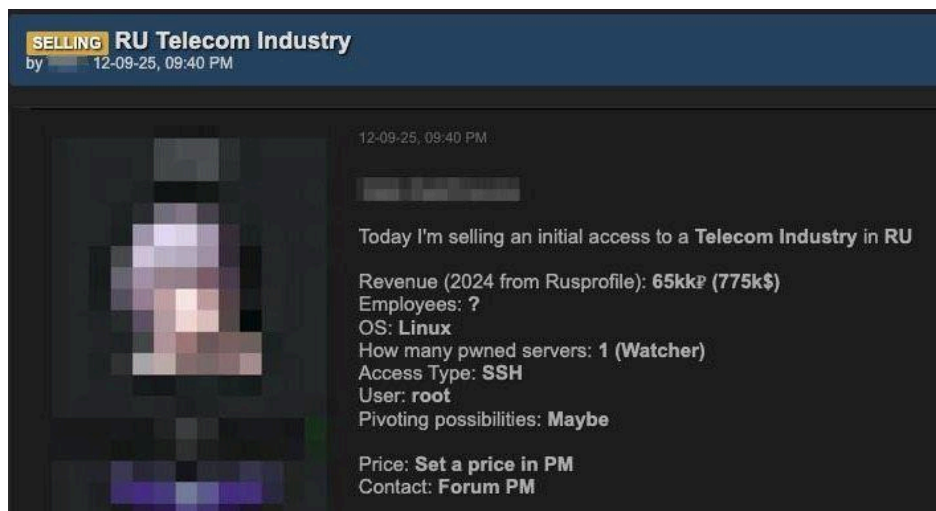


Рисунок 10. Объявление о продаже SSH-доступа к телеком-компании



Тем не менее не все похищенные массивы информации попадают в продажу. В 55% случаев данные выкладываются в открытый доступ. Причины у этого разные:

- хактивисты могут публиковать данные не ради прибыли, а с целью нанести ущерб конкретной организации, государству или подчеркнуть свои геополитические мотивы;
- бесплатная публикация нередко используется как элемент вымогательства: злоумышленники выкладывают часть базы, демонстрируя серьезность угрозы, и обещают опубликовать оставшиеся данные в случае отказа от выплаты;
- в ситуации, когда требование о выкупе было отклонено, злоумышленники могут выложить похищенные материалы в открытый доступ, чтобы усилить негативные последствия для скомпрометированной организации;
- публикация служит способом саморекламы, а также инструментом продвижения более ценных лотов, предлагаемых уже за деньги.

Важно, что бесплатное распространение может наносить не меньший урон, чем продажа: попавшие в открытый доступ базы моментально начинают копироваться и распространяться по множеству площадок, и контролировать их дальнейшее использование уже невозможно.

Половина (50%) объявлений о продаже или бесплатной раздаче данных связана с относительно небольшими объемами — до 100 тыс. записей. Однако на теневых площадках встречаются и крупные утечки: 12% объявлений содержало базы объемом свыше 5 млн записей. В 6% случаев предлагались архивы размером более 100 ГБ. Наличие столь крупных архивов говорит о высоком уровне подготовки злоумышленников, способных не только проникнуть в защищенные системы, но и извлечь, структурировать и подготовить к продаже или публикации огромные объемы информации. Кроме того, крупные утечки могут использоваться не только для прямой монетизации, но и как инструмент давления, шантажа или информационно-психологического воздействия. Масштаб подобных инцидентов значительно повышает риски для всех вовлеченных сторон: от клиентов и партнеров пострадавшей организации до целых отраслей.

Рисунок 11. Распределение объявлений по количеству строк в базах данных

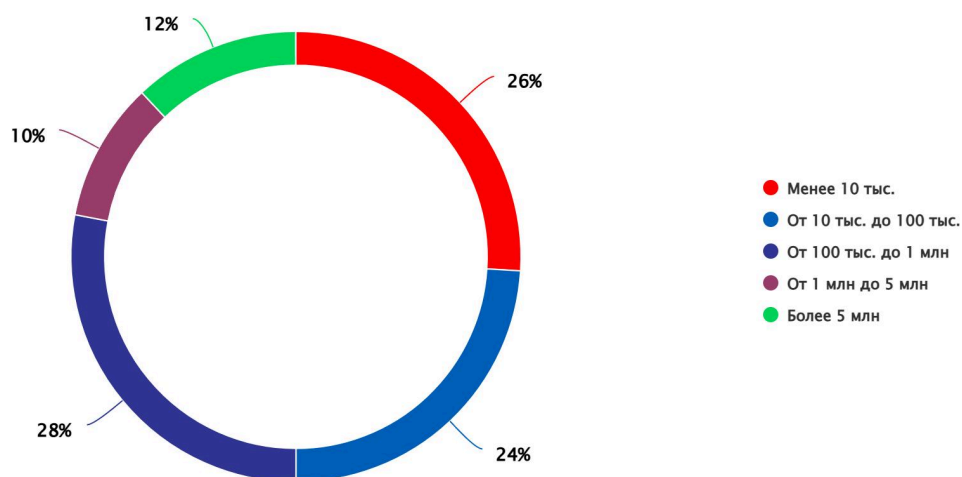
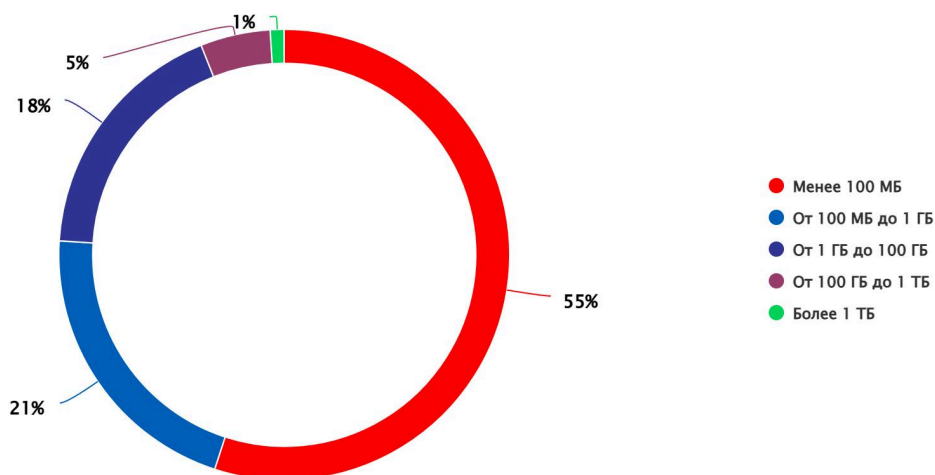


Рисунок 12. Распределение объявлений по размеру архивов и баз данных



Помимо утечек данных, одним из наиболее серьезных последствий кибератак для российских компаний стало нарушение их основной деятельности. Оно отмечалось в 40% успешных кибератак на российские организации. Нарушение основной деятельности может выражаться в остановке производственных линий, недоступности веб-сайтов и критически важных сервисов, срыве логистических и финансовых операций. Для государственных структур такие инциденты оборачиваются перебоями в оказании социальных услуг, а для бизнеса — убытками, снижением конкурентоспособности и даже риском полной остановки деятельности.

Рост цифровизации сделал государственные и коммерческие IT-системы гораздо более взаимосвязанными. Экономика и управление теперь напрямую зависят от онлайн-сервисов, тогда как раньше цифровые решения выполняли лишь вспомогательную роль и их сбой редко влиял на ключевые процессы. Сегодня же государственные услуги, банковские транзакции, логистика, энергетика и медицина во многом опираются на цифровую инфраструктуру.

В таких условиях любая атака или технический сбой способен запустить каскадную реакцию. Так, нарушение работы энергосистемы может привести к отключениям, затрагивающим промышленность, транспорт и сферу ЖКХ. Утечки баз данных несут не только финансовые потери, но и разрушают доверие к государственным и коммерческим цифровым сервисам, подрывая саму идею цифровой трансформации.

Иными словами, последствия кибератак сегодня стали гораздо более глубокими, поскольку цифровые технологии перестали быть «надстройкой» и превратились в основу повседневной жизни и государственного управления. Теперь удар по IT-инфраструктуре способен сказаться не только на отдельных компаниях или ведомствах, но и на социальной стабильности, экономике и уровне доверия в обществе.

Выводы и прогнозы



Темпы цифровизации и геополитическая обстановка — ключевые факторы, которые окажут влияние на российский ландшафт киберугроз в 2026 году. Чем быстрее в России происходит цифровая трансформация, тем больше цифровых систем и сервисов внедряется в бизнес-процессы и тем шире становится поверхность атак. При этом защита далеко не всегда развивается с той же скоростью, что и технологии, особенно в условиях дефицита квалифицированных кадров и зрелых решений. Внедрение новых технологий (ИИ, интернета вещей, цифровых двойников, автоматизации производства и управления) будут создавать новые классы уязвимостей, которые часто не замечаются на ранних этапах внедрения.

Дополнительным фактором риска становится курс на импортозамещение. Если в организации переход на отечественное ПО и оборудование происходит в сжатые сроки, без должного внимания к анализу защищенности, создается благоприятная среда для злоумышленников — незрелые системы легче атаковать, особенно в условиях уязвимостей нулевого дня или утечек исходного кода.

Параллельно с технологическими рисками на ландшафт киберугроз в 2026 году будет напрямую влиять геополитическая обстановка. При снижении напряженности активность хактивистов будет уменьшаться, а вектор сместится в сторону традиционной киберпреступности: вымогательства, кражи данных, атак на бизнес с целью прямой финансовой выгоды. Кроме того, в таких условиях возрастает вероятность международного сотрудничества в сфере кибербезопасности: обмена информацией об угрозах, совместного расследования инцидентов и разработки единых стандартов защиты.

В случае обострения геополитической ситуации хактивизм получит новый импульс к развитию, возрастет риск целенаправленных атак на критическую инфраструктуру, киберпреступники продолжат совершенствовать техники атак. Они чаще будут сопровождаться деструктивными действиями, направленными на дестабилизацию экономики.



Социальная инженерия и вредоносное ПО останутся превалирующими методами кибератак, однако будут эволюционировать. Из года в год мы наблюдаем, что основными методами атак на российские организации остаются социальная инженерия и использование вредоносного ПО. В 2026 году эти методы по-прежнему будут доминировать, однако их характер и уровень сложности может заметно измениться.

Уже сегодня мы фиксируем сложные многоступенчатые фишинговые кампании, нацеленные на усыпление бдительности жертв. Но в 2026 году социальная инженерия может стать еще более сложной: злоумышленники все чаще будут использовать искусственный интеллект для создания персонализированных фишинговых сообщений, генерации правдоподобных голосовых звонков и видеодипфейков, имитирующих реальных сотрудников или руководителей. Это повысит эффективность психологического давления на потенциальных жертв и усложнит выявление атак.

Что касается вредоносного ПО, то основное внимание будет уделяться многофункциональным троянам, которые способны сочетать шпионские и деструктивные функции. При этом акцент сместится на «тихие» атаки, в которых присутствие атакующих длительное время остается скрытым, пока они ведут систематический сбор данных и подготовку к целенаправленным ударам. Чтобы оставаться незамеченными, для разведки в инфраструктуре злоумышленники продолжают использовать легитимные средства, команды ОС, системные утилиты и инструменты из категории living off the land.



Ключевые последствия кибератак в 2026 году: компрометация данных и сбои в бизнесе. Наиболее частыми последствиями кибератак на российские организации остаются утечка конфиденциальной информации и нарушение основной деятельности компаний. Однако в 2026 году эти последствия все чаще будут носить комбинированный характер: злоумышленники не только шифруют данные, нарушая бизнес-процессы, но и похищают их для вымогательства или шантажа.

На фоне активного курса на импортозамещение и возросшего внимания к решениям российских разработчиков утечки могут стать особенно чувствительными. В открытом доступе может оказаться исходный код отечественного ПО, а также персональные данные пользователей, включая данные особо охраняемых категорий граждан.

По мере цифровизации в зону риска попадут системы промышленной автоматизации, IoT-устройства и интеллектуальные датчики. Их вывод из строя может привести к остановке производственных процессов и срыву операций на объектах критической инфраструктуры. Кроме того, ожидается рост атак на цепочки поставок: через подрядчиков и IT-провайдеров злоумышленники будут проникать в крупные бизнес-системы, что будет приводить к наиболее масштабным последствиям.

Дополнительным фактором риска выступают юридические и регуляторные последствия. В условиях усиления государственного контроля за обращением с персональными данными и соблюдением требований в области ИБ, организациям, ставшим жертвами утечек, грозят существенные штрафы, а в отдельных случаях — уголовная ответственность должностных лиц.

Гроссмейстеры тени: кто атакует организации в России



Кибератаки на российские организации совершаются разными категориями злоумышленников, и у каждой из них есть свои цели, ресурсы и методы.

Наиболее многочисленную категорию составляют киберпреступные группировки, главная цель которых — получение финансовой выгоды. Они распространяют программы-вымогатели, похищают персональные данные для дальнейшей продажи или использования в мошеннических схемах. Как правило, такие группировки действуют сразу в нескольких странах и совершают атаки без привязки к определенной отрасли.

Другую значимую категорию представляют государственно поддерживаемые кибершпионские структуры. Их интересует не столько прибыль, сколько доступ к информации и стратегическое влияние. Эти группы ведут кибершпионаж против государственных учреждений, военных организаций и стратегически важных отраслей — энергетики, оборонной промышленности, телекоммуникаций. Их цель — сбор разведданных, получение доступа к конфиденциальной информации и воздействие на политическую стабильность.

Отдельное место занимают хактивисты — идеологически и политически мотивированные злоумышленники. Уровень их технической подготовки варьируется, однако их действия часто оказываются заметными и ощутимыми. Обычно они шифруют либо уничтожают данные скомпрометированной организации, взламывают сайты для публикации лозунгов или компрометирующих материалов, проводят DDoS-атаки. Интенсивность таких атак нарастает на фоне политических или социальных конфликтов.

Наконец, существуют и одиночки-киберпреступники, действующие вне какой-либо организованной структуры. Их мотивы разнообразны: от желания проверить собственные навыки и получить признание в сообществе до стремления к быстрой финансовой выгоде. С 2022 года Россия, по мнению ряда западных стран, превратилась в своеобразную площадку для легальной отработки инструментов и техник кибератак, что усилило активность таких злоумышленников. В данном разделе их деятельность подробно рассматриваться не будет: основное внимание сосредоточено на трех ключевых категориях атакующих — финансово мотивированных группировках, кибершпионских структурах и хактивистах.

Финансово мотивированные атакующие

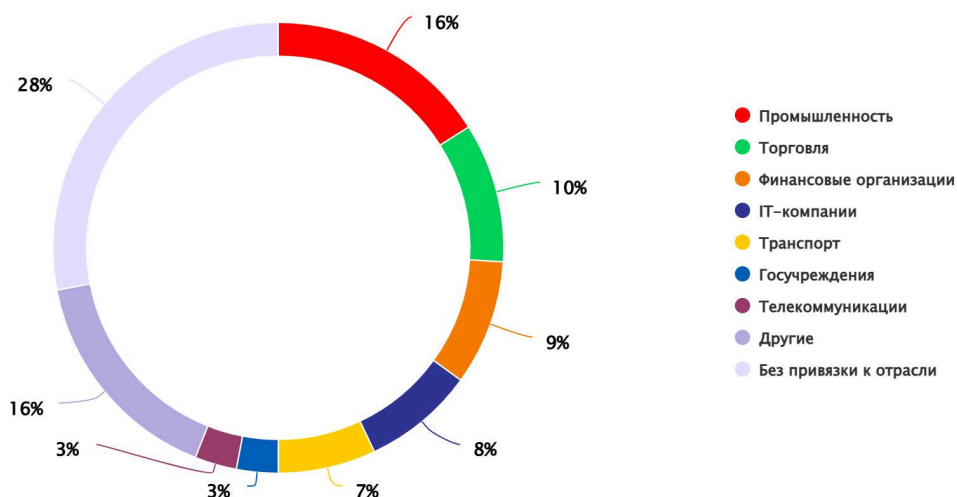


Финансово мотивированные кибергруппировки представляют серьезную угрозу кибербезопасности российских организаций. Их главная цель — получение прямой экономической выгоды, будь то за счет атак на государственные структуры или на частный бизнес. По нашим данным, во второй половине 2024-го и первых трех кварталах 2025 года 28% финансово мотивированных кибератак, жертвами которых становились организации в России, совершались без привязки к отрасли.

Среди жертв, чаще всего подвергавшихся атакам финансово мотивированных группировок, лидируют промышленные предприятия (16%), организации из сферы торговли (10%) и финансовые организации (9%). Наиболее распространенный сценарий атак на промышленность — применение программ-вымогателей. Для предприятий промышленного сектора простои особенно критичны: остановка производственных линий влечет за собой многомиллионные убытки, что повышает вероятность того, что компания согласится выплатить выкуп ради восстановления работы инфраструктуры.

Популярность атак на организации торговой сферы объясняется тем, что ритейлеры обрабатывают большие объемы клиентских данных: данные банковских карт, контактные сведения, историю покупок, дисконтные программы. Такая информация востребована на теневых рынках и может использоваться как для кражи средств, так и для организации новых атак.

Рисунок 13. Категории жертв среди организаций в успешных атаках финансово мотивированных группировок



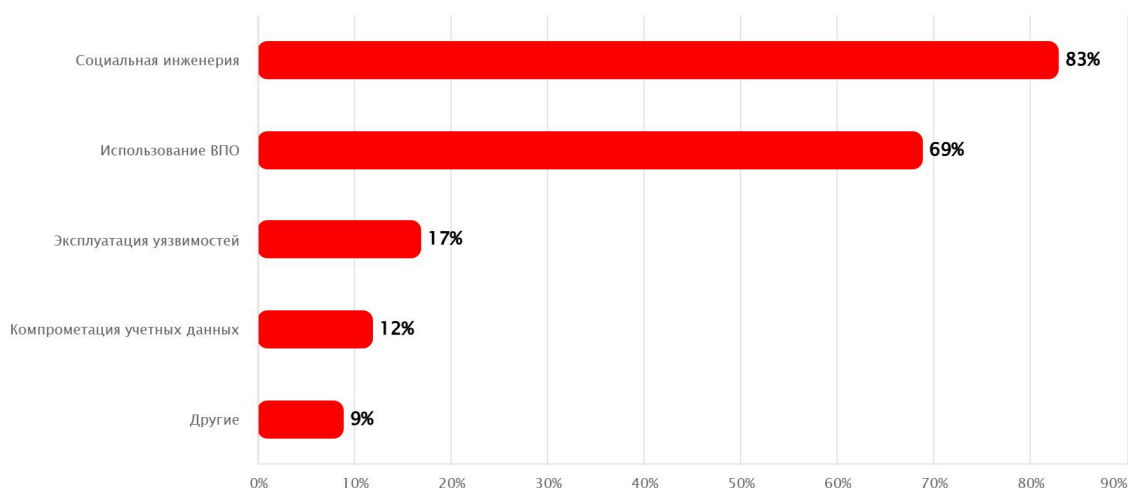
Иногда финансовая мотивация сочетается с элементами кибершпионажа или давления. Например, злоумышленники могут требовать деньги за прекращение публикации конфиденциальных данных, которые подрывают репутацию предприятия, или за полное прекращение атаки. Показателен инцидент июня 2025 года: по данным СМИ, финансово мотивированные киберпреступники скомпрометировали онлайн-магазин, проникнув в инфраструктуру компании через систему 1С, где отсутствовала двухфакторная аутентификация. Злоумышленники зашифровали и частично удалили данные, включая около 30% резервных копий, после чего потребовали 20 млн рублей за ключи расшифрования и неразглашение похищенной информации.

Кто стоит за финансово мотивированными атаками

Во втором полугодии 2024-го и первых трех кварталах 2025 года на российские организации совершали кибератаки не менее 28 финансово мотивированных группировок. На их долю пришлось 33% всех кибератак, направленных против России в указанный период.

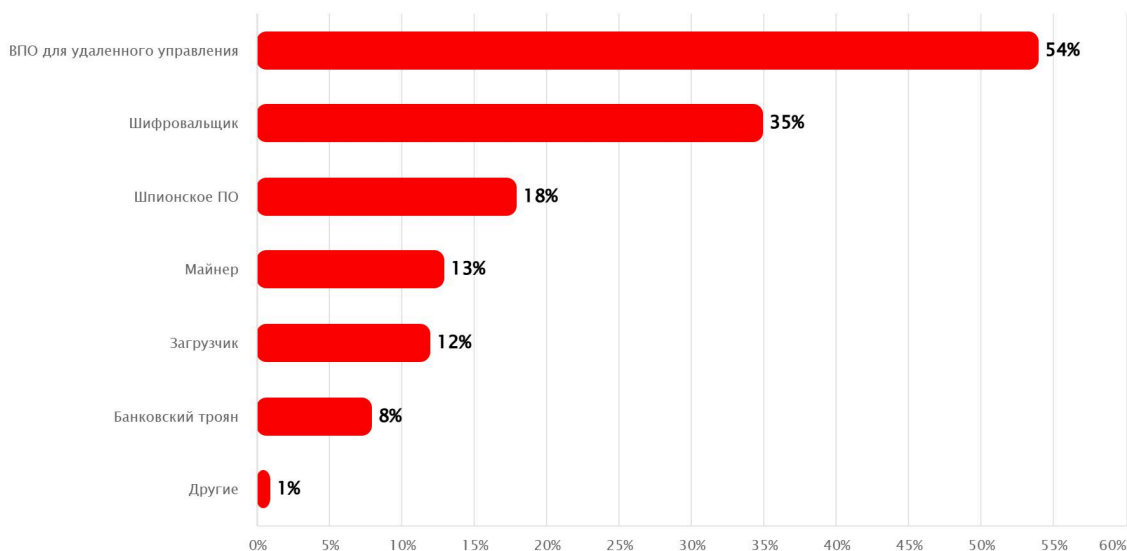
В 83% финансово мотивированных кибератак использовались методы социальной инженерии. Прежде всего речь идет о фишинговых письмах с вредоносными вложениями. Их рассылали не менее 15 группировок. Помимо социальной инженерии, на этапе начального проникновения в инфраструктуру организаций киберпреступники эксплуатировали уязвимости в публичных приложениях (не менее 8 группировок) и использовали в качестве точки входа незащищенные службы удаленного доступа (не менее 5 группировок). О деятельности наиболее активных группировок расскажем подробнее.

Рисунок 14. Методы атак финансово мотивированных группировок (доля успешных атак)



В 35% финансово мотивированных атак использовались шифровальщики. Они есть в арсенале не менее 14 группировок с финансовой мотивацией. Прежде всего речь идет о шифровальщиках LockBit Black (3.0), Babuk и Conti. В рассматриваемый период эти шифровальщики использовались, в частности, такими группировками, как Shadow, Masque, DarkGaboon, Werewolves, Bearlyfy.

Рисунок 15. Типы ВПО, использованного в атаках финансово мотивированных группировок (доля успешных атак с использованием ВПО)



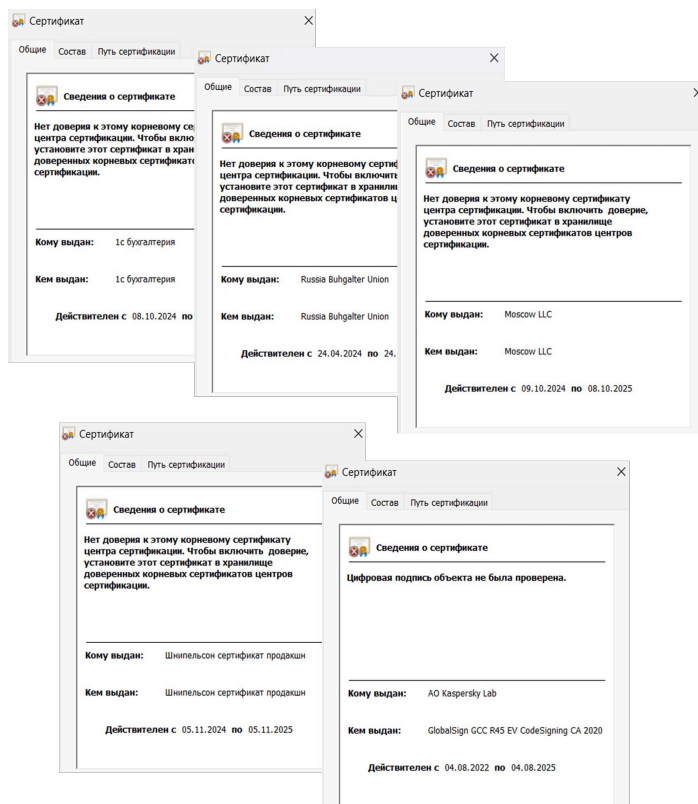
DarkGaboon

В январе 2025 года специалисты PT ESC сообщили об атаках ранее неизвестной группировки DarkGaboon, которая в течение полутора лет атаковала российские компании и оставалась незамеченной. В качестве основного вектора проникновения злоумышленники используют фишинговые письма с вложенным архивом. Внутри архива содержится вредоносное ПО, подписанное поддельным сертификатом X.509, а также документ-приманка, загруженный с легитимных российских ресурсов финансовой тематики. Для повышения правдоподобия в названиях исполняемых файлов и вложений, а также в темах писем применяются омоглифы¹. Арсенал DarkGaboon включает трояны, такие как Revenge RAT и XWorm, а также шифровальщик LockBit Black (3.0).

¹ Омоглифы — графически одинаковые или схожие символы, которые имеют разное значение. Например, кириллическая буква «а» и латинская буква «a».

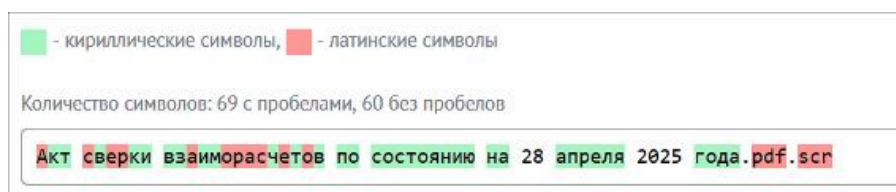
Источник: PT ESC

Рисунок 16. Сертификат X.509



Источник: PT ESC

Рисунок 17. Омоглифы в названии файла



Группировка была активна в период с 2020 по 2022 год, после чего в ее деятельности наступил продолжительный перерыв. Однако во второй половине 2024 года OldGremLin возобновили атаки. В августе 2024 года специалисты PT ESC зафиксировали фишинговые рассылки, нацеленные на российские промышленные предприятия, банки, медицинские организации и разработчиков программного обеспечения. Рассылки приводили к заражению вредоносным ПО для удаленного управления XWorm. В качестве приманки использовались поддельные счет-фактуры.

Рисунок 18. Счет-фактура из фишингового письма группировки OldGremlin

Счет-фактура № **23891-2** **от "09" Августа 2024г.**

Исправление № **01** **от** **09.08.2024**

Продавец: **ООО "Альфа"**
 Адрес: **125090, город Москва, ул. Ленина, д. 123, этаж 3, комната 301**
 ИНН/КПП: **7707083893 / 7707083893**
 Грузополучатель и его адрес: **ООО "Бета", г. Москва, ул. Пушкина, д. 45**
 Грузополучатель и его адрес к платежно-расчетному документу: **ООО "Бета", г. Москва, ул. Пушкина, д. 45**

Документ об оплате: **№ 23891-2 от 01.08.2024**

Получатель: **ООО "Бета"**
 Адрес: **125090, город Москва, ул. Ленина, д. 123, этаж 3, комната 301**
 ИНН/КПП: **7707083893 / 7707083893**
 Валюта, наименование, код: **Российский рубль, 643**
 Идентификатор государственного контракта, договора (соглашения): **№ 01-08.2024**

№ п/п	наименование товаров (работ, услуг) (полное наименование товаров, работ, выполняемых работ, услуг), группировка товаров	Ед. изм.	Количество	Цена (тариф)	Стоимость	В том числе	Сумма	Стоимость	Страна происхождения	Регистр	Адрес	Адрес
1	1	1	1	1	1	1	1	1	1	1	1	1
1	Консультационные услуги в сфере маркетинга	шт	1	207120	207 120	0	207 120	250 000,00	1 500 000,00	1	1	1
Итого:					1 250 000,00	0	250 000,00	1 500 000,00				
Всего к оплате					1 250 000,00	0	250 000,00	1 500 000,00				

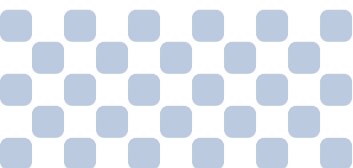
Руководитель организации или иное уполномоченное лицо

Индивидуальный предприниматель или иное уполномоченное лицо

Главный бухгалтер или иное уполномоченное лицо

Индивидуальный предприниматель или иное уполномоченное лицо

Конечной целью атак группы является получение выкупа за расшифрование данных. Так, в ходе одной из атак в начале 2025 года злоумышленники затребовали выплату в размере 500 млн рублей. Специалисты PT ESC отмечают, что для отключения средств защиты информации злоумышленники используют технику Bring Your Own Vulnerable Driver (BYOVD) — эксплуатируют уязвимость PT-2023-6892 (CVE-2023-20598) в драйвере AMD для загрузки своего неподписанного драйвера.



Кейс из практики команды Incident Response экспертного центра безопасности Positive Technologies (PT ESC IR)

Злоумышленники проникли в инфраструктуру заказчика с помощью фишингового письма, открытого одним из сотрудников. Письмо содержало вредоносный ZIP-архив. Внутри архива находился LNK-файл, при запуске которого с удаленного ресурса загружался документ для отвлечения внимания, а также интерпретатор NodeJS с полезной нагрузкой. В результате на скомпрометированном узле был создан DNS-туннель, обеспечивший злоумышленникам канал доступа во внутреннюю сеть.

Для сетевой разведки, закрепления, сбора учетных данных и перемещения внутри сети атакующие применяли общедоступные утилиты (к примеру, ADEplorer, Mimikatz), фреймворк Impacket, а также собственные вредоносные сценарии, драйверы и ПО. Был установлен факт использования образцов уникального вредоносного ПО — TinyIsolator, TinyKiller и шифровальщика TinyCrypt, что указывает на причастность к атаке группировки OldGremlin.

После получения доступа и закрепления злоумышленники останавливали работу локальных средств защиты и распространяли шифровальщик. Основной целью атаки, как и в других кампаниях данной группы, являлось получение финансовой выгоды. Существенным фактором, способствовавшим успешному проведению атаки, стал недостаточный уровень процессов мониторинга в организации.

Для закрепления на скомпрометированных узлах использовался механизм запланированных задач Windows, с помощью которых запускался NodeJS с полезной нагрузкой, обеспечившей злоумышленникам дополнительные каналы доступа и управления. На этапе шифрования использовались вредоносные сервисы Windows, задействованные для запуска TinyKiller. Он удалял правила локального межсетевого экрана, теневые копии ОС и завершал работу локальных средств защиты.

Общая зафиксированная активность атакующих охватила период не менее 99 дней.

DCHelp

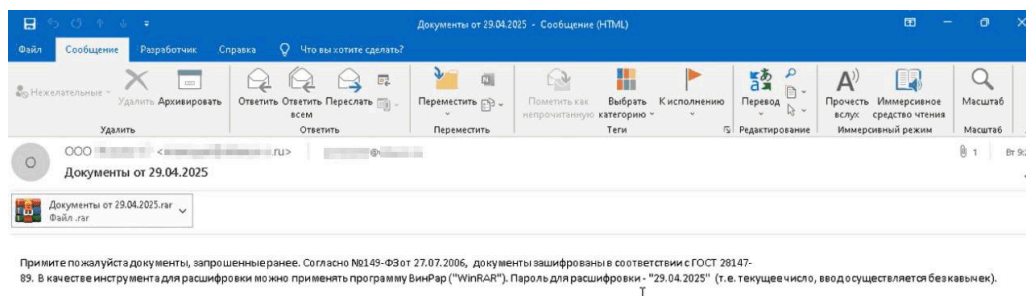
Об активности группировки DCHelp впервые стало известно в 2023 году. Ее целями становятся российские компании из различных отраслей. Для шифрования данных злоумышленники применяют легитимное программное обеспечение DiskCryptor. Первоначальный доступ к инфраструктуре жертв они получают разными способами: путем брутфорса, эксплуатации уязвимостей в публично доступных сервисах, а также с использованием учетных данных, утекших в сеть или приобретенных у брокеров первоначального доступа.

DarkWatchman

Впервые группировка была замечена в ноябре 2021 года и на протяжении всего рассматриваемого периода продолжала проявлять активность. В ее арсенале находятся одноименный DarkWatchman RAT и Buhtrap RAT. Для их распространения злоумышленники используют фишинговые рассылки, а также вредоносные сайты, продвигаемые через рекламные кампании или технику SEO Poisoning. В одном из недавних инцидентов группа задействовала домен компании, ликвидированной еще в 2016 году, повторно активировав его для проведения рассылки.

Источник: PT.ESC

Рисунок 19. Фишинговая рассылка группировки DarkWatchman



Bloody Wolf

Деятельность группировки Bloody Wolf впервые зафиксирована в конце 2023 года в ходе серии атак на организации в Казахстане. Позднее злоумышленники расширили географию своих целей, включив в нее российские организации. Недавно специалисты PT ESC выявили новую волну атак, начавшуюся в мае 2025 года и направленную против организаций в Кыргызстане. Как и в кампании конца 2024 года против казахстанских организаций, вместо вредоносного ПО STRRAT атакующие использовали легитимное средство удаленного администрирования NetSupport.

Proxy Trickster

С 2024 года группировка Proxy Trickster ведет активную деятельность, в ходе которой были скомпрометированы сотни систем в 58 странах, включая Россию. Основные цели злоумышленников – заражение жертв вредоносным ПО для скрытого майнинга криптовалют и организация проксирования трафика в целях его монетизации (прохуjacking). Для проникновения в инфраструктуру они эксплуатируют уязвимости в публично доступных сервисах. В частности, специалисты компании Cado Security Labs обнаружили атаки, направленные на некорректно сконфигурированные экземпляры Selenium Grid – компонента фреймворка Selenium, который используется для автоматизированного тестирования веб-приложений.

Согласно результатам пилотных проектов анализатора сетевого трафика PT NAD, проведенных во втором полугодии 2024 года и первом полугодии 2025 года, в инфраструктуре 82% организаций были выявлены индикаторы, указывающие на наличие майнеров. Также в трафике 46% компаний обнаружены признаки активности резидентных прокси. Это может означать, что на устройствах сотрудников установлены программы категории прохуware, которые позволяют сдавать часть интернет-трафика в аренду сторонним сервисам. Наличие следов прохуware и майнеров в корпоративной сети может указывать на присутствие в ней финансово мотивированных киберпреступников.

В атаках Proxy Trickster использовались майнер XMRig и утилиты, связанные с платформами Honeygain, PacketShare, IPRoyal Pawns, Traffmonetizer и другими сервисами монетизации интернет-канала. Подобная активность создает серьезные риски: снижение производительности сети, компрометацию IP-адреса компании и даже возможную юридическую ответственность в случае использования корпоративной сети для противоправных действий.

Какие факторы способствуют эскалации финансово мотивированных атак в России

- **Слияние мотиваций в кибератаках.** В последнее время политические и идеологические мотивы хактивистов все чаще переплетаются с финансовыми интересами. После 2022 года некоторые группы вымогателей начали публично заявлять, что атакуют российские компании по политическим соображениям. Однако с каждым годом становится все больше хактивистов, которые не просто шифруют информацию, но и оставляют записки с требованиями заплатить выкуп.

Характерным примером стала атака группировки Black Owl на одну из производственных организаций. Используя фишинговое письмо, злоумышленники внедрили шифровальщик и скомпрометировали инфраструктуру. В результате были парализованы ключевые бизнес-процессы: остановились отгрузки, прекратился прием заказов, а из личных кабинетов клиентов исчезли данные. За восстановление группировка потребовала 50 тыс. долларов. Однако несмотря на то, что компания, по утверждению самих злоумышленников, согласилась выплатить выкуп, ключи расшифрования так и не были предоставлены.

В ряде случаев хактивисты получают финансовую, техническую или информационную поддержку от структур, разделяющих их позицию. При этом доход от атак становится для них дополнительным стимулом. В результате киберпреступные группы со смешанными мотивами отличаются большей устойчивостью и мотивацией, продолжая свою деятельность даже при снижении прибыльности кибератак, поскольку в этом случае для них остается вторая, не менее важная цель — политическая или идеологическая.

- **Готовность организаций платить выкупы вымогателям.** При успешной атаке со стороны финансово мотивированных злоумышленников российские организации оказываются перед выбором: либо длительные простои из-за зашифрованных данных и потеря клиентов, либо относительно быстрое восстановление работы за счет выплаты выкупа.

Репутационные риски и возможные санкции со стороны регуляторов (например, штрафы за утечку персональных данных) могут подталкивать организацию к закрытому урегулированию инцидента. Кажется, что выплата выкупа позволяет сократить время простоя и скрыть масштабы проблемы от партнеров и клиентов.

Именно готовность жертв идти на уступки становится одним из ключевых факторов, стимулирующих рост финансово мотивированных атак с применением шифровальщиков. Логика проста: если модель вымогательства приносит доход, она будет воспроизводиться и масштабироваться. Наглядный пример — динамика развития новой группировки Bearlyfy, впервые обнаруженной специалистами компании F6 в начале 2025 года. В первых зафиксированных кампаниях размер выкупа составлял всего несколько тысяч долларов, тогда как в последней атаке злоумышленники просили уже 80 тыс. евро. Как отмечают эксперты, из-за относительно невысоких сумм требований в среднем каждая пятая жертва группировки соглашается приобрести у злоумышленников ключи расшифрования.

Почему не стоит платить вымогателям

1 Нет гарантии восстановления данных

- Ключ расшифрования могут не прислать.
- Ключ отправят, но он может оказаться нерабочим.
- Данные могут быть безвозвратно повреждены.

2 Нет гарантии, что данные не будут опубликованы или проданы третьим лицам

Даже если вы получите рабочий ключ, ваши данные все равно могут быть опубликованы или проданы в дарквебе. Это касается и случаев, когда данные не были зашифрованы, но злоумышленники требовали деньги за их неразглашение.

3 Вы станете мишенью для повторных атак

Заплатив, вы становитесь в глазах киберпреступников платежеспособной жертвой, и риск повторных атак возрастает.

4 Вы финансируете преступную деятельность

Готовность организаций платить лишь стимулирует киберпреступников к развитию и проведению новых атак.



 Низкая международная кооперация по киберпреступлениям.

В нормальных условиях правоохранительные органы разных стран активно обмениваются информацией: передают данные о группировках, помогают в расследованиях, выдают подозреваемых и координируют операции. Однако санкции и геополитическая напряженность ограничили или вовсе оборвали эти каналы — ряд стран перестали сотрудничать с Россией в правовой сфере.

Если киберпреступную деятельность сложно пресечь на международном уровне, преступники чаще выбирают цели с прямой денежной выгодой: кража денежных средств со счетов, вымогательство с использованием шифровальщиков, мошенничество с платежами и криптовалютой. К тому же сокращение доступа к международным каналам обмена киберразведданными и взаимодействия с иностранными вендорами ИБ и DFIR-подрядчиками увеличивает время обнаружения злоумышленников и реагирования на кибератаку, а значит — растет и финансовая результативность злоумышленников.

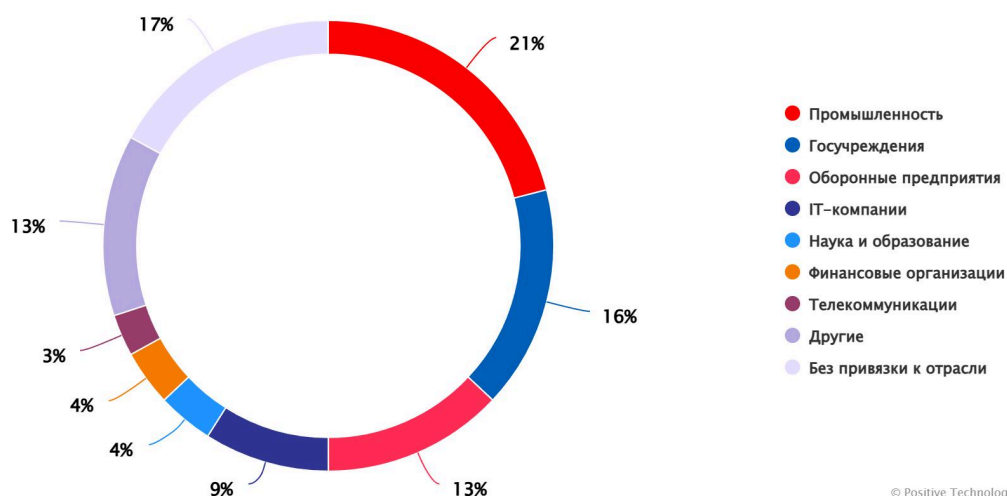


Кибершпионские группировки представляют еще одну серьезную угрозу для кибербезопасности российских организаций. В отличие от финансово мотивированных злоумышленников, их деятельность направлена не на получение быстрой прибыли, а на долгосрочное извлечение информации, имеющей стратегическую ценность. Это могут быть государственные документы, технологические разработки, коммерческая информация, а также сведения о партнерах и клиентах.

Во второй половине 2024-го и первых трех кварталах 2025 года чаще всего кибершпионы атаковали промышленные предприятия (21%), государственные учреждения (16%) и организации оборонного комплекса (13%). Эти отрасли становятся приоритетными целями в силу высокой концентрации чувствительных данных — от массивов персональных данных и служебных сведений до результатов научно-технических разработок и конструкторской документации. Контроль над такими ресурсами дает возможности для стратегической разведки и длительного мониторинга внутренних процессов инфраструктуры.

При этом доступ к системам таких организаций может использоваться не только для скрытой эксфильтрации данных, но и для создания плацдарма под будущие операции. Речь может идти о внедрении в сегменты АСУ ТП, закладке вредоносных модулей в цепочки поставок ПО и оборудования, а также о подготовке сценариев, способных вызвать нарушения в критически важных технологических процессах. Таким образом, атакующие формируют не просто разовый канал утечки информации, а устойчивый механизм влияния на организацию или даже целую отрасль.

Рисунок 20. Категории жертв среди организаций в успешных атаках кибершпионских группировок



Кейс из практики команды Incident Response экспертного центра безопасности Positive Technologies (PT ESC IR)

Злоумышленникам удалось скомпрометировать ряд сетевых маршрутизаторов Cisco, доступных напрямую из интернета. В одном из случаев они воспользовались ошибкой в настройке протокола SNMPv2 (настройка SNMP community): для всех устройств был задан режим «чтение-запись» на несуществующий список доступа, что позволило получить доступ на данный маршрутизатор по SNMP по стандартному паролю.

На протяжении нескольких месяцев злоумышленники применяли системные возможности Cisco IOS для организации туннелирования трафика по протоколу GRE, проведения разведки сетевых устройств и корпоративной инфраструктуры, создания локальных учетных записей с расширенными привилегиями, попыток выгрузки данных с сервера резервного копирования, а также сокрытия своей активности. Для этого использовались специально созданные сценарии на базе механизма Cisco Embedded Event Manager (EEM-апплеты), которые при выполнении определенных штатных команд инициировали сброс конфигурации устройства и удаляли следы активности. Использование распространенных административных команд усложняет обнаружение злоумышленников.

В результате атаки злоумышленники на протяжении как минимум двух месяцев контролировали часть сетевого трафика инфраструктуры. Было зафиксировано перенаправление значительных объемов данных (не менее 15 ГБ), включая трафик почтовых протоколов SMTP, POP3 и IMAP.

Анализ материалов, предоставленных заказчиком, и характер активности указывали на то, что основной целью злоумышленников являлся кибершпионаж.

Среди факторов, способствовавших успеху атаки, выделяются недостаточный уровень мониторинга и небезопасная настройка разграничения доступа.

Общая продолжительность активности атакующих составила не менее 84 дней.

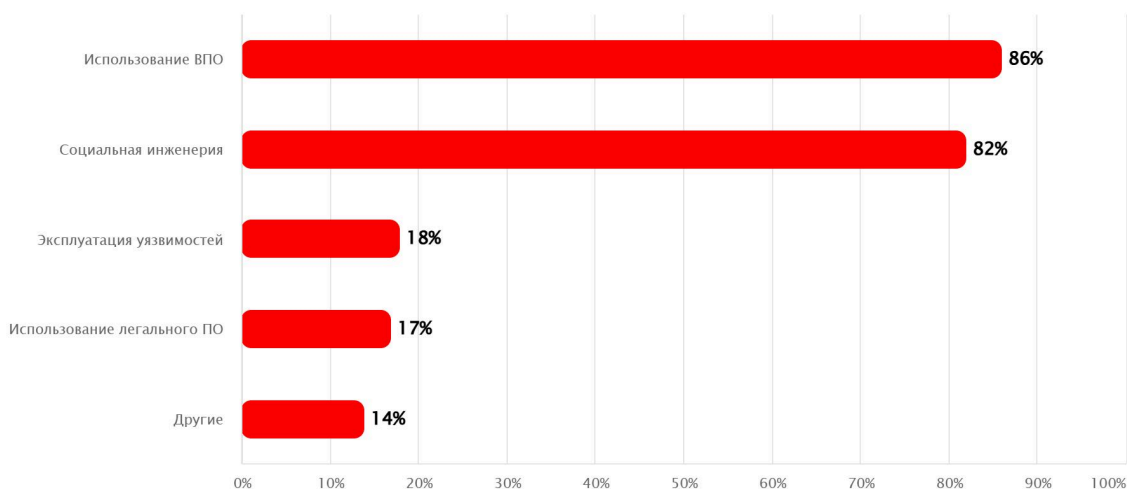
Кто стоит за кибершпионскими кампаниями

Во второй половине 2024-го и в первых трех кварталах 2025 года зафиксированы кибератаки на организации в России со стороны не менее 22 кибершпионских группировок. На долю успешных атак со стороны кибершпионов в этот период пришлось 22% всех успешных кибератак в России.

Особую угрозу представляет то, что такие группировки нередко действуют при поддержке или в интересах иностранных государств. Это делает их атаки более организованными и трудными для обнаружения. Отдельно стоит отметить, что подобные атаки отличаются высокой степенью подготовки. В 82% случаев кибершпионские кампании сопровождались целевой социальной инженерией и кампаниями фишинга, зачастую направленными против конкретных сотрудников с доступом к нужным данным.

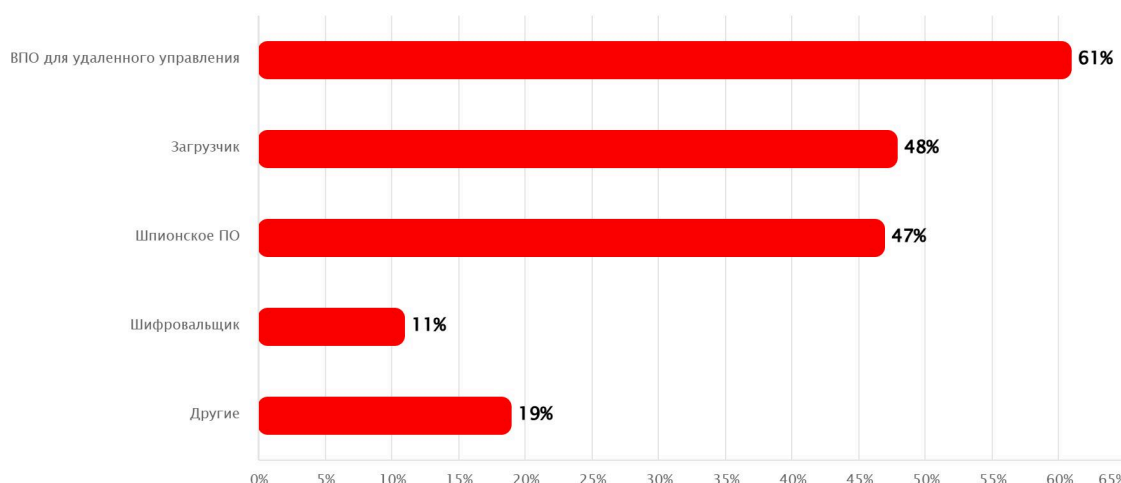
В 86% атак применялось вредоносное ПО, включая инструменты собственной разработки. В каждой пятой атаке (18%) злоумышленники эксплуатировали уязвимости, в том числе нулевого дня.

Рисунок 21. Методы атак кибершпионских группировок (доля успешных атак)



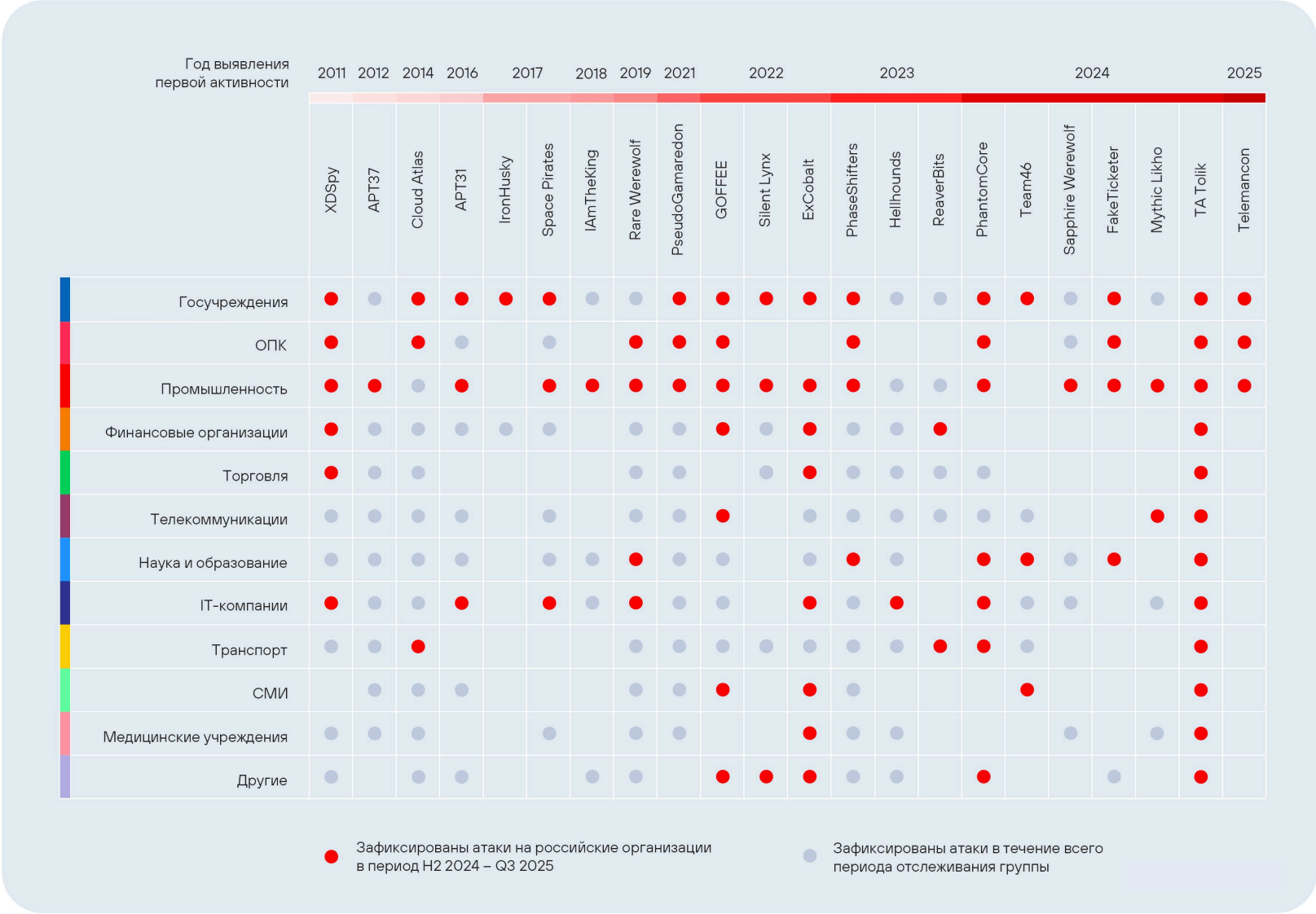
Получив доступ к инфраструктуре, кибершпионы стремятся закрепиться в системе: создают скрытые каналы связи, настраивают сетевые туннели и внедряют инструменты для удаленного управления. Вредоносное ПО для удаленного управления использовалось в 61% успешных атак.

Рисунок 22. Типы ВПО, использованного в атаках кибершпионских группировок (доля успешных атак с использованием ВПО)



В числе наиболее активных кибершпионских группировок можно выделить ExCobalt, Rare Werewolf, GOFFEE, PhaseShifters, PseudoGamaredon, Cloud Atlas, PhantomCore. Помимо этого выявлена активность новых групп, например Telemancor, TA Tolik, Mythic Likho, FakeTicketer, Team46. Список кибершпионских группировок, атаковавших Россию во второй половине 2024-го и в 2025 году, представлен на рисунке 23. О деятельности некоторых из них будет рассказано более подробно.

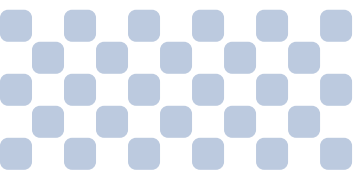
Рисунок 23. Отрасли, атакуемые кибершпионскими группировками во втором полугодии 2024-го и в первых трех кварталах 2025 года



ExCobalt

На раннем этапе своей киберпреступной деятельности, начавшейся еще в 2016 году, группировка была известна под названием Cobalt. Однако по мере ее трансформации из финансово мотивированной в шпионскую исследователи дали ей новое имя — ExCobalt. Сегодня эта группа входит в число наиболее активных на территории России. Во втором полугодии 2024-го и в первой половине 2025 года команда Incident Response PT ESC расследовала более десяти инцидентов, связанных с ее атаками.

За все годы своей активности злоумышленники никогда не стояли на месте: они постоянно модифицируют и усложняют свой арсенал, совершенствуют тактики и техники. Так, специалисты PT ESC отмечают, что вместо привычных методов первоначального доступа — фишинга или эксплуатации уязвимостей в публичных приложениях — преступники все чаще используют украденные учетные данные подрядчиков. Кроме того, зафиксировано применение нового многофункционального вредоносного ПО Ruma, которое сочетает возможности дроппера, бэкдора, загрузчика и руткита уровня ядра для Linux, а также обладает функцией стилера.



Кейс из практики команды Incident Response экспертного центра безопасности Positive Technologies (PT ESC IR): атака группировки ExCobalt

Злоумышленники использовали широкий набор инструментов, включая:

утилиты для повышения привилегий на скомпрометированных узлах:

- DeadPotato, CoercedPotato, EfsPotato и GodPotato – эксплойты, использующие уязвимости в механизмах межпроцессного взаимодействия Windows;
- инструменты для туннелирования трафика и организации защищенных соединений: cloudflared, модифицированная версия утилиты FRP (Fast Reverse Proxy), утилита vnt;
- инструмент для получения учетных данных из памяти системы Mimikatz;
- инструменты для удаленного выполнения команд: suo5, PsExec, NetExec, Atexec-pro и фреймворк Impacket;
- легитимное ПО для удаленного управления Radmin – используется для постоянного доступа и управления скомпрометированными узлами.

Отдельного внимания заслуживает модификация легитимного файла flogon.js, позволившая злоумышленникам похищать учетные данные пользователей на почтовом сервере Microsoft Exchange. В результате им удалось получить примерно 650 учетных записей. Кроме того, злоумышленники изменили временные метки файлов для затруднения расследования инцидента.

На финальной стадии атаки киберпреступники централизованно распространили и запустили в инфраструктуре шифровальщики: LockBit на узлах под управлением Windows и Babuk на системах Linux. Эти действия указывают на связь атаки с группировкой ExCobalt.

Несмотря на использование шифровальщиков, имеются основания полагать, что основной целью злоумышленников было не получение финансовой выгоды, а максимальное выведение из строя узлов инфраструктуры, в том числе критически важных.

Ключевыми факторами, способствовавшими успешности атаки, стали недостаточный уровень мониторинга и слабая сегментация сети.

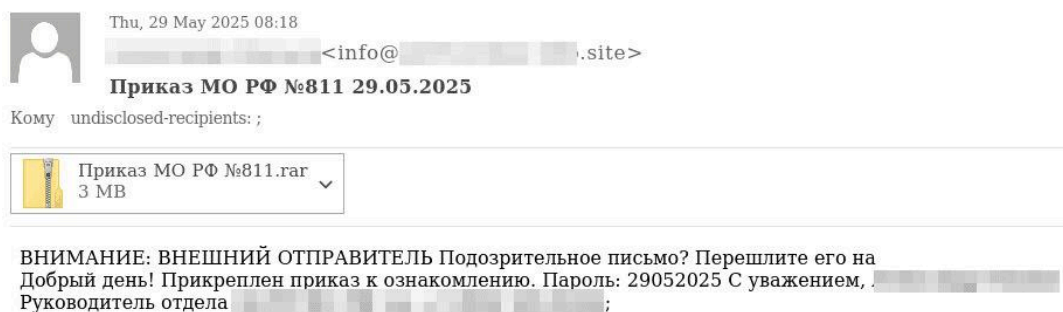
Зафиксированная активность атакующих продолжалась не менее 24 дней.

Rare Werewolf

Группировка Rare Werewolf в течение последнего года проводила атаки на организации различных отраслей в России, Белоруссии и Казахстане. Для первоначального доступа злоумышленники используют фишинговые рассылки, содержащие архивы с паролем, который указывается в тексте письма. Такой подход помогает обходить почтовые фильтры. С начала 2025 года команда киберразведки PT ESC фиксирует появление новых серверов управления, задействованных группировкой, а также использование дополнительных инструментов в атаках. Во втором квартале Rare Werewolf пыталась выдать себя за российский военный концерн, распространяя вредоносное ПО через домены, максимально похожие на домен реальной организации, от имени которой велась рассылка.

Источник: PT ESC

Рисунок 24. Пример фишингового письма группировки Rare Werewolf



Изначально эксперты относили Rare Werewolf к финансово мотивированным группировкам. Однако детальный анализ ее инфраструктуры и активности показал, что основным приоритетом является кража конфиденциальной информации, а использование майнера XMRig в отдельных инцидентах носит второстепенный характер и служит лишь дополнительным инструментом.

GOFFEE

Группировка известна с 2022 года. Для получения первоначального доступа она традиционно использует фишинг. В атаках, описанных в 2024 году, в качестве вложений злоумышленники рассылали документы с вредоносными макросами. В ряде случаев для организации фишинговых кампаний они злоупотребляли фреймворком с открытым исходным кодом Gophish, изначально предназначенным для проведения фишинговых симуляций и обучения сотрудников кибербезопасности.

В более поздних кампаниях, обнаруженных специалистами PT ESC, киберпреступники распространяли RAR-архивы, эксплуатирующие уязвимости в WinRAR. В одном случае использовалась уязвимость PT-2025-26225 (CVE-2025-6218), о которой мы подробно рассказывали в дайджесте трендовых уязвимостей. В другом применялся эксплойт для уязвимости нулевого дня, пока не получившей идентификатор. По данным экспертов, эксплойт мог быть приобретен на одном из хакерских форумов за 80 тыс. долларов и впоследствии доработан для проведения кибератак. Факт покупки столь дорогостоящих эксплойтов указывает на то, что киберпреступники инвестируют в развитие собственной инфраструктуры. Это свидетельствует о высокой рентабельности их операций: прибыль от кибератак, вероятно, значительно превышает понесенные затраты.

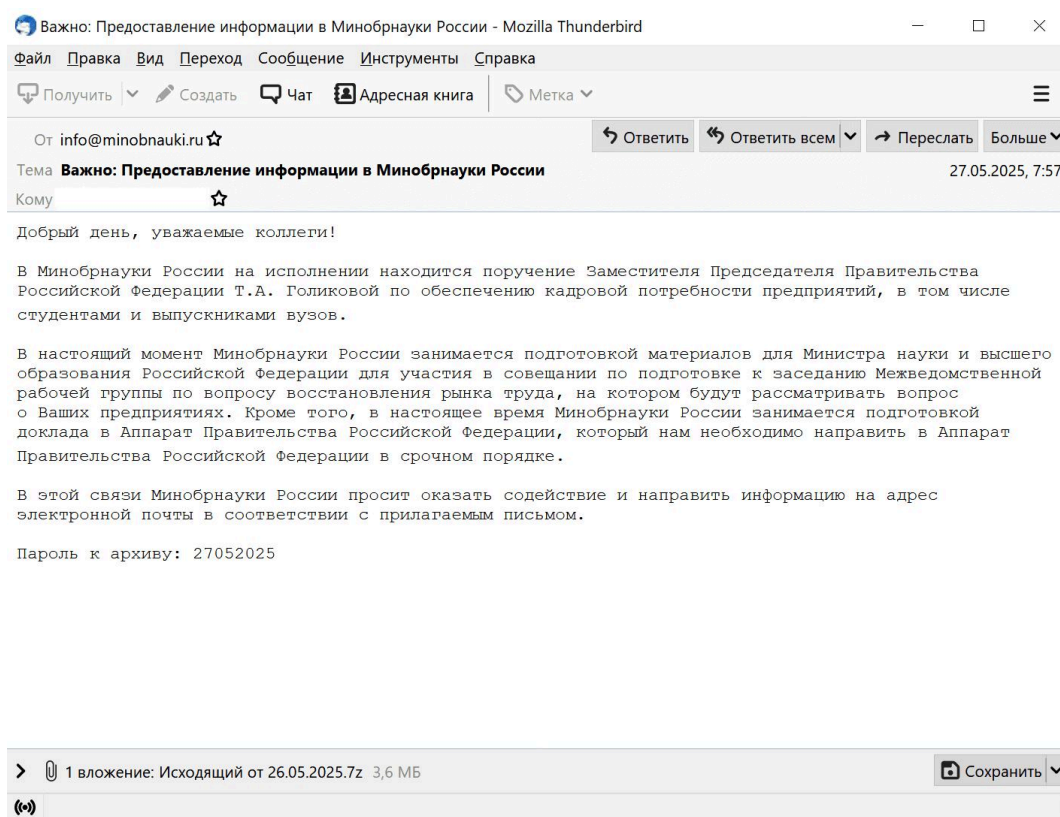
Во втором полугодии 2024 года в ходе расследования инцидентов команда PT ESC IR выявила, что группировка GOFFEE продолжает применять привычные для себя инструменты – Owowa, PowerTaskel, TinyShell, Chisel и другие. Вместе с этим злоумышленники расширили свой арсенал, добавив средства для туннелирования трафика BindSycler и DQuic, новый Mythic-агент MiRat и руткит Sauropsida. Подробнее об этом можно узнать в статье «Гадание на Goffeеной гуще: актуальные инструменты и особенности группировки Goffee в атаках на Россию».

PhaseShifters

Группировка PhaseShifters атакует организации в России и Белоруссии как минимум с 2023 года и сохраняла активность на протяжении всего рассматриваемого периода. Как и ранее, для получения первоначального доступа злоумышленники преимущественно используют фишинговые письма с вредоносными вложениями, например зашифрованными архивами, пароль к которым указывается прямо в тексте письма.

Источник: PT ESC

Рисунок 25. Пример фишингового письма группировки PhaseShifters



В описанной в ноябре 2024 года специалистами PT ESC кампании атакующие использовали стеганографию для сокрытия вредоносного ПО в изображениях — таким образом они пытались обойти антивирусную защиту. В атаках, обнаруженных в январе 2025 года, использовался вредоносный документ с техникой Forced Authentication, позволявшей получать NTLM-хеши пользователей. Инструментарий группировки продолжает расширяться: к уже имеющемуся арсеналу добавились различные трояны, стилеры, а также крипторы по подписке².

² Сервис крипторов по подписке (crypter as a service, CaaS) — услуга, предоставляемая пользователям на платной основе, позволяющая зашифровывать, упаковывать или обфусцировать файлы (не обязательно вредоносные).

PseudoGamaredon

Злоумышленники из группы PseudoGamaredon действуют как минимум с 2021 года. Их основными целями являются российские государственные органы, организации ОПК и объекты критической инфраструктуры. Они распространяют вредоносные файлы не только через электронную почту, но и через мессенджеры, включая Telegram. Фишинговые приманки нередко маскируются под приказы и другие документы от госструктур. Так, в I квартале 2025 года специалисты PT ESC обнаружили письмо, отправленное якобы от имени ФСБ России. Для обеспечения удаленного доступа группировка применяет легитимное программное обеспечение UltraVNC и MeshCentral.

Источник: PT ESC

Рисунок 26. Документ-приманка из фишинговой рассылки группировки PseudoGamaredon



Cloud Atlas

Первая активность группировки была зафиксирована еще в 2014 году. За период своего существования она атаковала множество организаций из различных отраслей по всему миру. В рассматриваемом периоде под ее прицел попали учреждения в России, Белоруссии, Кыргызстане и Молдове.

Специалисты TI-департамента PT ESC регулярно фиксируют фишинговые кампании этой группы, что позволяет отслеживать изменения в ее тактиках и своевременно пресекать вредоносную активность в инфраструктуре пользователей продуктов Positive Technologies. Так, было установлено, что злоумышленники используют документы, похищенные из ранее скомпрометированных организаций, а также задействуют взломанные адреса электронной почты для проведения новых фишинговых рассылок.

Источник: PT ESC

Рисунок 27. Пример вредоносного документа, рассылаемого с корпоративных адресов электронной почты ранее зараженных предприятий

АКТ СВЕРКИ

Взаимных расчетов по состоянию на _____ 2024 года

Между _____ и _____

«__» _____ 2024 года

Мы нижеподписавшиеся, _____ ООО _____, с одной стороны, и _____, с другой стороны, составили настоящий акт сверки в том, что состояние взаимных расчетов по данным учета следующее:

По данным				По данным			
№ п/п	Наименование операции, документы	Дебет	Кредит	№ п/п	Наименование операции, документы	Дебет	Кредит
1.	Сальдо						
2.							
3.							
4.							

PhantomCore

О группе стало известно в январе 2024 года, и на протяжении рассматриваемого периода она наращивала активность против российских кампаний. По данным специалистов TI-департамента PT ESC, с мая по июль 2025 года злоумышленники заразили более 180 хостов в российских организациях.

Для первоначального доступа атакующие продолжают использовать фишинговые рассылки, которые могут отправляться со скомпрометированных адресов реальных организаций. При этом они интегрируют в фишинг трендовые техники, такие как fakeCaptcha. Кроме того, группа расширила инструментарий: обновила ранее применявшиеся средства и дополнила их новыми.

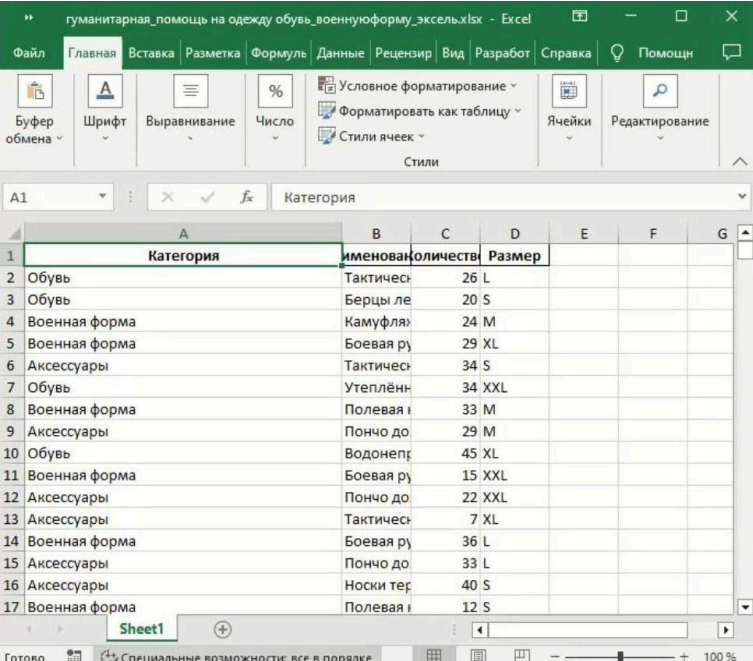
Telemancor

Группировка Telemancor впервые привлекла внимание специалистов по кибербезопасности в феврале 2025 года в ходе атак на российские промышленные организации. В своих кампаниях злоумышленники применяют самописные инструменты — дроппер TMCDropper и бэкдор TMCShell, которые они продолжают активно развивать.

Так, в последней операции, зафиксированной специалистами PT ESC, в обновленной версии TMCDropper была реализована техника VM-based obfuscation, усложняющая анализ кода. В рамках той же кампании преступники использовали фишинговые приманки, связанные с гуманитарной помощью.

Источник: PT ESC

Рисунок 28. Фишинговая приманка, связанная с гуманитарной помощью



Категория	Именованное количество	Размер
Обувь	Тактические	26 L
Обувь	Берцы ле	20 S
Военная форма	Камуфляж	24 M
Военная форма	Боевая ру	29 XL
Аксессуары	Тактические	34 S
Обувь	Утепленные	34 XXL
Военная форма	Полевая и	33 M
Аксессуары	Пончо до	29 M
Обувь	Водонепр	45 XL
Военная форма	Боевая ру	15 XXL
Аксессуары	Пончо до	22 XXL
Аксессуары	Тактические	7 XL
Военная форма	Боевая ру	36 L
Аксессуары	Пончо до	33 L
Аксессуары	Носки тер	40 S
Военная форма	Полевая и	12 S

TA Tolik

Активность группы TA Tolik впервые была зафиксирована в сентябре 2024 года в ходе кибершпионской кампании, связанной с распространением ранее неизвестного инфостилера Unicorn. С апреля 2025 года специалисты PT ESC отмечают возобновление активности группировки, при этом ключевым инструментом атак остается вредоносное ПО Unicorn.

Для первоначального доступа злоумышленники традиционно используют фишинговые письма, содержащие архив с HTA-файлом, маскирующимся под легитимный документ или уведомление от государственных служб. В майской кампании злоумышленники, как и группировка PseudoGamaredon, задействовали новый вектор распространения - через мессенджер Telegram.

Ранее в нашем исследовании, посвященном фишинговым атакам, мы прогнозировали рост числа кампаний с первоначальным вектором через мессенджеры и социальные сети, и текущие события подтверждают эти предположения.

FakeTicketer

Дебют группы FakeTicketer состоялся в июне 2024 года: под видом билетов на спортивное мероприятие атакующие распространяли собственное вредоносное ПО — стилер, ВПО для удаленного управления и дроппер, объединенные под названием Zagrebator.

Источник: F6

Рисунок 29. Фишинговая приманка, обнаруженная в рамках первой кампании группы FakeTicketer



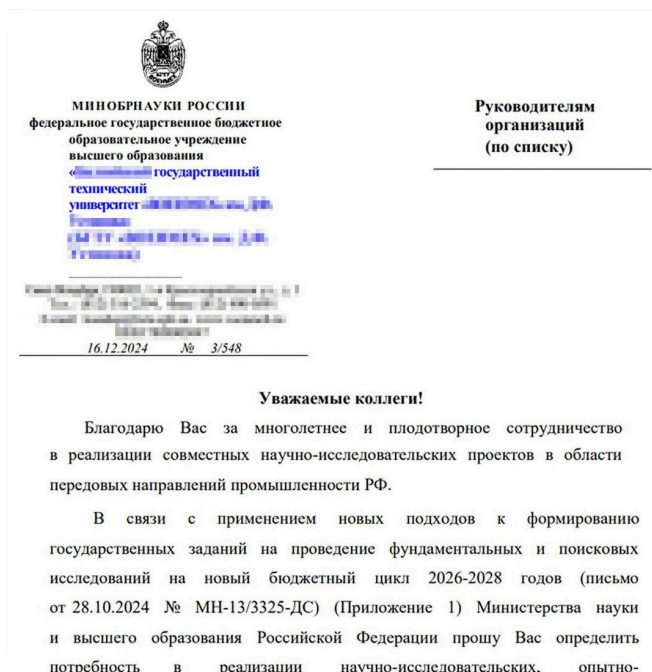
В дальнейшем злоумышленники применяли различные документы в качестве приманок: школьный аттестат, нормативные акты администрации города Симферополь, а в последней известной атаке — официальный документ, якобы подготовленный от имени одного из государственных технических университетов.

Впервые об этой активности сообщили специалисты PT ESC в январе 2025 года. В марте специалисты Seqrite Labs описали эту кампанию, дав ей название Operation HollowQuill, а эксперты F6 связали ее с группировкой FakeTicketer.

Основными целями преступников стали российские промышленные, научные и оборонные организации. В качестве конечной полезной нагрузки применялся постэксплуатационный фреймворк Cobalt Strike.

Источник: PT ESC

Рисунок 30. Фишинговый документ-приманка, распространяемый в рамках операции HollowQuill



Team46

В ноябре 2024 года специалисты PT ESC сообщили об атаке ранее неизвестной группировки TaxOff, нацеленной на государственные структуры России. Отличительной чертой киберпреступников стал собственный многопоточный бэкдор Trinper.

В середине марта 2025 года исследователи из «Лаборатории Касперского» зафиксировали целевую кампанию под названием «Форумный тролль», в ходе которой распространялись фишинговые письма, эксплуатирующие уязвимость нулевого дня в браузере Chrome (PT-2025-12837, CVE-2025-2783). Изучив подробнее атаку, специалисты PT ESC установили, что в рамках этой операции загружался бэкдор Trinper, ранее связанный с TaxOff, а также выявили пересечения с деятельностью группы Team46, описанной в сентябре 2024 года.

Сходство наблюдалось и в используемых векторах атак: так, в ранних кампаниях Team46 эксплуатировалась уязвимость нулевого дня в «Яндекс Браузере» (PT-2024-5901, CVE-2024-6473). Совокупность этих фактов позволила сделать вывод, что операция «Форумный тролль» связана с обеими группами, которые на деле представляют собой одну и ту же структуру.

Подробнее об этом читайте в статье «Team46 и TaxOff: две стороны одной медали».

Какие факторы способствуют эскалации кибершпионских кампаний в России

- **Экономическая трансформация и технологический рывок под давлением санкций.** В 2014 году начался уход иностранных компаний из России, а в 2022-м он приобрел массовый характер. В результате освободились ниши, которые теперь занимают российские предприятия или партнеры из дружественных стран. Санкции и отток зарубежных конкурентов, как ни парадоксально, стали катализатором развития: страна стремится закрыть все технологические «узкие места» и превратить внешнее давление в стимул внутреннего роста. Ведутся активные разработки в области высоких технологий (ИИ, кибербезопасность, квантовые вычисления), энергетики, космической и авиационных отраслей, медицины, биотехнологий и других.

Информация обо всех новых разработках, будь то технические характеристики, производственные мощности, логистика или этапы внедрения, может интересовать различные страны, независимо от уровня сотрудничества с ними. Владение такими данными позволяет злоумышленникам совершать кибератаки, направленные на ослабление экономического потенциала организации или даже целой отрасли.

- **Повышенный интерес к оборонно-промышленному комплексу.** В России идет системная перестройка ОПК: разработка новейших видов вооружения, цифровизация, привлечение новых участников и увеличение производства. Так, в 2024 году государственная программа развития ОПК была продлена до 2034 года, а в 2025-м установлены приоритеты господдержки проектов в сфере искусственного интеллекта для предприятий отрасли.

Любое технологическое усиление России в ОПК воспринимается оппонентами как угроза. Это подталкивает их к проактивному кибершпионажу. Недружественные страны следят за новыми разработками, чтобы понять, какие технологии Россия осваивает быстрее всего, оценить устойчивость российского ОПК к санкциям и выработать контрмеры. В свою очередь, союзники также могут проводить кибершпионские кампании — чтобы перенять тактические решения, которые уже доказали эффективность.

Перестройка означает подключение множества новых подрядчиков, в том числе малых компаний, которые часто имеют более низкий уровень защищенности. Одновременно масштабная модернизация ОПК сопровождается значительным потоком данных, представляющих интерес для злоумышленников: проектной документации, результатов испытаний, служебной переписки с подрядчиками. Все это делает инженерные, научно-производственные и оборонно-промышленные предприятия приоритетной целью для кибершпионов.



В отличие от киберпреступников с финансовой мотивацией или кибершпионов, работающих на получение стратегически ценной информации, хактивисты руководствуются идеологическими, политическими или социальными мотивами. Так, 87% всех успешных атак хактивистских группировок в странах СНГ были направлены против России. Хотя отдельные инциденты отмечались и в других государствах региона — например, в Азербайджане, Армении и Молдове, — их значение в глобальных конфликтах не столь велико, и сами атаки не оказывают заметного политического эффекта. Россия воспринимается как ключевой участник крупных геополитических процессов, что делает ее более привлекательной и приоритетной целью.

Хактивисты представляют угрозу не только для отдельных компаний, но и для целых отраслей. Наибольшему риску подвержены:

- **государственные учреждения** — кибератаки могут нарушить работу критически важных сервисов, повлиять на функционирование систем управления и подорвать доверие граждан к государственным структурам;
- **промышленность**, особенно предприятия **топливно-энергетического комплекса** — вмешательство в их работу носит стратегический характер и может привести к остановке производственных линий, сбоям в работе больниц, общественного транспорта и других жизненно важных служб;
- **телекоммуникации** — кибератаки могут вызвать перебои в связи, ограничить доступ к интернет-сервисам и нарушить работу цифровой инфраструктуры, что, в свою очередь, осложнит реагирование на чрезвычайные ситуации и оказание экстренной помощи;
- **транспортная инфраструктура**, включая аэропорты, железные дороги, морские порты и городские системы управления движением — вмешательство в их работу грозит срывом своевременной доставки сырья, продуктов питания, промышленных товаров и других необходимых ресурсов, а также ограничением или полной остановкой пассажирских перевозок;
- **сфера здравоохранения** — из-за высокой социальной значимости: вмешательство в работу больниц ставит под угрозу жизни пациентов, а атаки на аптеки нарушают доступ к жизненно важным лекарствам.

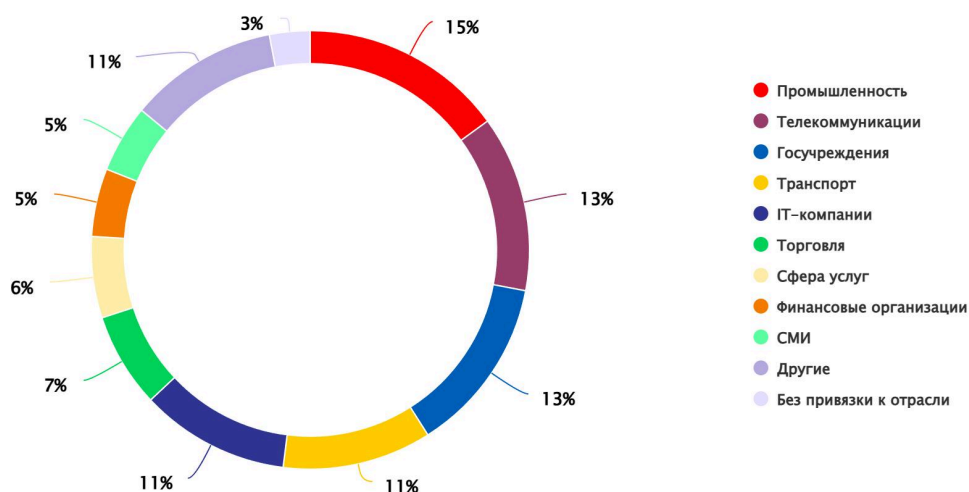
Несмотря на то что во второй половине 2024-го и первых трех кварталах 2025 года не фиксировалось масштабных деструктивных атак на медицинские учреждения, включая критически важные системы жизнеобеспечения пациентов, сама потенциальная угроза делает эту сферу одной из наиболее уязвимых. Отсутствие большого числа атак может указывать на наличие у хактивистов определенных этических границ, которым они пока следуют. Вместе с тем зафиксированы случаи атак на сетевые аптеки, что показывает: при дальнейшем обострении геополитической обстановки моральные ограничения могут быть легко вытеснены идеологическими мотивами.

Мишенями хактивистов нередко становятся организации, сбои в работе которых способны затронуть смежные сегменты экономики. Так, в начале сентября группировка C.A.S. заявила об ответственности за атаку на один из транспортных холдингов. Пострадавшая компания специализируется на перевозке промышленных грузов — угля, руды, металлов, нефтепродуктов, химикатов и стройматериалов — и сотрудничает с крупными промышленными предприятиями, экспортерами и подрядчиками. Кибератаки на подобные инфраструктурные узлы могут приводить к задержкам поставок энергоресурсов, металлов и других стратегически важных грузов, что превращает их в мощный инструмент давления и делает приоритетными целями для хактивистов.

Важно отметить, что в 2023-м и первой половине 2024 года больше всего атак со стороны хактивистов в России пришлось на телекоммуникационную отрасль (30%). За последний год доля хактивистских атак на этот сектор заметно сократилась — с 30% до 13%. На наш взгляд, это связано не столько с потерей интереса к отрасли, сколько с тем, что хактивисты ищут более «громкие» цели, которые соответствуют их геополитическим задачам. Кроме того, атаки на телеком оказались менее результативными в информационном плане: даже при временных перебоях связь быстро восстанавливалась, а резонанс был краткосрочным.

Госучреждения и промышленные предприятия аккумулируют массивы чувствительных данных. Их утечка создает большой инфоповод и позволяет дольше удерживать внимание аудитории. Таким образом, публикация похищенной информации вкупе с удалением или шифрованием данных в скомпрометированной инфраструктуре становится более эффективным инструментом давления, в отличие от сугубо деструктивных DDoS-атак на телеком.

Рисунок 31. Категории жертв среди организаций в успешных атаках хактивистов

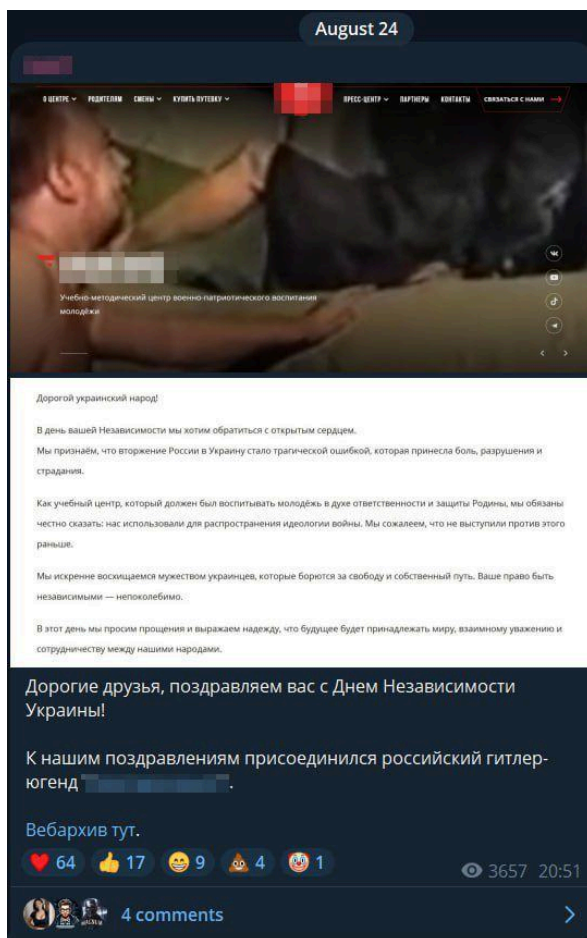


Кто стоит за хактивистскими атаками

Во второй половине 2024 года и в течение первых трех кварталов 2025-го организации в России стали мишенями не менее чем 18 хактивистских группировок. Их атаки составили в общей сложности 19% от всех зафиксированных в стране кибератак за этот период.

Веб-ресурсы остаются наиболее уязвимыми и удобными целями для хактивистов: в 53% зафиксированных случаев объектами атак становились именно они. Чаще всего злоумышленники ограничиваются дефейсом: изменяют главную страницу, размещают лозунги, символику или агитационные материалы. Такой подход не требует высокой технической подготовки, но позволяет быстро добиться заметного эффекта. Нередко подобные акции бывают привязаны к политическим событиям или историческим годовщинам.

Рисунок 32. Сообщение хактивистов о дефейсе сайта учебного центра патриотического воспитания



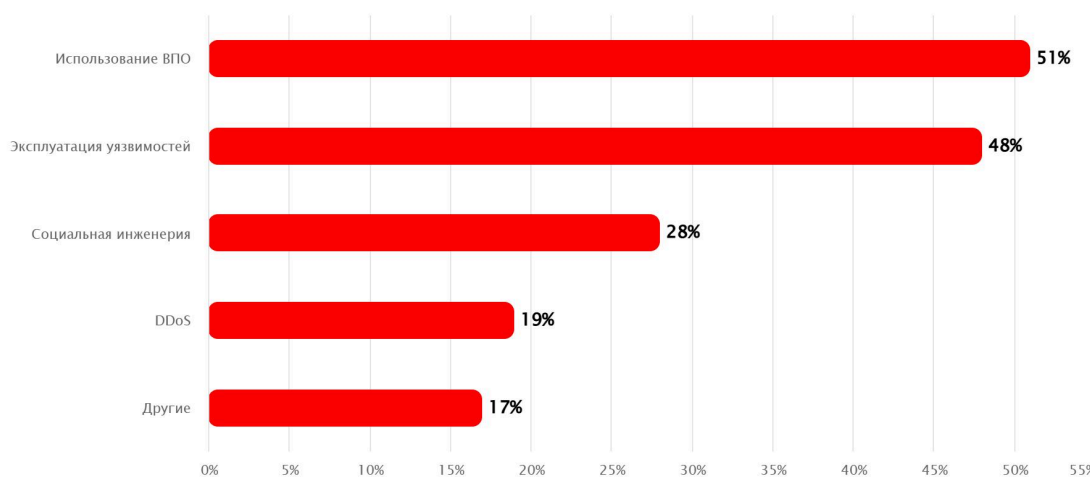
Как минимум 9 из 18 действующих группировок прибегают к подобному сценарию. При этом дефейс нередко становится лишь первым этапом атаки: используя уязвимости в веб-приложениях, устаревшие CMS и плагины, а также ошибки в конфигурации серверов, злоумышленники могут похищать базы данных, внедрять вредоносный код или использовать скомпрометированный ресурс для дальнейших атак. Хактивисты эксплуатировали уязвимости в каждой второй (48%) атаке.

По результатам тестов на проникновение, проведенных специалистами команды PT SWARM, в 60% векторов получения доступа во внутренние сети организации эксплуатировались именно уязвимости веб-приложений. С основными проблемами в системах кибербезопасности, выявляемыми в ходе работ по тестированию на проникновение и анализу защищенности веб-приложений, можно подробнее ознакомиться в разделе «Тайные ходы: проблемы в системах кибербезопасности российских компаний».

В 79% случаев успешные атаки хактивистов приводили к сбоям в основной деятельности организаций. При этом лишь 19% атак хактивистов были связаны с DDoS. Если еще несколько лет назад массовые отключения сервисов воспринимались как серьезный инцидент, то сегодня бизнес научился быстрее адаптироваться к подобным ситуациям. На первый план вышли более сложные сценарии: эксплуатация уязвимостей в приложениях и системах, внедрение вредоносного ПО, шифрование и уничтожение инфраструктуры. Эти методы позволяют не только вызывать кратковременные сбои, но и проникать во внутренние сети, похищать конфиденциальные данные и устанавливать контроль над IT-инфраструктурой.

Однако несмотря на то, что DDoS-атаки перестали быть основным методом хактивистов в России, отдельные регионы и отрасли продолжают регулярно сталкиваться с ними — прежде всего в связи с геополитической обстановкой. Так, в августе 2024 года операторы связи Курской области подверглись DDoS-атаке. Уже в октябре аналогичные действия были направлены, по данным СМИ, против информационных систем правительства региона: часть ресурсов администрации оказалась недоступной, а ответственность за кампанию взяла на себя группировка IT Army of Ukraine. В марте 2025 года фиксировалась новая серия атак — на ресурсы курских СМИ, при этом их продолжительность составила более двух суток.

Рисунок 33. Методы атак хактивистских группировок
(доля успешных атак)

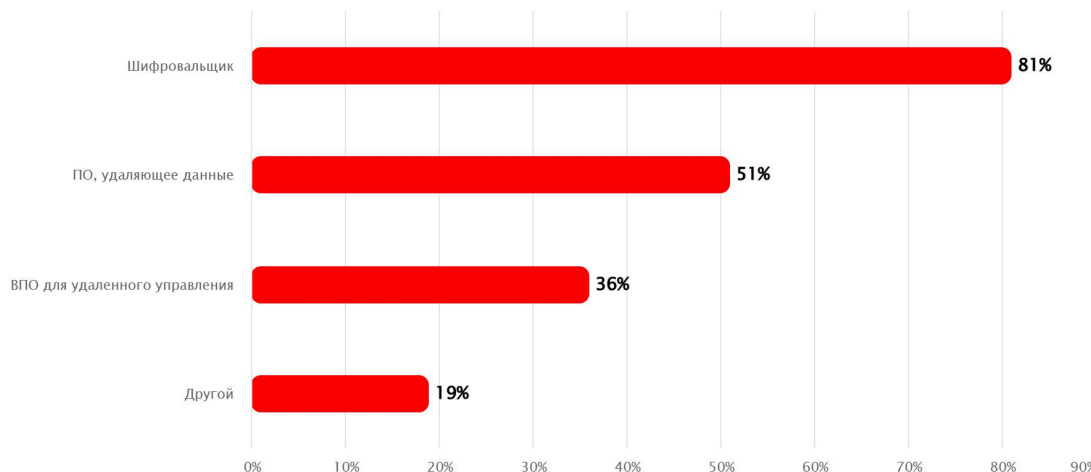


В 81% случаев хактивистских атак, где применялось вредоносное ПО, это были шифровальщики. Их используют не менее 9 из 18 исследованных хактивистских группировок. Как и в случае с финансово мотивированными злоумышленниками, речь идет преимущественно о шифровальщиках LockBit Black (3.0) и Babuk.

В каждой второй (51%) хактивистской атаке с использованием ВПО были задействованы специализированные инструменты для удаления данных (вайперы). Уничтожают данные в скомпрометированной инфраструктуре также не менее 9 из 18 группировок.

Хактивисты, действующие против российских организаций, чаще всего используют общедоступные утилиты. Это связано с тем, что использование общедоступного ПО снижает затраты на подготовку атак и позволяет быстро адаптироваться под разные цели. Однако ряд группировок создают или модифицируют инструменты под свои кампании. Такие разработки дают им ряд преимуществ: позволяют обходить средства защиты, повышают скрытность атак и делают их более целенаправленными. В числе таких группировок, например, Head Mare, «Киберпартизаны», Black Owl.

Рисунок 34. Типы ВПО, использованного в атаках хактивистов
(доля успешных атак с использованием ВПО)

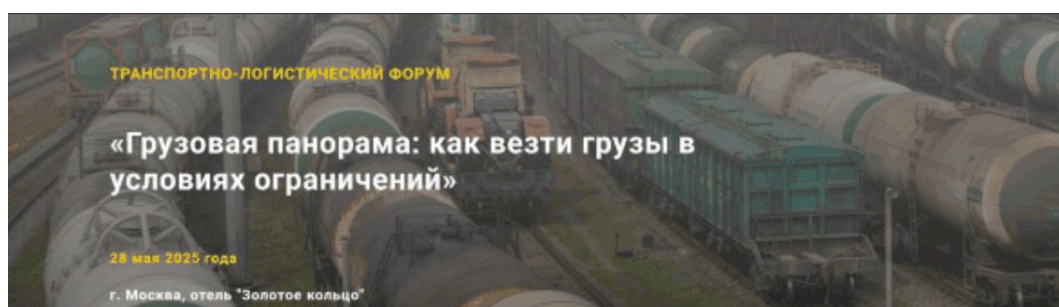


Black Owl

Впервые группировка заявила о себе в 2024 году через Telegram-канал, который ведет до сих пор, публикуя информацию об атакованных жертвах. Black Owl проводит деструктивные атаки исключительно на российские организации, применяя шифровальщик Babuk для Windows и ПО, предназначенное для удаления данных. Для проникновения в системы жертв преступники используют тщательно спланированный фишинг. Например, в конце мая 2025 года специалисты IT-департамента РТ ESC выявили кампанию, приуроченную к транспортно-логистическому форуму, в ходе которой злоумышленники зарегистрировали домены, имитирующие адрес сайта железнодорожной компании, а также создали документ, связанный с программой мероприятия.

Источник: РТ ESC

Рисунок 35. Документ-приманка группировки Black Owl



ПРОГРАММА ФОРУМА

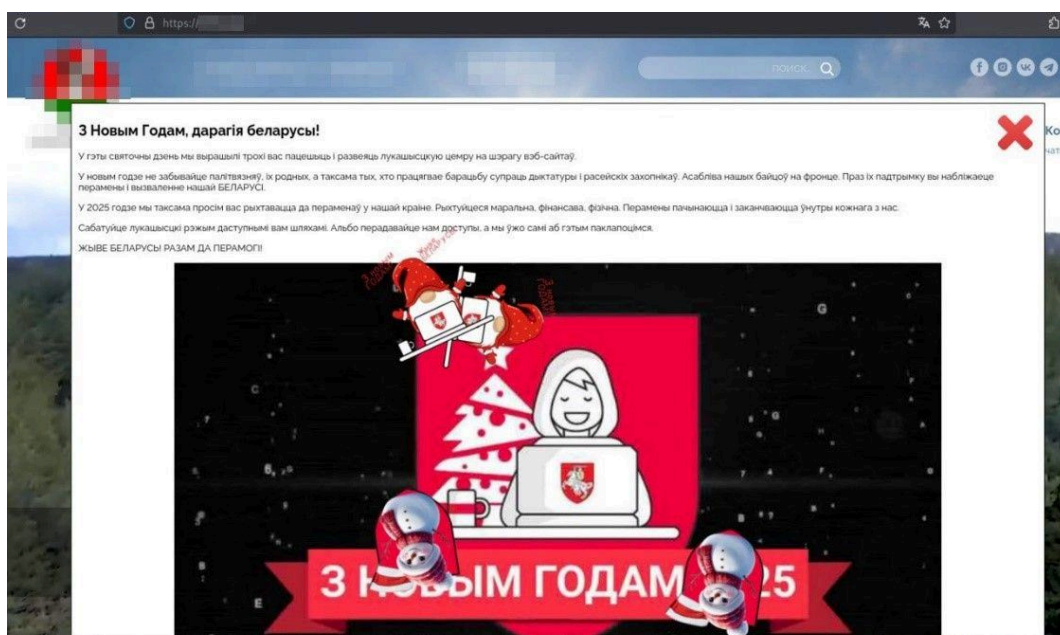
9:00 – 10:00	Регистрация участников, приветственный кофе
10:00 – 12:00	Дискуссия «Грузовая работа: как восстановить погрузку и привлечь дополнительные объемы?»
12:00 – 12:30	Кофе брейк
12:30 – 14:30	Дискуссия «Что делать рынку в условиях ограничений пропускной способности и нормирования перемещения вагонов?»
14:30 – 15:30	Обед
15:30 – 16:30	Доклады участников
16:30 – 17:00	Круглый стол

Темы дискуссий и круглого стола:

«Киберпартизаны»

Группировка «Киберпартизаны» впервые заявила о себе в 2020 году. Первоначально ее атаки были сосредоточены на белорусских организациях, однако со временем в список целей вошли и российские компании. Деятельность «Киберпартизан» характеризуется проведением резонансных кибератак, направленных на шифрование или уничтожение данных. Для этого в их арсенале имеется вредоносное ПО собственной разработки: бэкдоры, вайпер, инструменты для туннелирования трафика. Помимо этого они периодически осуществляют дефейс-атаки. Так, в конце 2024 года группа заявила о компрометации и изменении содержимого порядка десяти сайтов. О своих кампаниях и жертвах злоумышленники сообщают через собственный Telegram-канал.

Рисунок 36. Дефейс одного из сайтов, проведенный группировкой «Киберпартизаны»



Cyber Anarchy Squad (C.A.S.)

Группировка C.A.S. действует с 2022 года и специализируется на атаках против организаций в России и Белоруссии. В ходе атак злоумышленники крадут, шифруют или удаляют информацию, к которой удается получить доступ, чаще всего проникая в инфраструктуру жертв через уязвимости в публично доступных приложениях и сервисах.

Silent Crow

Группировка Silent Crow стала известна благодаря ряду известных атак, совершенных в 2024–2025 годах. Фокусируется на краже конфиденциальной информации, которую нередко публикует в своем Telegram-канале, а также на уничтожении данных. Активно взаимодействует с другими хактивистскими группами, например с «Киберпартизанами», — вместе они атаковали не только российские, но и белорусские учреждения.

HdrO

Объектом атак киберпреступников становятся сайты российских компаний из различных отраслей. Целью злоумышленников является хищение конфиденциальных данных и дефейс. Так, стало известно, что группировка опубликовала учетные данные к PhpMyAdmin сайта российской компании, специализирующейся на установке систем безопасности.

Какие факторы способствуют эскалации хактивизма в России

■ **Геополитическая напряженность.** Как мы уже отмечали, продолжительная геополитическая напряженность является одним из пяти ключевых драйверов кибератак в России. В отношении хактивизма этот драйвер имеет особо сильное влияние. Во время геополитической напряженности в России большинство хактивистских кампаний нацелено на нарушение бизнес-процессов. Многие коммерческие организации в стране прямо или косвенно связаны с государственными программами, ОПК или критической инфраструктурой. Однако даже атаки на формально «гражданский» сектор — розничную торговлю, промышленное производство, транспорт и логистику — способны оказывать косвенное, но ощутимое влияние на государственные ресурсы и возможности. Для хактивистов вмешательство в бизнес-процессы рассматривается не только как инструмент экономического ущерба, но и как средство стратегического давления.

■ **Низкий порог входа.** Росту хактивистской активности в России способствует низкий порог входа в проведение атак, в первую очередь DDoS. Его формирование связано с широкой доступностью инструментов для атак в открытых источниках. На специализированных форумах, в Telegram-каналах и даже в публичных репозиториях GitHub распространяются утилиты для генерации DDoS-трафика, скрипты для перебора учетных данных и эксплойты для эксплуатации уязвимостей в конкретных приложениях. Нередко такие инструменты сопровождаются подробной документацией и пошаговыми инструкциями, что делает их доступными даже для пользователей без практического опыта в сфере кибербезопасности.

Дополнительным фактором выступает координация политически мотивированных исполнителей более опытными кураторами. Участникам нередко предоставляют не только готовый набор инструментов, но и зашифрованные конфигурационные файлы, содержащие списки целей и сопутствующие метаданные. Такая организация позволяет оперативно масштабировать DDoS-кампании и заметно снижает технический барьер для новичков.

Существенным фактором также выступает сохранение анонимности за счет использования VPN, прокси-сервисов и криптовалютных платежных систем. Эти механизмы снижают вероятность деанонимизации и привлечения к ответственности: участие в массовых DDoS-атаках, дефейсах или иных акциях зачастую не влечет ощутимых юридических последствий. В результате многие участники воспринимают подобную активность как относительно безопасную форму выражения своих политических убеждений, что стимулирует дальнейшее вовлечение новых участников.

Низкий порог входа актуален не только для хактивизма, но и, в отдельных случаях, для кибершпионских операций. Так, специалисты группы киберразведки TI-департамента PT ESC выявили новый образец вредоносного ПО, названный PhantomGoShell, схожий с инструментами PhantomRAT и PhantomRShell из арсенала группировки PhantomCore. Анализ и последующее расследование показали, что за его использованием стояли малоопытные атакующие, в том числе несовершеннолетние. Они получили исходный код кастомного бэкдора, а также консультации по его использованию от более опытного участника PhantomCore, обладающего развитым киберкриминальным бэкграундом. Это наглядно иллюстрирует, насколько легко даже неопытные участники могут включиться в сложные атаки, опираясь на чужие наработки и наставничество из киберпреступного сообщества.

Выводы и прогнозы



В России по-прежнему высока активность кибершпионов, финансово мотивированных злоумышленников и хактивистов, регулярно выявляются новые группировки. Во втором полугодии 2024-го и в первых трех кварталах 2025 года на российские организации совершали кибератаки не менее 68 группировок с различной мотивацией. Все чаще фиксируются случаи, когда отнести ту или иную группу к определенной категории затруднительно: появляются гибридные формирования со смешанной мотивацией. Ряд злоумышленников, которые ранее только шифровали инфраструктуру, теперь начинают оставлять сообщения с требованиями выкупа. Готовность организаций идти на уступки вымогателям и платить приводит к масштабированию подобных операций и росту аппетитов финансово мотивированных злоумышленников.

Низкий порог входа в киберпреступность, особенно в сфере хактивизма и финансово мотивированных атак, способствует активному вовлечению новых лиц в киберпреступную деятельность, формированию новых группировок и созданию ответвлений уже существующих.

Основными векторами проникновения в корпоративную инфраструктуру по-прежнему остаются фишинговые рассылки, будь то сложные атаки Team46 с эксплойтами нулевого дня или действия Bloody Wolf, использующих JAR-архивы в связке с легитимным средством удаленного управления NetSupport. Также в качестве первоначальных векторов используются уязвимости в публичных приложениях, незащищенные службы удаленного доступа и скомпрометированные учетные данные подрядчиков. В арсенале кибершпионов нередко присутствует собственное уникальное вредоносное ПО, тогда как финансово мотивированные группировки и хактивисты чаще используют общедоступные инструменты и коммерческое вредоносное ПО, распространяемое на теневых ресурсах по модели malware as a service.

В 2026 году ожидается рост интереса к шантажу утечками персональных данных. С 30 мая 2025 года в России существенно увеличены штрафы за нарушения в обработке и защите персональных данных. Новые санкции по КоАП теперь могут достигать миллионов рублей. Если раньше возможные утечки воспринимались как управляемый риск (штрафы были относительно невелики), то теперь даже единичный инцидент может повлечь тяжелые финансовые последствия и повлиять на устойчивость бизнеса.

Ужесточение штрафов формирует благоприятную почву для вымогательских схем. Злоумышленники могут угрожать раскрытием факта нарушения или публикацией данных, обещая в случае отказа сообщить о нарушении в Роскомнадзор. Первые признаки тенденции уже проявились: в августе 2025 года группировка C.A.S. заявила о взломе платформы с базой инвестиционных проектов и предупредила о возможном штрафе в 20 миллионов рублей.

В зоне повышенного риска оказались прежде всего малые и средние предприятия (МСП). Здесь чаще встречаются неполные политики обработки персональных данных, устаревшее ПО, недостаточная сегментация внутренней сети. Кроме того, МСП могут быть более чувствительны к репутационным потерям и, как следствие, проще идти на уступки вымогателям, чтобы избежать проверок и крупных штрафов.

В 2026 году геополитика будет напрямую влиять на выбор приоритетных целей для кибершпионажа. В случае роста напряженности кибершпионы могут перераспределять ресурсы на наиболее приоритетные цели, в числе которых ОПК, государственные структуры и топливно-энергетический комплекс.

В условиях снижения политической напряженности основной фокус сместится в сторону экономической и технологической разведки — сбора информации о конкурентных отраслях, разработках в области IT и медицины. Приоритет получают атаки на научно-исследовательские организации, университеты, частные компании с уникальными технологиями и на стартапы. Методы атак при этом могут стать более скрытными и длительными. При отсутствии срочной необходимости в дестабилизации инфраструктуры злоумышленники будут делать ставку на невидимое присутствие в сетях, собирая данные месяцами и даже годами. Это позволит поддерживать постоянный информационный поток и быть готовыми к быстрой переориентации в случае изменения политической ситуации.

 **За ослаблением геополитической повестки последует переориентация хактивистов на финансово мотивированные атаки.** Активному росту хактивизма в России с 2022 года во многом способствовало массовое вовлечение в атаки малоквалифицированных, но легко поддающихся влиянию новичков. Их обучение и координацию взяли на себя более опытные кураторы: они создают инструкции по проведению атак и формируют закрытые сообщества, где эта деятельность активно популяризируется.

За несколько лет многие из участников накопили достаточно опыта, чтобы понять: их навыки можно использовать не только в хактивизме, но и для получения прямой финансовой выгоды. Отсюда возникает закономерный вопрос — куда будет направлена их активность после снижения геополитической напряженности? Наиболее вероятно, что значительная часть переключится на вымогательство, и уже сейчас некоторые из них совмещают его с политически мотивированными атаками. Аналогичная перспектива ожидает и их кураторов: потеряв внешний стимул в виде геополитической повестки, они также будут искать новые источники дохода.

Сегодня мы наблюдаем переходный этап: бывшие новички уже перестали быть дилетантами, но пока не достигли уровня профессиональных киберпреступников. Тем не менее они осознают свои возможности, и как только внешняя мотивация ослабнет, ожидается резкий рост финансово мотивированных кампаний. Причем в первую очередь мишенью, вероятнее всего, станут именно российские организации, так как особенности их инфраструктуры уже детально изучены и отработаны в ходе хактивистской активности.



В течение следующих пяти лет ожидается рост применения ИИ в кибершпионаже и атаках с финансовой мотивацией. В ближайшие годы технологии искусственного интеллекта будут играть все более заметную роль в кибершпионских и финансово мотивированных атаках против организаций в России. Машинное обучение позволит злоумышленникам автоматизировать широкий спектр задач — от сбора разведывательных данных и подготовки фишинговых кампаний до анализа инфраструктуры жертвы и поиска уязвимостей. Уже сегодня генеративные модели используются для создания персонализированных фишинговых писем, имитации переписки сотрудников и генерации реалистичных голосовых или видеосообщений (дипфейков), что значительно повышает эффективность социальной инженерии.

В кибершпионаже ИИ может помочь атакующим быстрее выявлять слабые места в системах защиты, анализировать большие объемы сетевого трафика и незаметно извлекать конфиденциальные данные. В финансово мотивированных кампаниях — повышать эффективность вымогательства, подбирать оптимальные тактики давления на бизнес и автоматизировать переговоры с жертвами.

Характерным примером стала серия атак, описанная в отчете Threat Intelligence Report: August 2025 компании Anthropic. В нем рассказывается, как финансово мотивированные злоумышленники использовали Claude Code для автоматизации всех этапов атаки против не менее чем 17 организаций: от сканирования интернет-узлов и поиска точек входа до подготовки персонализированных вымогательских записок. Эти сообщения формировались на основе анализа похищенных данных, включая финансовые показатели компаний, численность сотрудников и особенности отраслевого законодательства, что делало угрозы злоумышленников максимально релевантными и убедительными.

В целом, использование ИИ в кибершпионаже и финансово мотивированных атаках становится закономерным этапом эволюции киберугроз. Для бизнеса и государственных структур в России это означает необходимость учитывать новые технологии в сценариях угроз и корректировать стратегии информационной безопасности с учетом их потенциального воздействия.



Инфраструктура умных городов станет новой точкой давления хактивистов. В России развиваются проекты умных городов, автоматизации транспортных узлов и цифровизации производства. К примеру, развитие концепции умных городов в России является частью национального проекта «Цифровая экономика». Технологии умных городов могут стать привлекательной целью для хактивистских кибератак.

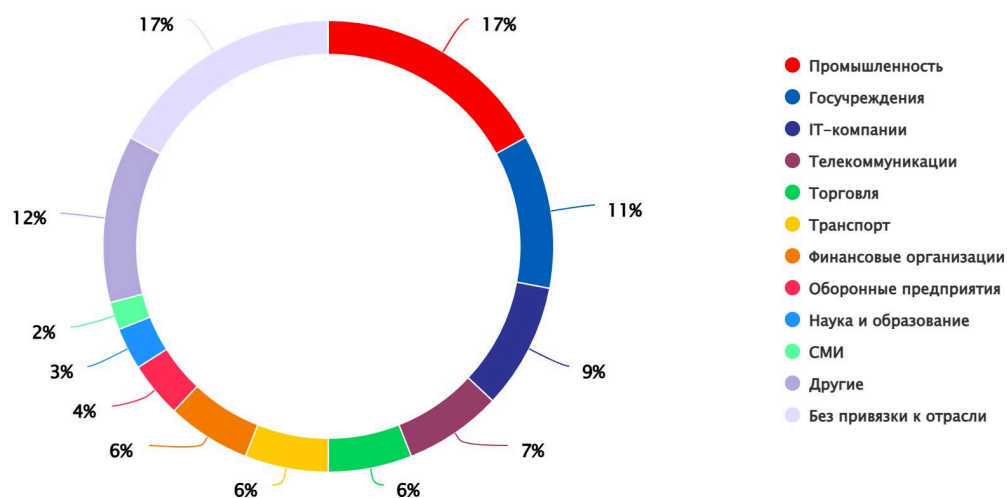
Для хактивистов это направление особенно привлекательно по нескольким причинам. Во-первых, взлом IoT-устройств может привести к ощутимым последствиям. Если сейчас DDoS-атаки и дефейсы сайтов редко затрагивают более одной организации, то в умных городах многие системы объединены в общую сеть, что при взломе одной подсистемы может дать доступ к другим. В результате кибератака может привести к отключению электроэнергии, остановке транспорта, сбоям в медицинских системах или даже аварии на производстве. Во-вторых, эффект от таких атак легко сделать заметным — отключение отопления или водоснабжения в городе моментально привлекает внимание СМИ и усиливает общественный резонанс. Наконец, многие умные устройства строятся на одинаковых аппаратных и программных решениях, что делает массовые кибератаки относительно дешевыми и быстрыми в реализации.

В центре шахматной партии: какие отрасли под особым прицелом



Во второй половине 2024-го и первых трех кварталах 2025 года наибольшее количество кибератак пришлось на промышленные организации (17%), государственный сектор (11%), IT-компании (9%) и телекоммуникации (7%). Чтобы сформировать целостное представление об отраслевом ландшафте киберугроз, рассмотрим ключевые факторы, привлекающие внимание злоумышленников к каждой из этих сфер, и проанализируем характерные особенности кибератак.

Рисунок 37. Категории жертв среди организаций





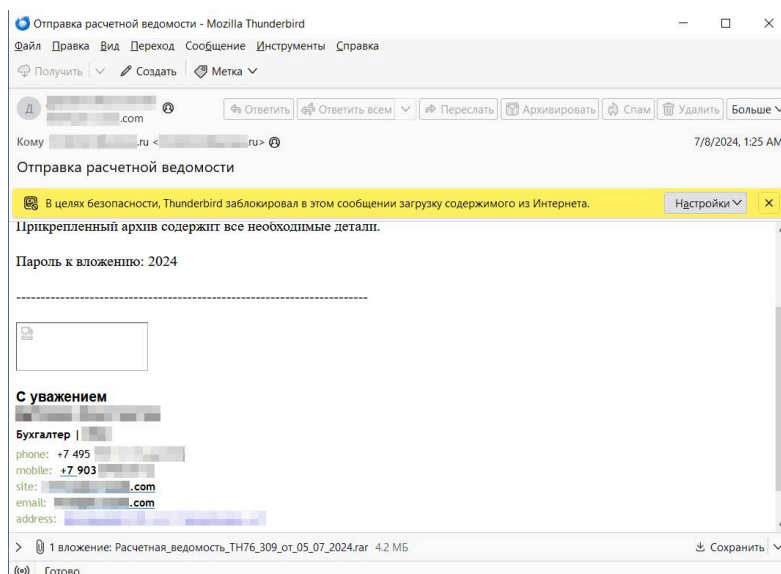
Во второй половине 2024-го и в течение 2025 года промышленные и производственные предприятия стали главной целью киберпреступников, обогнав по числу атак даже государственный сектор. На их долю пришлось 17% всех атак, что на 6 п. п. выше показателя 2023 года и первой половины 2024-го. Важность этого сектора объясняется его ключевой ролью не только в экономике, но и в обеспечении государственных интересов, поскольку он связан с ценными технологиями, разработками и уникальными ноу-хау.

Большие объемы данных о технологиях, производственных процессах и научных разработках делают промышленные предприятия одной из ключевых целей кибершпионов. В рассматриваемый период 37% успешных атак на этот сектор были совершены кибершпионскими группировками. В числе наиболее активных, атаковавших промышленность, можно выделить PhantomCore, PseudoGamaredon, GOFEE, XDspy, ExCobalt. Всего же на отрасль совершали атаки не менее 17 из 22 кибершпионских группировок, атакующих российские организации.

Для получения первоначального доступа злоумышленники чаще всего прибегали к фишинговым рассылкам. Тематика заголовков и вложений в таких письмах, как правило, напрямую связана с рабочей деятельностью адресатов. Например, в одной из кампаний, зафиксированной специалистами PT ESC в III квартале 2024 года, группировка PhantomCore рассылала письма с вложениями в виде расчетных ведомостей. Архив, приложенный к письму, эксплуатировал уязвимость [PT-2023-4552 \(CVE-2023-38831\)](#). В свою очередь, в I квартале 2025 года группировка Telemancon использовала приманку, связанную с деятельностью органов власти, рассылая письма с якобы официальными указаниями от имени ФСТЭК России.

Источник: PT ESC

Рисунок 38. Пример фишингового письма группировки PhantomCore, направленного в адрес российского завода



Методы социальной инженерии использовались в 69% кибератак на российский промышленный сектор. Этот способ киберпреступники могут применять, например, для получения учетных данных жертвы. В одной из кампаний, зафиксированной специалистами PT ESC, злоумышленники отправили фишинговое письмо в адрес компании топливно-энергетического сектора. В письме содержалось HTML-вложение с формой для ввода логина и пароля. Полученные данные могли быть использованы как для дальнейшего развития атаки внутри инфраструктуры жертвы, так и для последующей продажи на теневых форумах.

Источник: PT ESC

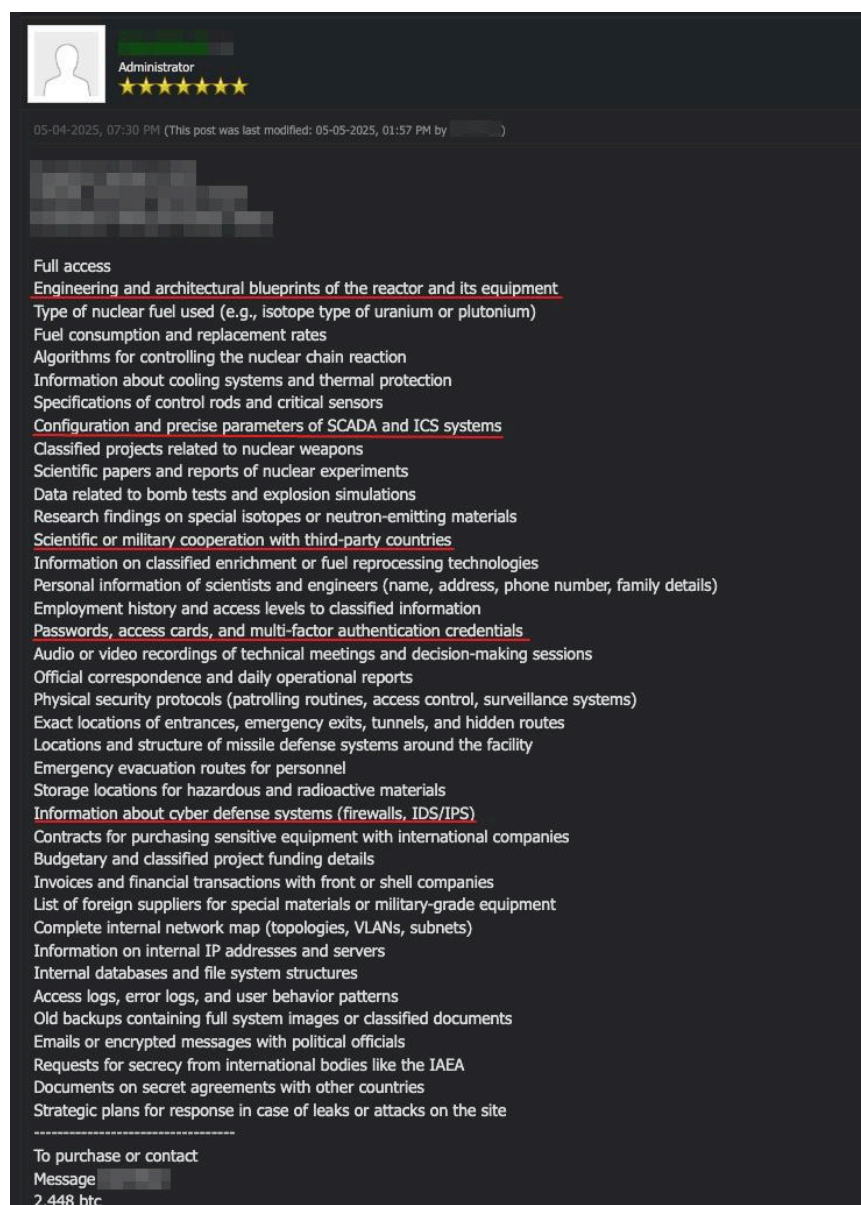
Рисунок 39. Форма для кражи учетных данных из фишингового письма в адрес организации топливно-энергетического сектора



Восемь из десяти атак (79%) на промышленность были совершены с применением вредоносного ПО. В 50% таких атак использовалось ВПО для удаленного управления, в 41% — шифровальщики. Кибератаки вызвали нарушения в работе предприятий в 38% случаев, часть из которых была связана с атаками группировок, использующих шифровальщики.

В 61% успешных кибератак на промышленные организации была похищена конфиденциальная информация. На специализированных дарквеб-площадках, где публикуются утечки данных, самая высокая заявленная стоимость набора информации, связанной с промышленным сектором, достигала 2,448 BTC (около 300 тыс. долларов США). По утверждению продавца, в архиве содержались отчеты экспериментов, персональные данные, учетные записи с паролями, протоколы совещаний, внутренние отчеты, финансовая документация, схемы охраны, планы расположения объектов, маршруты эвакуации, сведения о системах кибербезопасности, внутренние IP-адреса, переписка и даже стратегические планы реагирования.

Рисунок 40. Объявление о продаже данных, похищенных из промышленной организации



The image is a screenshot of a dark web marketplace listing. At the top, there is a profile picture of a person and the title 'Administrator' with five yellow stars. Below this, the date '05-04-2025, 07:30 PM' and a note '(This post was last modified: 05-05-2025, 01:57 PM by [redacted])' are visible. The main content is a list of stolen data items, many of which are underlined. The list includes: 'Full access', 'Engineering and architectural blueprints of the reactor and its equipment', 'Type of nuclear fuel used (e.g., isotope type of uranium or plutonium)', 'Fuel consumption and replacement rates', 'Algorithms for controlling the nuclear chain reaction', 'Information about cooling systems and thermal protection', 'Specifications of control rods and critical sensors', 'Configuration and precise parameters of SCADA and ICS systems', 'Classified projects related to nuclear weapons', 'Scientific papers and reports of nuclear experiments', 'Data related to bomb tests and explosion simulations', 'Research findings on special isotopes or neutron-emitting materials', 'Scientific or military cooperation with third-party countries', 'Information on classified enrichment or fuel reprocessing technologies', 'Personal information of scientists and engineers (name, address, phone number, family details)', 'Employment history and access levels to classified information', 'Passwords, access cards, and multi-factor authentication credentials', 'Audio or video recordings of technical meetings and decision-making sessions', 'Official correspondence and daily operational reports', 'Physical security protocols (patrolling routines, access control, surveillance systems)', 'Exact locations of entrances, emergency exits, tunnels, and hidden routes', 'Locations and structure of missile defense systems around the facility', 'Emergency evacuation routes for personnel', 'Storage locations for hazardous and radioactive materials', 'Information about cyber defense systems (firewalls, IDS/IPS)', 'Contracts for purchasing sensitive equipment with international companies', 'Budgetary and classified project funding details', 'Invoices and financial transactions with front or shell companies', 'List of foreign suppliers for special materials or military-grade equipment', 'Complete internal network map (topologies, VLANs, subnets)', 'Information on internal IP addresses and servers', 'Internal databases and file system structures', 'Access logs, error logs, and user behavior patterns', 'Old backups containing full system images or classified documents', 'Emails or encrypted messages with political officials', 'Requests for secrecy from international bodies like the IAEA', 'Documents on secret agreements with other countries', and 'Strategic plans for response in case of leaks or attacks on the site'. At the bottom, there is a section 'To purchase or contact:' followed by 'Message [redacted]' and '2.448 btc'.

Administrator
★★★★★

05-04-2025, 07:30 PM (This post was last modified: 05-05-2025, 01:57 PM by [redacted])

Full access
Engineering and architectural blueprints of the reactor and its equipment
Type of nuclear fuel used (e.g., isotope type of uranium or plutonium)
Fuel consumption and replacement rates
Algorithms for controlling the nuclear chain reaction
Information about cooling systems and thermal protection
Specifications of control rods and critical sensors
Configuration and precise parameters of SCADA and ICS systems
Classified projects related to nuclear weapons
Scientific papers and reports of nuclear experiments
Data related to bomb tests and explosion simulations
Research findings on special isotopes or neutron-emitting materials
Scientific or military cooperation with third-party countries
Information on classified enrichment or fuel reprocessing technologies
Personal information of scientists and engineers (name, address, phone number, family details)
Employment history and access levels to classified information
Passwords, access cards, and multi-factor authentication credentials
Audio or video recordings of technical meetings and decision-making sessions
Official correspondence and daily operational reports
Physical security protocols (patrolling routines, access control, surveillance systems)
Exact locations of entrances, emergency exits, tunnels, and hidden routes
Locations and structure of missile defense systems around the facility
Emergency evacuation routes for personnel
Storage locations for hazardous and radioactive materials
Information about cyber defense systems (firewalls, IDS/IPS)
Contracts for purchasing sensitive equipment with international companies
Budgetary and classified project funding details
Invoices and financial transactions with front or shell companies
List of foreign suppliers for special materials or military-grade equipment
Complete internal network map (topologies, VLANs, subnets)
Information on internal IP addresses and servers
Internal databases and file system structures
Access logs, error logs, and user behavior patterns
Old backups containing full system images or classified documents
Emails or encrypted messages with political officials
Requests for secrecy from international bodies like the IAEA
Documents on secret agreements with other countries
Strategic plans for response in case of leaks or attacks on the site

To purchase or contact:
Message [redacted]
2.448 btc

Нарастающий масштаб атак на промышленные предприятия отражает системную трансформацию ландшафта киберугроз. Если ранее злоумышленники ориентировались преимущественно на государственные структуры, то сегодня промышленность становится не менее значимой целью. Это связано с возрастающей цифровизацией производственных процессов и активным внедрением IoT-устройств, что расширяет поверхность атаки и повышает вероятность успешных компрометаций.

Кроме того, интерес к промышленным данным объясняется их стратегической ценностью: утечка технологической информации может напрямую влиять на конкурентоспособность компаний и даже на обороноспособность государства. Участвовавшие кейсы с применением вымогательского ПО и дальнейшей монетизацией похищенных данных показывают, что угрозы приобретают комплексный характер, объединяя кибершпионаж, финансовую мотивацию и элементы хактивизма.

Рисунок 41. Сводная статистика по промышленности





За последние годы государственные учреждения остаются одной из наиболее привлекательных целей для киберпреступников по всему миру, и Россия не является исключением. В условиях глобализации, технологического прогресса и растущей зависимости от цифровой инфраструктуры госсектор оказывается в эпицентре киберугроз.

В министерствах, ведомствах и госкорпорациях хранится и обрабатывается критически важная информация: данные о внешней политике, оборонных проектах, переговорах, внутренней безопасности. Это делает их приоритетной целью для различных категорий злоумышленников: кибершпионов (46% от всех успешных кибератак на госучреждения), хактивистов (31%) и финансово мотивированных групп (7%).

Более половины (61%) успешных атак на государственные структуры осуществлялись с применением вредоносного ПО, в первую очередь средств удаленного управления (55% всех успешных атак на госучреждения с использованием ВПО). Этот тип вредоносного ПО позволяет злоумышленникам сохранять устойчивый доступ к скомпрометированным устройствам, вести разведку, контролировать действия жертв и использовать зараженные системы как точку входа для последующих атак. В отдельных случаях доступ поддерживается годами: так, с помощью GoblinRAT киберпреступники не менее трех лет шпионили за российскими ведомствами.

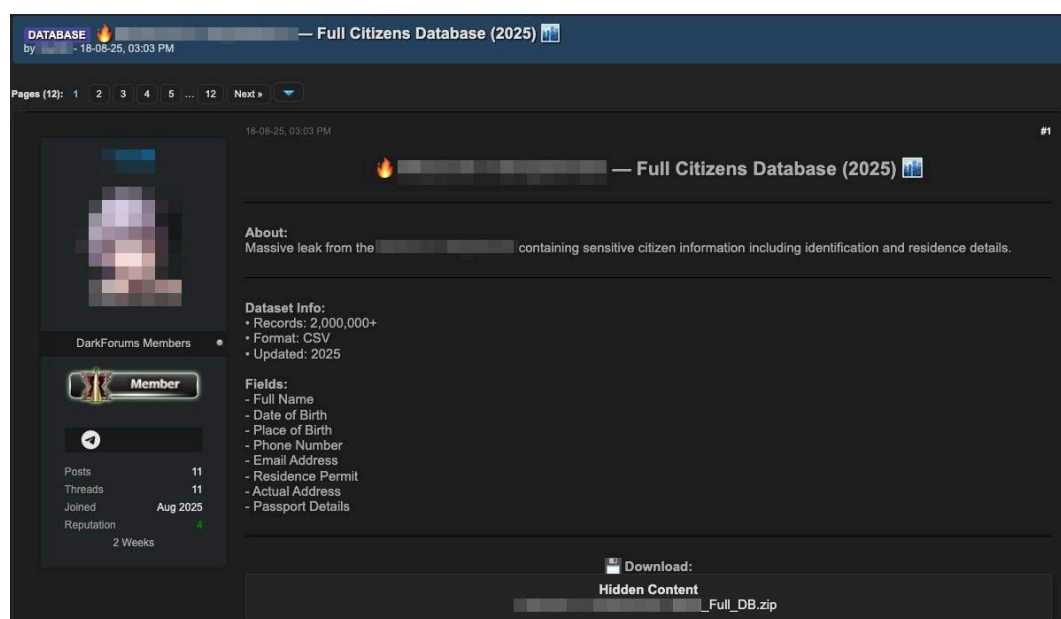
Вторым по частоте использования в атаках на государственные учреждения стало шпионское ПО (36%), что напрямую связано с преобладанием кибершпионских атак на государственный сектор. Так, группировка PhantomCore применяет собственные инструменты PhantomStealer и PhantomRAT, а в кампании, обнаруженной специалистами PT ESC, группировка TA Tolik использовала стилер Unicorn, дополненный функцией кражи файлов с расширениями, характерными для военной топографии.

Каждый шестой инцидент (17%) в государственных учреждениях был связан с DDoS-атаками, всплеск которых часто приходится на значимые политические или социальные события. Например, по данным СМИ, в день саммита БРИКС интернет-ресурсы МИД России подверглись атаке, из-за чего работа сайта была временно нарушена. Этот метод нередко используют хактивисты как инструмент давления, привлечения внимания или дестабилизации.

Государственные учреждения располагают значительным объемом как конфиденциальной информации о гражданах и предприятиях, так и данных, затрагивающих национальную и государственную безопасность. Успешные атаки на госорганизации приводили к компрометации данных в 63% случаев. Кражей информации занимаются все категории злоумышленников, включая хактивистов и финансово мотивированные группировки. Украденные данные чаще всего распространяются через теневые ресурсы: в 44% объявлений, связанных с утечками из российских организаций, данные раздавались бесплатно, в 37% — были выставлены на продажу.

Наибольшим спросом пользуются персональные данные (79% всех объявлений о бесплатной раздаче или продаже), в том числе паспортные и иные идентификационные сведения. Так, на одном из дарквеб-форумов была опубликована база с информацией более чем о двух миллионах жителей российского города, включая Ф.И.О. и паспортные данные. Подобные утечки представляют ценность на подпольном рынке, так как могут использоваться для мошенничества и кражи личности. Средняя цена в объявлениях о продаже данных из госучреждений составляет 225 долларов.

Рисунок 42. Объявление о бесплатной раздаче базы данных с информацией о жителях одного из российских городов



В 39% успешных кибератак на госучреждения наносился ущерб интересам страны, треть инцидентов (33%) приводили к нарушению работы госучреждений. Так, по данным СМИ, в начале октября киберпреступники совершили атаку на один из государственных сервисов, из-за которой оказались недоступны интернет-ресурсы российских судов, включая личные кабинеты сотрудников и систему интернет-телефонии. Полное восстановление заняло около месяца. При этом телефония судов, по данным СМИ, функционировала на устаревшем сервисе Lync от Microsoft, давно снятом с поддержки. После инцидента для судебной системы было закуплено несколько сотен отечественных серверов.

По результатам тестов на проникновение, проведенных специалистами команды PT SWARM, устаревшие версии программного обеспечения были обнаружены в 80% компаний. С другими проблемами в системах кибербезопасности, выявленными в ходе работ по тестированию на проникновение и анализу защищенности веб-приложений, можно подробнее ознакомиться в разделе «Тайные ходы: проблемы в системах кибербезопасности российских компаний».

Кибератаки на российские государственные учреждения отражают общую мировую тенденцию: госсектор остается приоритетной целью для кибершпионажа и хактивизма. Наибольшие риски связаны с компрометацией данных и подрывом функционирования ключевых сервисов, что напрямую влияет на устойчивость государственных систем. Для снижения угроз необходим комплексный подход: модернизация инфраструктуры, развитие национальных решений в области ИБ, внедрение системного мониторинга и повышение уровня цифровой грамотности сотрудников.

Рисунок 43. Сводная статистика по госучреждениям





IT-компании занимают третье место по числу успешных кибератак на российские организации, на их долю приходится 9%. Наибольший интерес к этому сектору проявляют кибершпионы (30%) и хактивисты (32%); доля успешных финансово мотивированных атак составила 25%.

Сегодня IT-сектор обеспечивает широкий спектр ключевых услуг: облачные решения и хостинг, системы удаленного администрирования, корпоративные приложения и многое другое. Именно поэтому компании этой отрасли нередко становятся «трамплином» для атак на другие организации: злоумышленники могут внедрить вредоносный код в программное обеспечение или похитить учетные данные для доступа к системам сотен и даже тысяч клиентов.

Для кибершпионов это возможность охватить широкий круг целей и получить доступ к массивам ценной информации, включая данные государственных структур и промышленных предприятий. Для хактивистов — шанс нанести удар по максимально большому числу организаций. Дополнительный интерес к российскому IT-сектору связан и с активным развитием отечественных решений. Так, специалисты PT ESC зафиксировали фишинговую кампанию против дистрибьютора российского ПО, конечной целью которой было заражение жертвы ВПО для удаленного управления DarkGate. Программы для удаленного управления применялись в половине (50%) успешных атак с использованием ВПО на IT-компании, позволяя злоумышленникам длительно удерживать доступ к устройствам и похищать данные как самих компаний, так и их клиентов.

Источник: PT ESC

Рисунок 44. Письмо, отправленное в рамках вредоносной кампании по распространению DarkGate

From: Юлия Прохорова <yulija.prohorova@promautomatic.ru>
Sent: Tuesday, June 11, 2024 11:06 PM
To: [REDACTED]
Subject: Вопрос по программной продукции Р7-Офис

Добрый день,

Компания «Промышленная Автоматизация» выполняет широкий комплекс работ на производстве в различных отраслях промышленности. Интересует приобретение лицензий Р7-Офис. Профессиональный. На сайте производителя указано, что вы являетесь партнером. Я могу отправить описание задачи и получить коммерческое предложение?

С уважением,
Юлия Прохорова.
Специалист по снабжению,
ООО «Промышленная Автоматизация»

Почти половина (48%) успешных атак на IT-компании приводили к сбоям в их работе. Последствия таких инцидентов могут выйти далеко за пределы самой компании: под угрозой оказываются клиенты, зависящие от ее инфраструктуры и программных решений. Это делает сектор особенно привлекательным для хактивистов. Как пишут СМИ, в результате атаки группировки Yellow Drift на одну из электронных торговых площадок по всей стране были приостановлены торги, что вызвало жалобы участников тендера на поставку оборудования для государственных нужд Санкт-Петербурга и повлекло остановку поставок.

Для проникновения в IT-компании злоумышленники нередко используют человеческий фактор: в 57% случаев применялись методы социальной инженерии, в частности направленные на разработчиков. Эта тенденция отмечалась еще в III квартале 2024 года. Для распространения вредоносного ПО киберпреступники активно задействуют менеджеры пакетов (PyPI, npm) и популярные сервисы, такие как GitHub. Например, специалисты PT ESC обнаружили вредоносные пакеты deepseek и deepseekai, загруженные в PyPI, среди пользователей которых оказались и российские компании.

К утечке конфиденциальной информации привели 61% успешных атак на IT, нередко затрагивая и сторонние организации. Так, в результате атаки на платформу автоматизации маркетинга Mindbox в сеть утекло более 5,6 млн строк данных, связанных с клиентами Burger King.

При этом три четверти (77%) публикаций в дарквебе, связанных с IT-компаниями, касаются бесплатной раздачи украденных данных, что подчеркивает хактивистскую направленность многих атак. Самая крупная из выявленных баз — более 10 ТБ персональных сведений, учетных данных и внутренних файлов — была выложена в открытый доступ для всех желающих.

Таким образом, IT-компании в России остаются не просто одними из самых частых целей атак, но и наиболее чувствительными к их последствиям. Взлом таких организаций несет риски не только для самих компаний, но и для десятков отраслей экономики, зависящих от их сервисов. Это делает необходимость укрепления киберзащиты IT-сектора стратегическим приоритетом для всей страны.

Рисунок 45. Сводная статистика по IT-компаниям





В течение второй половины 2024-го и в первых трех кварталах 2025 года доля атак на телекоммуникационную отрасль снизилась с 10% до 7%. Внимание злоумышленников смещается на B2B-направление телеком-операторов. Многие из них развивают IT- и облачные сервисы для корпоративных клиентов — предоставляют дата-центры, виртуальные серверы, облачные хранилища, почтовые и CRM-системы. Эти сервисы активно используют финансовые организации, промышленные предприятия и государственные структуры, что делает их привлекательной целью: атака на телеком в роли провайдера IT-услуг автоматически открывает доступ ко множеству организаций. Кроме того, внедрить вредоносный код или похитить учетные данные в облачном сегменте зачастую проще, чем атаковать физическую инфраструктуру связи. Таким образом, снижение числа атак на «классический» телеком не означает потери интереса к отрасли. Фокус смещается на облачные и корпоративные сервисы, где злоумышленники могут получить больший охват и больше возможностей для компрометации.

В то же время операторы связи продолжают оставаться привлекательной целью для хактивистских атак. На долю хактивистов пришлось 49% всех успешных атак на телеком в рассматриваемый период. Для подобных группировок решающим фактором является не столько финансовая выгода, сколько максимальный общественный резонанс. Нарушение работы телекоммуникационных компаний может затронуть миллионы пользователей одновременно, вызвав перебои в работе интернета, мобильной связи, онлайн-сервисов и государственных порталов.

Прежде всего, к сбоям в работе интернет-провайдеров приводят DDoS-атаки — с ними связаны более половины (57%) успешных кибератак в секторе телекоммуникаций. Чаще всего мишенью становятся региональные операторы, не располагающие комплексными средствами защиты от подобных атак. Так, по данным СМИ, с ними сталкивались провайдер Приморья VladLink, петербургский AirNet, а также крымские и херсонские мобильные операторы, в результате чего на проблемы с интернет-доступом пожаловались не менее 20 тыс. пользователей.

Важно отметить, что DDoS-атаки, особенно на крупные телеком телекоммуникационные компании, вызывают не только проблемы с интернетом и мобильной связью, но и каскадные сбои в смежных системах, нарушая бизнес-процессы клиентов пострадавших компаний. Так, инцидент с оператором АСВТ привел к отключению банковских терминалов, а домофоны могли работать лишь в механическом режиме. В другом случае, при атаке на оператора Lovit, обслуживающего жилые комплексы компании ПИК, вышли из строя отдельные системы «умных зданий», что затруднило жителям доступ в квартиры и на парковки. Кроме того, были парализованы магазины в жилых комплексах: из-за сбоя перестали функционировать кассы.

Помимо DDoS-атак, серьезные сбои в работе телеком-операторов вызывают успешные атаки с применением вредоносного ПО, на их долю приходится более трети (34%) инцидентов. Так, по данным СМИ, в январе 2025 года была полностью выведена из строя инфраструктура одного из российских провайдеров: по заявлениям киберпреступников, были похищены конфиденциальные документы и уничтожены все данные со взломанных систем.

Храня и обрабатывая огромные массивы информации, телеком-компании становятся особенно привлекательной целью: 31% успешных атак на этот сектор приводили к утечкам данных. При этом на теневых форумах подавляющее большинство (76%) объявлений связано с бесплатной раздачей украденной информации, что отражает хактивистскую направленность атак. Чаще всего в свободный доступ попадают персональные данные (95%), преимущественно похищенные у региональных операторов. Крупнейшая из раздаваемых баз содержала около 9,4 млн строк с персональными данными пользователей. Наибольшую стоимость (1360 долларов) имел архив объемом около 50 ГБ. В нем содержались полные пользовательские профили, включающие персональные сведения, хешированные пароли, финансовую информацию, а также ряд технических данных.

Рисунок 46. Объявление о продаже базы данных телекоммуникационной компании

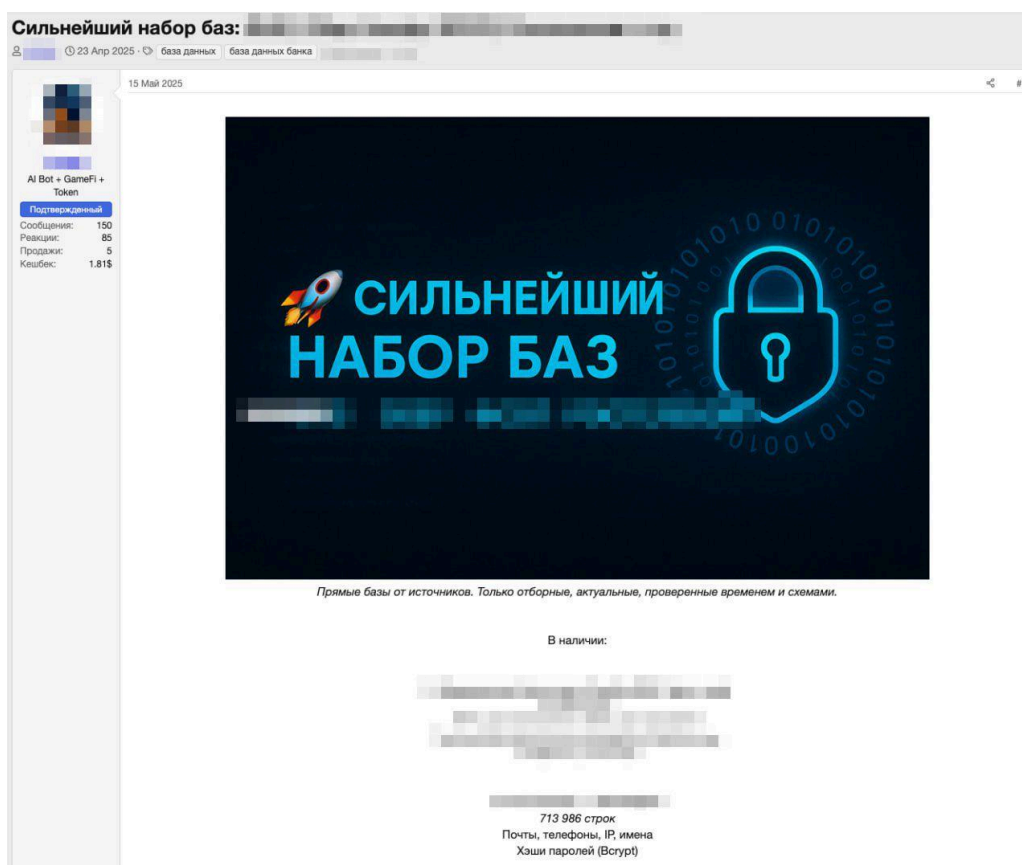


Рисунок 47. Сводная статистика по телекоммуникациям



Выводы и прогнозы

 **Промышленность, госучреждения, IT и телеком — ключевые мишени кибератак.** Сегодня мы наблюдаем отраслевую трансформацию ландшафта киберугроз: если ранее злоумышленники в основном фокусировались на госструктурах, то сегодня не менее значимой целью становится промышленность. Большие объемы данных о технологиях, производственных процессах и научных разработках сделали промышленность приоритетной целью кибершпионов — практически каждая кибершпионская группировка, атакующая Россию, предпринимала хотя бы одну попытку скомпрометировать инфраструктуру промышленного предприятия. Активная цифровизация, внедрение IoT-устройств и расширение IT-инфраструктуры увеличивает поверхность атаки, а следовательно, и вероятность успешных компрометаций.

Кибератаки на государственные учреждения России вписываются в общемировую тенденцию: госсектор остается приоритетной целью кибершпионажа и хактивизма. В 39% успешных атак на госучреждения наносился ущерб интересам страны, и треть атак привели к нарушению работы госучреждений. Основные риски — утечка чувствительных данных и подрыв устойчивости государственных систем.

Российские IT-компании остаются не только одними из самых частых мишеней, но и наиболее уязвимыми к последствиям атак. Компрометация IT-компании может повлечь риски для десятков других организаций, зависящих от ее продуктов и услуг. Для кибершпионов это возможность получить доступ к массивам ценной информации, включая данные госсектора и промышленности. Для хактивистов — способ нанести удар по широкому кругу целей. Дополнительный интерес к IT-сектору подпитывается курсом на импортозамещение и активным развитием отечественных разработок.

Не менее чувствительна к последствиям кибератак и телекоммуникационная отрасль. Крупные телеком-компании предоставляют облачные и IT-сервисы корпоративным клиентам из множества отраслей, становясь узловыми точками интереса. Это делает их привлекательной целью как для кибершпионов, так и для хактивистов. Таким образом, компрометация телекоммуникационных компаний может иметь эффект домино — одна успешная атака способна повлечь за собой утечку данных и нарушение работы сразу нескольких секторов экономики. Надежная защита телеком-операторов становится критически важной для обеспечения киберустойчивости всей цифровой инфраструктуры страны.

 **Промышленность и госучреждения надолго сохраняют лидерство по интенсивности кибератак.** Промышленный сектор продолжит оставаться одной из ключевых целей киберпреступников, прежде всего из-за высокого интереса со стороны кибершпионских группировок. Предприятия этой сферы имеют доступ к крупным массивам ценной информации, а сбои в их работе способны привести не только к серьезным финансовым потерям, но и к техногенным катастрофам. Дополнительным фактором риска является высокая капитализация промышленных компаний, которая свидетельствует о наличии значительных финансовых ресурсов и повышает вероятность выплаты выкупа. Злоумышленники понимают, что ущерб от простоя или утечки данных многократно превышает размер выкупа, и рассчитывают, что организации предпочтут заплатить, нежели понести убытки. Эти обстоятельства превращаются в инструмент давления и вымогательства, поэтому снижение активности атакующих в этой сфере в 2026 году маловероятно.

Отдельный фактор угроз для промышленности и топливно-энергетического комплекса связан с активным внедрением технологий искусственного интеллекта. Несмотря на значительный потенциал для модернизации и повышения эффективности производства, ИИ-системы увеличивают поверхность атак и становятся привлекательными целями для злоумышленников.

В 2026 году госучреждения также останутся в числе основных мишеней злоумышленников. Высокая интенсивность атак на этот сектор сохранится даже в случае, если геополитический кризис пойдет на спад. Активность кибершпионских группировок, охотящихся за конфиденциальными данными государственных учреждений, не снизится: доступ к этой информации по-прежнему будет рассматриваться как важный инструмент политического и экономического влияния.

Кража конфиденциальной информации продолжит быть одним из наиболее распространенных последствий атак на госорганы. В условиях геополитической нестабильности ожидается рост числа утечек, инициируемых хактивистами, для которых такие инциденты служат инструментом привлечения внимания.

Дополнительным фактором риска остается использование устаревшего оборудования в ряде государственных систем. Массовый переход на отечественные решения также может повлечь новые уязвимости: интеграция новых технологий зачастую сопровождается «побочными эффектами», повышающими вероятность киберинцидентов.



В 2026 году интенсивность и характер атак на телеком будет варьироваться в зависимости от геополитической обстановки. На сегодняшний день атаки на телекоммуникационный сектор преимущественно носят хактивистский характер, а их интенсивность напрямую зависит от уровня геополитической напряженности. В случае ее снижения количество атак может существенно уменьшиться. DDoS-атаки в 2026 году полностью не исчезнут: они останутся актуальным инструментом давления, но будут чаще использоваться с целью получения выкупа за их прекращение.

При росте напряженности, напротив, стоит ожидать не только увеличения числа атак, но и их большей агрессивности. Региональные интернет-провайдеры обслуживают не только население, но и предприятия, для которых стабильный доступ к сети критически важен. В условиях сложной геополитической ситуации атаки на таких провайдеров становятся инструментом давления: отключение связи влияет не только на граждан, но и на устойчивость региональной экономики. Поэтому провайдеры все чаще становятся целью злоумышленников, стремящихся дестабилизировать ситуацию в стране. В первую очередь в зону риска попадут региональные интернет-провайдеры, не обладающие достаточными ресурсами для эффективной защиты.

Ускоряющаяся цифровизация усиливает значение телекоммуникационного сектора. Так, в 2024 году индекс «IQ городов», отражающий уровень внедрения цифровых решений в городское хозяйство, вырос на 11% по сравнению с 2023 годом и на 55% — относительно базового уровня 2018 года. Поскольку концепции умного города напрямую зависят от устойчивости телеком-инфраструктуры, атаки на этот сектор в горизонте нескольких лет могут стать инструментом воздействия не только на бизнес, но и на функционирование целых городских систем. активности.



IT-сектор России в ближайшие годы может стать одной из главных целей для кибератак наравне с промышленностью и госучреждениями. Его стремительное развитие неизбежно привлекает внимание злоумышленников. Сегодня основную долю инцидентов составляет хактивистская активность, обусловленная геополитической напряженностью. Однако при ее снижении можно ожидать роста числа кибершпионских кампаний.

Требования по импортозамещению и уход части иностранных вендоров вынуждают организации постепенно заменять привычные популярные решения на российские аналоги. Мы прогнозируем рост уровня интереса злоумышленников к решениям российских разработчиков. Атакующие уже начали исследовать эти решения на наличие уязвимостей, и в этой работе им могут поспособствовать утечки исходного кода продуктов. Поэтому стоит ожидать атак, которые будут нацелены на кражу исходного кода из IT-компаний, и в целом атак с использованием уязвимостей нулевого дня в ПО российских разработчиков.

Особую опасность представляют атаки на цепочки поставок и доверительные отношения, поскольку IT-компании тесно взаимодействуют с множеством отраслей. Как мы уже отмечали, такие атаки способны нанести ущерб сразу большому количеству организаций и потому будут оставаться ключевой целью для всех типов атакующих.

Дополнительный риск связан с использованием проектов open source. Злоумышленники продолжают использовать менеджеры пакетов для распространения вредоносного ПО, а также эксплуатируют уязвимости в решениях open source для проникновения в инфраструктуру компаний. По некоторым данным, около 30% российского ПО на базе открытого кода содержит критические уязвимости, что делает этот вектор одним из наиболее опасных.

A person wearing a black hoodie is shown in profile, looking down at a chessboard. Their hands are positioned over the pieces. The chessboard is illuminated with a strong red light, and the pieces are dark. In the background, the words "PT SWARM" are displayed in large, glowing red letters. The overall atmosphere is mysterious and high-tech.

PT
SWARM

Тайные ходы: проблемы
в системах кибербезопасности
российских компаний

Понимание всех этапов развития атаки — от первоначального доступа до сложных сценариев перемещения внутри сети и способов выгрузки данных — имеет ключевое значение для принятия обоснованных инвестиционных решений в сфере безопасности и эффективной защиты от постоянно расширяющейся и изменяющейся поверхности атак. Для комплексной оценки уровня защищенности необходимо учитывать как актуальные техники злоумышленников, так и слабые места в корпоративной инфраструктуре. В этом помогают тесты на проникновение (пентесты), автоматизированные пентесты, оценка устойчивости организации к кибератакам, участие в программах багбаунти и киберучения³.

³ Киберучения — это мероприятия по моделированию атак на организацию, в рамках которых проверяется актуальность и работоспособность процедур выявления атак, а также эффективность имеющихся планов, схем реагирования и мер по ликвидации последствий.

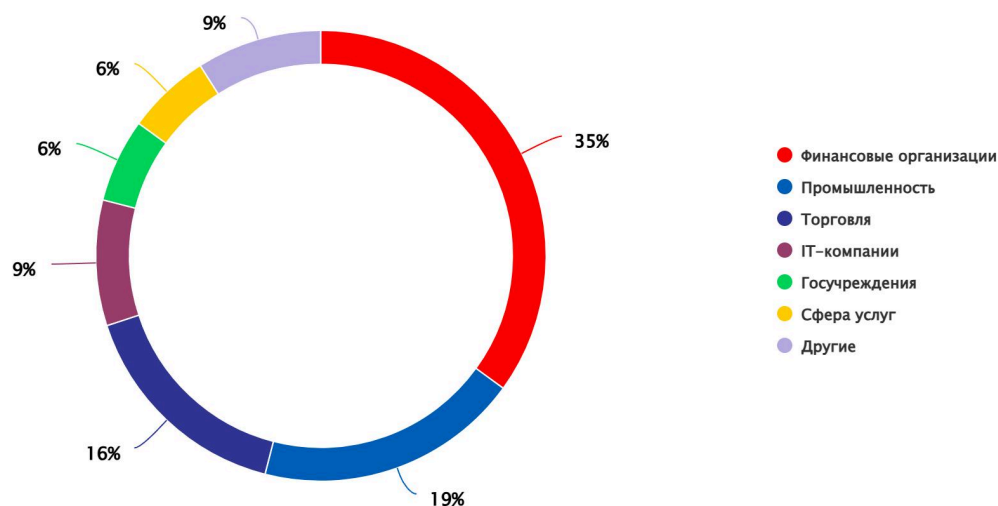
В этом разделе рассмотрены основные проблемы информационной безопасности, выявленные специалистами команды PT SWARM в ходе пентестов и проектов по анализу защищенности веб-приложений российских компаний во второй половине 2024 года и в первых трех кварталах 2025 года⁴.

⁴ Примеры использовавшихся специалистами PT SWARM тактик, техник и подтехник приведены в терминах MITRE ATT&CK Matrix for Enterprise. Качественный уровень риска обнаруженных уязвимостей оценивался экспертами с учетом оценки уровня рейтинга по системе CVSS v4.0: например, значения от 0,1 до 3,9 соответствуют низкому уровню риска, а от 9 до 10 — критическому. При этом, поскольку система CVSS носит универсальный характер и не учитывает специфику конкретных систем, специалисты Positive Technologies в ряде случаев корректировали итоговую качественную оценку риска.

Когда тестирование на проникновение проводится из внешних сетей (например, из интернета), его называют **внешним**. Основная цель внешнего пентеста — получение доступа к корпоративной сети.

Если моделируются атаки со стороны нарушителя, находящегося внутри компании (например, с типовым набором привилегий сотрудника или от лица случайного посетителя), то пентест принято называть **внутренним**. Его ключевая задача — достижение максимального уровня привилегий в инфраструктуре. Дополнительно заказчик может определить собственные цели пентеста — например, подтвердить возможность реализации недопустимого события.

Рисунок 48. Распределение протестированных организаций по отраслям



Чувствительные данные в открытом доступе

Один из первых шагов как при тестировании на проникновение, так и в реальной кибератаке на целевую организацию — это сбор информации о цели из открытых источников (open source intelligence, OSINT). Даже при массовых фишинговых рассылках злоумышленники нередко предварительно собирают данные об атакуемой социальной группе людей, чтобы сделать приманки более правдоподобными и, следовательно, более эффективными.

При целевых атаках на конкретную компанию или сотрудника OSINT позволяет получить точную и релевантную информацию, которую впоследствии можно использовать для развития атаки. Так, специалисты PT SWARM в ходе пентестов российских компаний неоднократно обнаруживали данные, потенциально пригодные для последующих этапов атаки, в том числе учетные записи и пароли, хранившиеся в свободном доступе.

Таблица 1. Основные источники OSINT и соответствующие им типы информации, выявленные в ходе тестирования российских компаний на проникновение

Источник	Возможная информация
Открытые репозитории кода	Исходные коды приложений и сервисов, описание используемого стека технологий (языки программирования, фреймворки, библиотеки), идентификаторы пользователей, сохраненные в коде учетные данные, имена и IP-адреса внутренних серверов и сервисов
Документация на официальных ресурсах	Описание используемого стека технологий и схем сети, упоминания внутренних сервисов, а также описание процессов и процедур информационной безопасности
Резюме сотрудников и вакансии	Сведения о применяемом стеке технологий, перечень используемых инструментов и программного обеспечения, а также персональные данные сотрудников (Ф.И.О., должность, контакты, опыт работы)
Фотографии из офиса	Визуальное подтверждение используемых технологий (названия ПО или сервисов на экранах, оборудование, схемы на досках), что позволяет определить технический стек компании

Важно отметить, что OSINT относится к пассивному сбору информации, то есть без прямого обращения к инфраструктуре компании. Для пассивного сбора информации используются публичные веб-службы, WHOIS, службы DNS и другие методы. Собранные с помощью пассивного анализа данные могут помочь атакующим составить приблизительную карту узлов внешнего периметра, определить наиболее приоритетные векторы компрометации, а также показать возможные дополнительные сценарии, расширяя поверхность атаки. Не менее значима и стадия активной разведки, когда специалисты исследуют сетевой периметр — определяют открытые порты и доступные на них сервисы, версии ПО, механизмы аутентификации и другое.

Особенно опасно, если на этапе разведки удастся обнаружить учетные данные. В сочетании с недостаточно частым обновлением паролей и отсутствием или неэффективной реализацией многофакторной аутентификации (MFA) это создает условия для прямого доступа к инфраструктуре. Проблемы с MFA были обнаружены в 8% проектов по анализу защищенности веб-приложений и в 52% тестов на проникновение. Отсутствие дополнительных факторов аутентификации позволяет злоумышленнику, получившему учетные данные посредством OSINT или других методов, напрямую подключаться к узлам сети, сервисам, приложениям на периметре и к внутренней сети через корпоративную VPN-службу.

Многофакторную аутентификацию рекомендуется использовать для защиты любых сервисов на периметре компании, а также для критичных внутренних сервисов, компрометация которых может привести к недопустимым событиям и нанести значительный ущерб организации. Советуем придерживаться общих рекомендаций по реализации MFA.

Рисунок 49. Возможный вектор проникновения в корпоративную инфраструктуру с использованием полученных в результате OSINT данных при отсутствии MFA



В ближайшем будущем к данным, собираемым на этапе разведки, все чаще будут добавляться аудио- и видеозаписи сотрудников, которые могут использоваться для проведения атак методами социальной инженерии с применением дипфейков. При этом в зоне риска окажутся как руководители компании, так и рядовой персонал — например, сотрудники отдела безопасности или HR.



Извечная проблема паролей

Пароли остаются одним из самых уязвимых звеньев в защите на всех уровнях корпоративных систем. Даже если на этапе разведки не удастся найти действующие пары логин-пароль, по найденным образцам учетных данных атакующий может получить представление о принципах формирования логинов и корпоративных почтовых адресов.

Это значительно упрощает процесс подбора учетных записей. Например, если из открытых источников становится понятно, что логины формируются по шаблону имя-фамилия@company.ru, то, имея список сотрудников, злоумышленник может сгенерировать десятки или даже сотни корректных адресов. При слабой парольной политике это создает предпосылки для потенциальной компрометации привилегированных учетных записей и развития атаки внутри инфраструктуры.

Проблемы с реализацией парольной политики выявлены у 97% протестированных компаний, при этом у 70% из них уровень риска, связанный с паролями, был оценен как критический.

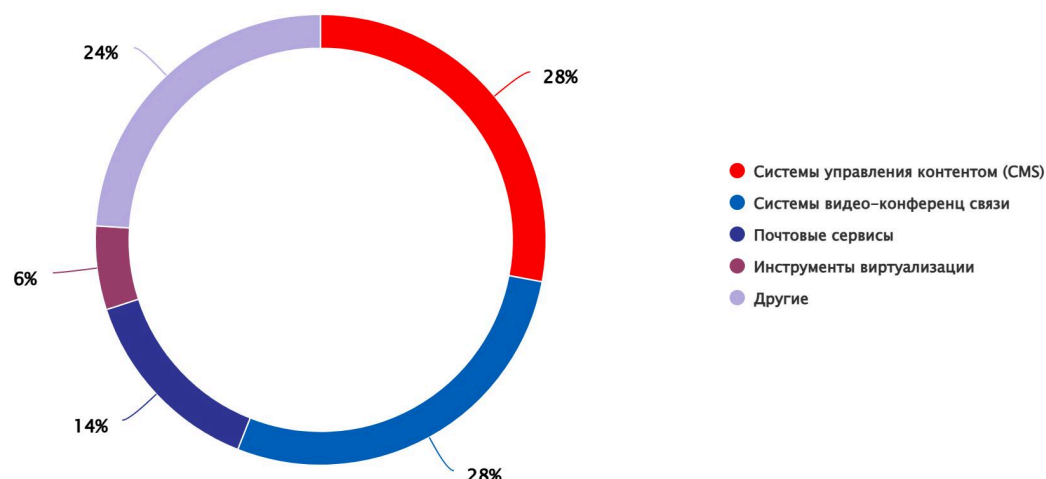
Из года в год исследования подтверждают популярность простейших комбинаций вроде «123456», «qwerty» и «password». Не теряют актуальности и другие типовые ошибки при создании и использовании учетных данных. Специалисты PT SWARM выявили весь спектр стандартных проблем с паролями во время внешних и внутренних пентестов российских компаний:

- пароли по шаблону «название компании + год + спецсимвол»;
- одинаковые логин и пароль;
- слишком короткие пароли;
- словарные комбинации (например: Qq123456, 12345678, 1234asd);
- использование паролей по умолчанию без изменений;
- повторное использование одинаковых паролей для разных сервисов и приложений.

Простые и предсказуемые пароли особенно уязвимы для атак методом перебора «грубой силой» (T1110 Brute Force), включая:

- атаку с распылением паролей — подстановку одного и того же пароля в различные учетные записи (T1110.003 Password Spraying);
- восстановление исходных паролей из данных, например хешей (T1110.002 Password Cracking);
- перебор по словарю (T1110.001 Password Guessing);
- атаку с применением готовых списков учетных данных (T1110.004 Credential Stuffing).

Рисунок 50. Подтехники Brute Force, применявшиеся в тестах на проникновение



Парольная политика должна распространяться на все узлы сети без исключения и включать следующие требования:

- минимальная длина пароля — не менее 15 символов;
- использование символов верхнего и нижнего регистра, цифр и спецсимволов;
- запрет на повторение хотя бы пяти последних паролей, чтобы исключить риск использования данных из прошлых утечек.

Также необходимо предотвращать использование предсказуемых комбинаций, формально соответствующих правилам, например «название компании + год». Советуем придерживаться полного перечня общих рекомендаций по созданию и применению надежных паролей.

Проникновение в корпоративную инфраструктуру

Получение доступа во внутреннюю сеть организации — один из ключевых этапов многих кибератак. Именно с него начинаются векторы реализации широкого спектра недопустимых событий: от хищения конфиденциальных данных до нарушения работы производственных систем.

Торговля первоначальными доступами к корпоративным системам стала распространенной и прибыльной сферой в теневом сегменте киберпреступности. Эту нишу на киберпреступном рынке занимают так называемые брокеры первоначального доступа — злоумышленники, которые специализируются на поиске и продаже доступов в корпоративные сети. Подробно их деятельность мы рассматривали в исследовании «Рынок киберпреступности».

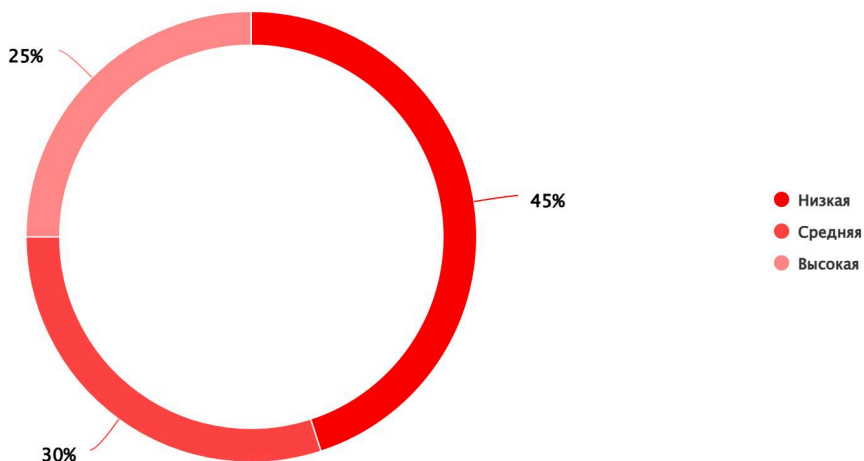
Результаты внешнего тестирования на проникновение показали: во внутреннюю сеть удалось попасть в 89% протестированных компаний. Еще в 3% случаев продвижение остановилось после получения доступа в демилитаризованную зону (ДМЗ). При этом в 57% протестированных организаций для получения доступа в корпоративную сеть достаточно вектора низкой сложности⁵.

Шаг атаки — отдельное, завершенное действие, которое позволяет получить информацию или привилегии, необходимые для дальнейшего развития атаки. Например, подбор учетных данных приложения или эксплуатация уязвимости.

Вектор атаки — последовательность шагов атаки, приводящая к определенному результату. Например, к получению доступа в корпоративную инфраструктуру, к получению максимальных привилегий в домене, к реализации недопустимого события.

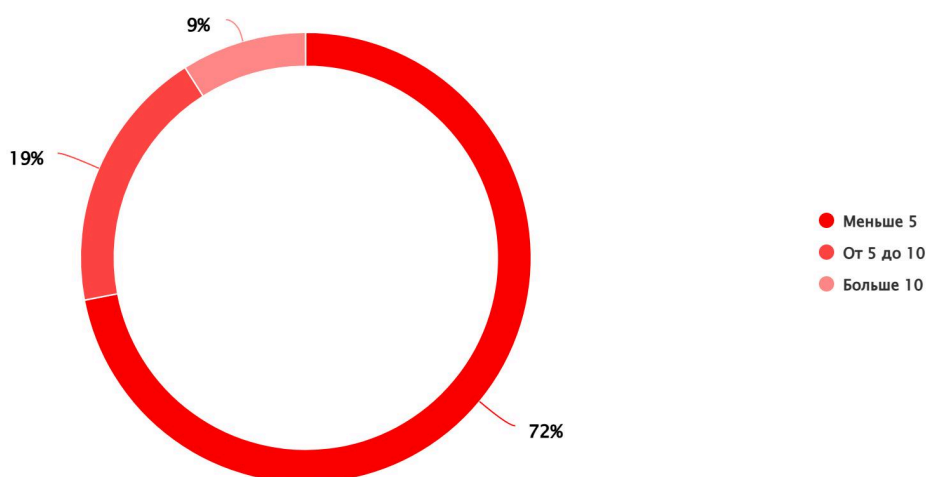
⁵ Сложность вектора определяется числом шагов и требуемой квалификацией. К вектору низкой сложности относят действия, которые может выполнить злоумышленник с минимальной подготовкой, применяя общедоступные инструменты для анализа защищенности и автоматизации атак и готовые эксплойты.

Рисунок 51. Сложность выявленных векторов получения доступа в корпоративную инфраструктуру (доля векторов)



В 72% случаев векторы получения доступа к корпоративной инфраструктуре включали менее пяти шагов. Более того, каждый пятый (19%) вектор состоял всего из одного шага.

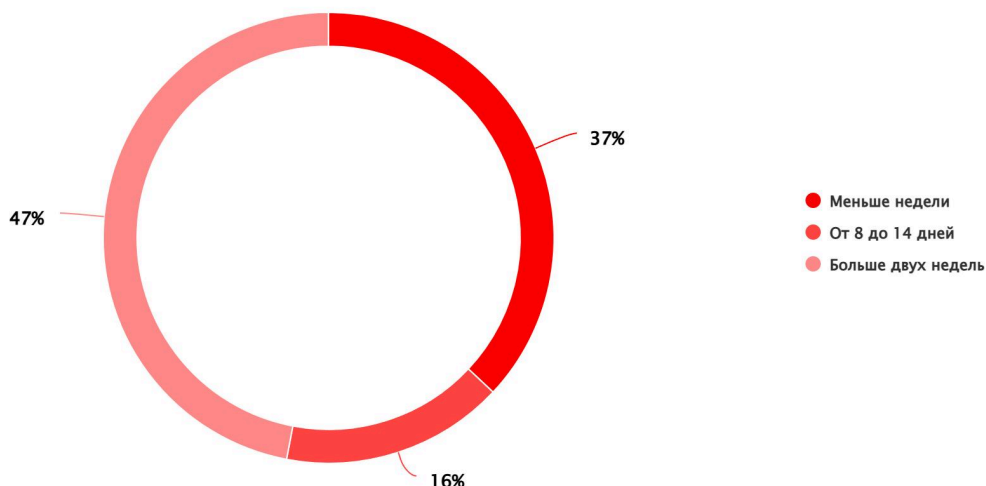
Рисунок 52. Количество шагов в выявленных векторах получения доступа в корпоративную инфраструктуру (доля векторов)



Время, которое требовалось специалистам PT SWARM на проникновение в корпоративную инфраструктуру⁶, зависело от множества факторов – уровня защищенности компании, размера тестируемого периметра и других параметров. Минимальное время, потребовавшееся для получения доступа с момента начала работ, составило всего два дня.

⁶ При расчете учитываются все этапы: сбор информации, подготовка атаки и реализация вектора доступа в корпоративную сеть.

Рисунок 53. Время до получения доступа к корпоративной инфраструктуре при внешнем тестировании на проникновение (доля проектов)



Основными причинами успешного проникновения в корпоративную инфраструктуру в ходе тестирования на проникновение стали слабые пароли, уязвимости веб-приложений, небезопасные настройки сервисов, а также человеческий фактор и недостаточная эффективность организационных мер защиты.

Проблемы веб-приложений и сервисов на периметре компании

Корпоративные веб-приложения, доступные из интернета, по-прежнему остаются одним из основных каналов проникновения в корпоративную инфраструктуру. В ходе внешних тестов на проникновение специалисты PT SWARM использовали уязвимости веб-приложений в 60% векторов получения доступа во внутреннюю сеть компаний.

В ходе проектов по анализу защищенности веб-приложений специалисты Positive Technologies выявили ряд типовых уязвимостей, эксплуатация которых может приводить к компрометации внутренних систем.

Наиболее распространенной уязвимостью веб-приложений российских компаний в рассматриваемый период стала недостаточная авторизация (CWE-863), ее доля составила 32% от всех выявленных уязвимостей. При этом для каждой второй (50%) такой уязвимости степень риска была оценена как высокая. Некорректная проверка прав доступа пользователя может приводить к утечкам конфиденциальных данных (46% обнаруженных уязвимостей), в том числе учетных и персональных, а также к несанкционированному использованию функциональных возможностей (42% обнаруженных уязвимостей). В ряде случаев это позволяло повысить привилегии до уровня суперпользователя, что фактически означало полный захват веб-приложения.

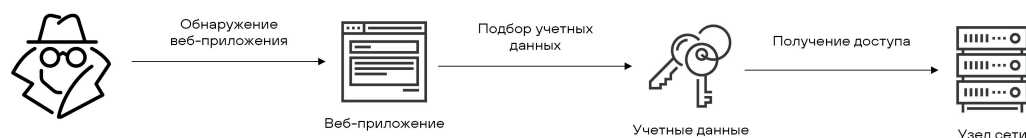
К уязвимостям с высоким уровнем риска также относятся те, что позволяют злоумышленнику выполнять произвольные команды на сервере веб-приложения. В их число входит, например, внедрение SQL-кода (CWE-89) и удаленное выполнение кода (CWE-94). Несмотря на сравнительно небольшую долю (9% от всех выявленных уязвимостей), эти ошибки представляют критическую угрозу безопасности и требуют первоочередного устранения.

Рисунок 54. Возможный вектор получения доступа к корпоративной сети



Значительная доля выявленных уязвимостей связана с недостатками парольной политики. Так, отсутствие защиты от подбора учетных данных (CWE-307) выявлено в каждом третьем (33%) протестированном приложении. Кроме того, в 12% приложений специалисты PT SWARM обнаружили хранение паролей в открытом виде (CWE-256).

Рисунок 55. Возможный вектор получения доступа к корпоративной сети



Каждая шестая уязвимость (16%), выявленная специалистами PT SWARM, связана с раскрытием конфигурационной информации веб-приложений — например, версий фреймворков и баз данных, отображаемых в HTTP-ответах сервера или сообщениях об ошибках. Подобные уязвимости могут стать источником чувствительной информации для злоумышленников.

Важно учитывать, что веб-приложение может выступать не только промежуточным звеном атаки на корпоративную инфраструктуру, но и являться самостоятельной целью киберпреступников. Злоумышленники могут провести дефейс веб-ресурса с целью нанесения репутационного ущерба или использовать его для дальнейших атак на пользователей. Наиболее распространенными в этой категории оказались уязвимости межсайтового выполнения сценариев (CWE-79), которые составили 59% от всех выявленных случаев.

Помимо веб-приложений, на периметре компании киберпреступники могут эксплуатировать уязвимости сторонних сервисов и решений.

Рисунок 56. Типы программных продуктов на внешнем сетевом периметре, в которых были выявлены уязвимости (доля типов продуктов)

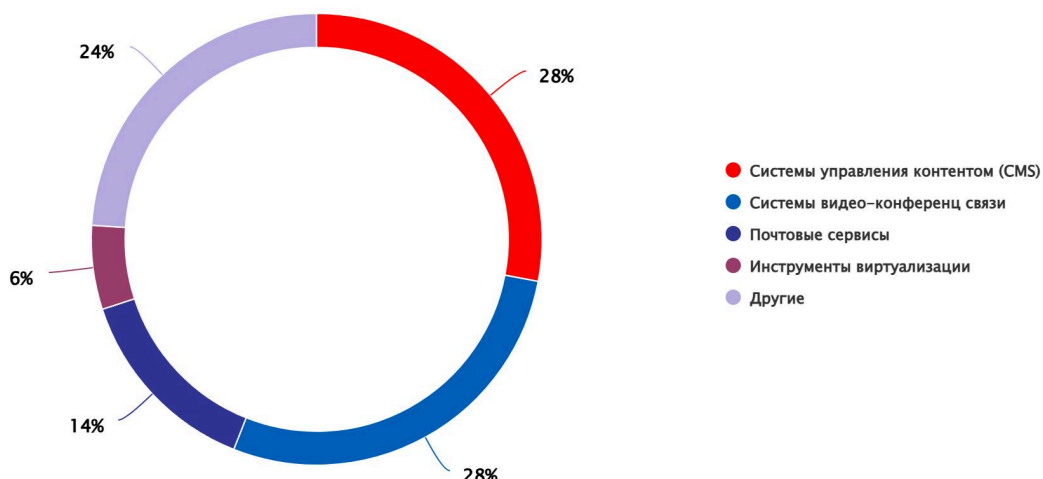
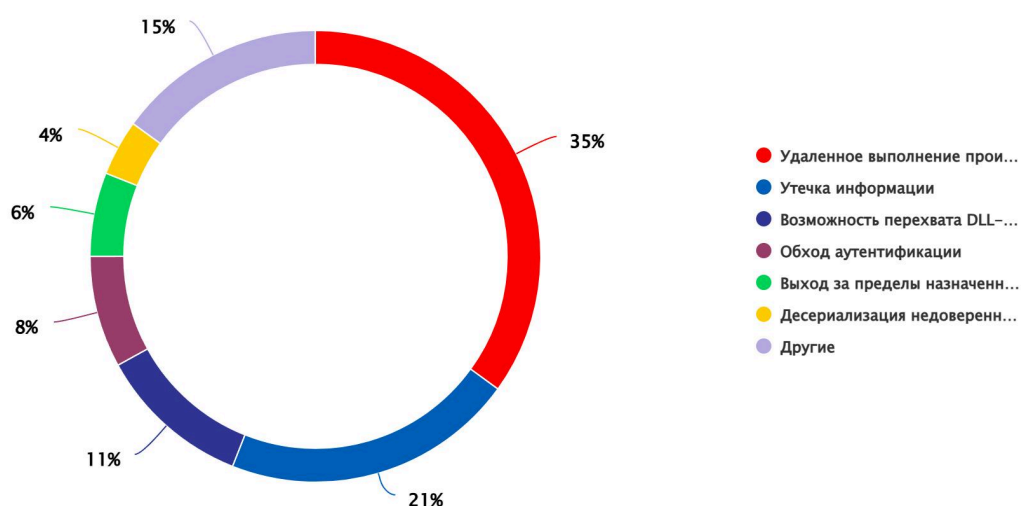


Рисунок 57. Типы уязвимостей, обнаруженных в программных продуктах на внешнем сетевом периметре (доля уязвимостей)



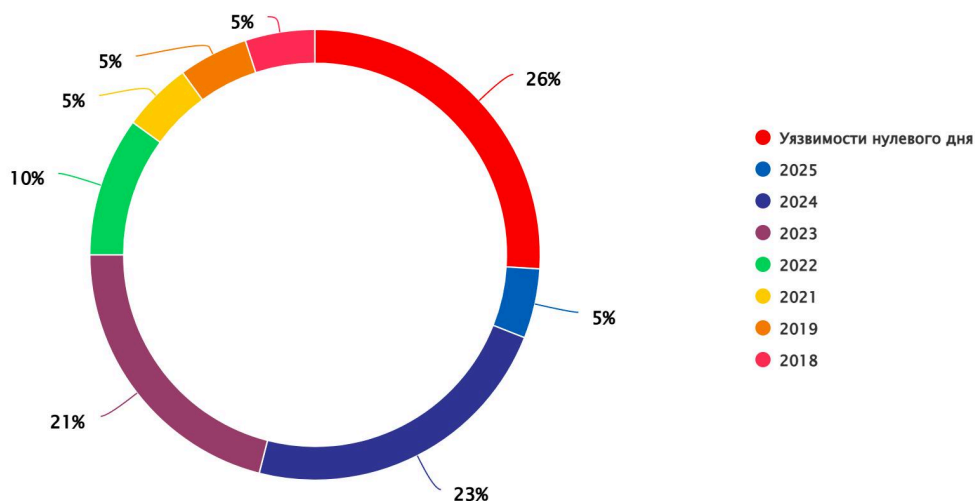
Для программных продуктов, доступных на внешнем сетевом периметре (см. рисунок 56), характерны проблемы, связанные с отсутствием своевременных обновлений. Они были выявлены в 80% компаний. При этом в каждой третьей (30%) компании угроза эксплуатации известных уязвимостей в таком ПО оценивалась как критическая.

Рисунок 58. Возможный вектор получения доступа к корпоративной сети в случае возможности загрузки веб-интерпретатора



Среди выявленных уязвимостей были как уязвимости нулевого дня, так и давно известные, причем некоторые из них сохраняют актуальность еще с 2018 года.

Рисунок 59. Распределение выявленных в ходе внешних пентестов уязвимостей по году публикации (доля уязвимостей)

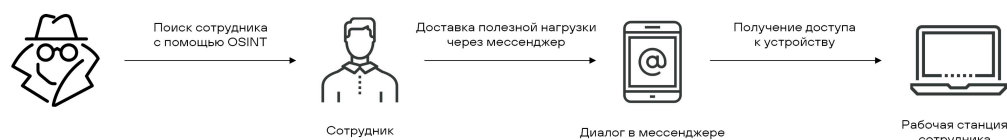


В одном из случаев специалисты зафиксировали использование не только устаревших программ, но и оборудования, которое уже не поддерживается производителем. Из-за проблемы end of life, то есть прекращения выпуска вендором обновлений для аппаратных модулей, на периметре компании могут оставаться уязвимые и незащищенные устройства. Необходимо обеспечивать постоянный контроль актуальности используемого программного обеспечения и своевременно устанавливать обновления.

Человек — слабое звено защиты

Как отмечалось ранее, в 60% успешных атак на российские организации использовалась социальная инженерия, что делает ее одним из ключевых инструментов киберпреступников. Результаты тестов на проникновение подтверждают эффективность атак методами социальной инженерии: сотрудники остаются уязвимым звеном в системе обеспечения кибербезопасности. О текущих и будущих тенденциях в фишинге можно узнать в исследовании «Какими будут фишинговые атаки в ближайшем будущем».

Рисунок 60. Типовой вектор проникновения в корпоративную инфраструктуру с помощью фишинговой атаки

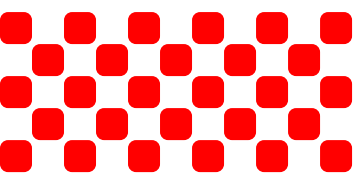


Важно учитывать, что киберпреступники могут комбинировать различные приемы и каналы взаимодействия с сотрудниками в рамках одной атаки. Они отправляют письма на корпоративную почту, выходят на связь через мессенджеры с использованием поддельных аккаунтов коллег или звонят по телефону, применяя дипфейки с подменой голоса.

Рисунок 61. Возможный вектор проникновения в корпоративную инфраструктуру с помощью фишинговой атаки



Обучение сотрудников распознаванию атак, проводимых методами социальной инженерии, должно охватывать не только классический фишинг, но и другие сценарии, основанные на человеческом факторе, например Push Bombing. Такая атака начинается после того, как злоумышленник получает учетные данные. Далее он многократно отправляет на устройство жертвы push-запросы для подтверждения входа. Поток навязчивых уведомлений в конечном счете побуждает пользователя одобрить запрос, тем самым предоставив киберпреступнику доступ к аккаунту.



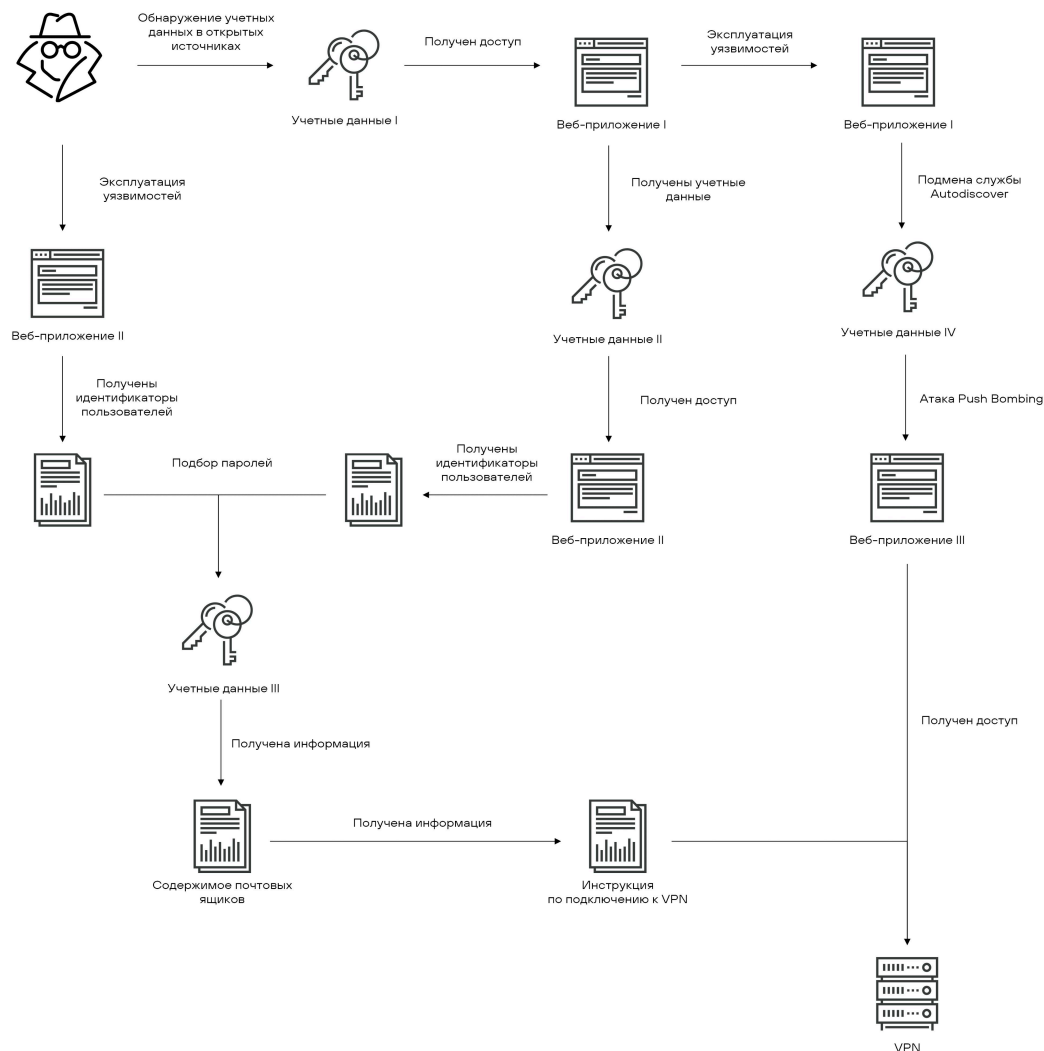
Кейс из практики специалистов по тестированию на проникновение Positive Technologies (PT SWARM): получение доступа к корпоративному VPN

Для получения доступа к корпоративному VPN специалисты PT SWARM использовали данные из открытых источников, эксплуатировали уязвимости веб-приложений, подбирали учетные данные, а также применяли атаку Push Bombing, опираясь на человеческий фактор. Этот сценарий наглядно показывает, что опытные киберпреступники способны комбинировать разные методы и уязвимости в системе защиты компании для достижения своей цели.

Шаги для получения доступа к корпоративному VPN:

- 1 В открытых источниках обнаружили учетные данные администратора веб-приложения А (учетные данные I), а также формат корпоративных адресов электронной почты.
- 2 С помощью доступной в сети службы Autodiscover Microsoft Exchange получили адреса электронной почты сотрудников.
- 3 Используя учетные данные I, получили доступ к веб-интерфейсу администрирования CMS на узле веб-приложения А.
- 4 Через встроенные возможности CMS получили доступ к ОС и извлекли учетные данные II.
- 5 С их помощью подключились к службе Autodiscover веб-приложения В, выгрузили адресную книгу и глобальный список адресов, провели атаку DNT Lookup и получили идентификаторы доменных записей.
- 6 Подобрали пароли к ряду доменных учетных записей (учетные данные III), используя идентификаторы, собранные на шагах 2 и 5.
- 7 Получили доступ к почтовым ящикам нескольких доменных пользователей с помощью учетных данных III и обнаружили инструкцию по подключению к корпоративному VPN.
- 8 Предоставили административные привилегии сервисной учетной записи на узле веб-приложения А.
- 9 Провели атаку «Подмена службы Autodiscover» и получили дополнительные доменные учетные записи, включая учетные данные IV.
- 10 Используя учетные данные IV, реализовали атаку Push Bombing на узле веб-приложения С и получили доступ к portalу второго фактора.
- 11 Для пользователя с учетными данными IV зарегистрировали второй фактор и успешно подключились к корпоративному VPN.

Схема получения доступа к корпоративной инфраструктуре из практики специалистов PT SWARM



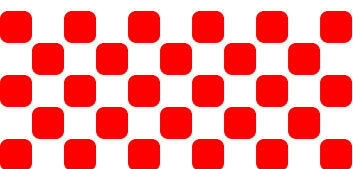
Меры кибербезопасности, направленные на устранение возможного вектора::

- реализовать строгую парольную политику;
- исключить хранение конфиденциальной информации в открытом виде;
- запретить прямой доступ к Microsoft Exchange из интернета;
- заменить Basic Authentication для службы Autodiscover в Microsoft Outlook на более безопасный механизм аутентификации;
- обеспечить эффективную реализацию двухфакторной аутентификации;
- повысить осведомленность сотрудников о работе с двухфакторной аутентификацией.

Физическая брешь — угроза кибербезопасности

Высококвалифицированные киберпреступники, нацеленные на конкретную организацию, способны действовать не только в киберпространстве, но и обходить цифровую защиту через бреши в физической защите.

Особое внимание необходимо уделять мерам безопасности в периоды проведения мероприятий, когда в офис получают доступ посторонние. Конкурс социальной инженерии SEQuest, проводимый на Positive Hack Days в 2024 и 2025 годах, наглядно демонстрирует уязвимость подобных событий перед социальными атаками. Грамотно подготовленный злоумышленник может проникнуть за периметр безопасности, получить доступ к устройствам сотрудников и даже в серверные помещения.



Кейс из практики специалистов по тестированию на проникновение Positive Technologies (PT SWARM):
получение доступа к корпоративной сети

Для получения доступа в корпоративную сеть специалисты PT SWARM выполнили следующие шаги:

- 1 Обнаружили беспроводные Wi-Fi-сети вблизи офиса тестируемой компании.
- 2 Создали поддельные точки доступа и реализовали атаку Evil Twin.
- 3 С ее помощью перехватили учетные данные сотрудников в открытом виде.
- 4 Во время мероприятия проникли в офис и обнаружили ноутбук сотрудника.

Используя перехваченные учетные данные, аутентифицировались в корпоративной сети, установили ПО SSF и настроили туннель к собственным устройствам.

Схема получения доступа к корпоративной инфраструктуре из практики специалистов PT SWARM

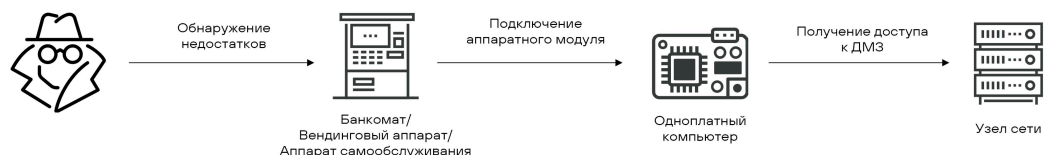


Меры кибербезопасности, направленные на устранение возможного вектора::

- применять единственно рекомендованный метод аутентификации EAP-TLS для Enterprise-сетей;
- использовать принцип наименьших привилегий при подключении устройств к корпоративной сети;
- реализовать строгую парольную политику.

Компаниям из финансовой, торговой и логистической сфер следует учитывать риск компрометации узлов сети, находящихся вне контролируемой зоны: банкоматов, вендинговых аппаратов, постаматов и других удаленных устройств. Необходимо обеспечивать достаточную сегментацию сети и исключать возможность подключения сторонних аппаратных средств к этим узлам.

Рисунок 64. Возможный вектор проникновения в корпоративную инфраструктуру через уязвимый внешний узел



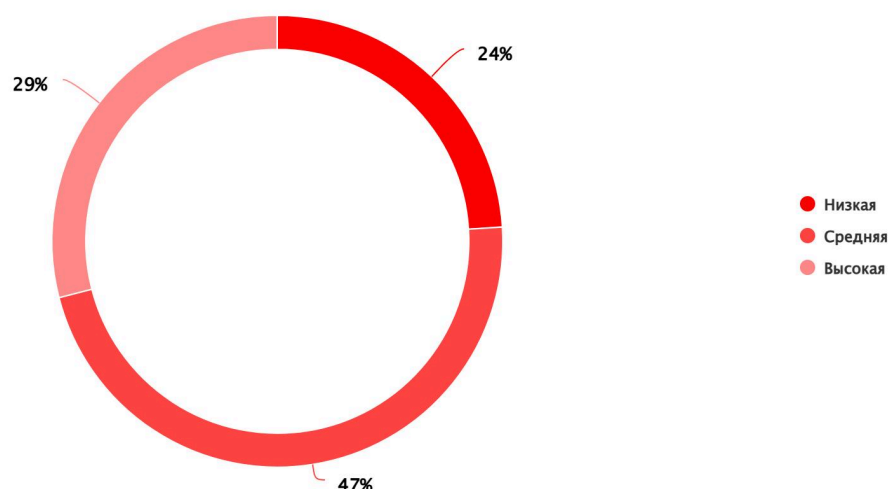
Проблемы внутри инфраструктуры

После проникновения во внутреннюю сеть наибольший ущерб злоумышленники способны нанести, получив привилегии администратора домена. Во всех тестах на проникновение с развитием атаки на внутренние ресурсы специалисты PT SWARM получали полный контроль над доменом. В условиях, когда доступ к инфраструктуре с высокой вероятностью может привести к захвату домена, необходимо прилагать дополнительные усилия для недопущения злоумышленников за защищенный периметр компании, а в случае их продвижения внутрь инфраструктуры — реагировать максимально оперативно.

Компрометация домена способна привести к критическим последствиям: утечке конфиденциальных данных, разрушению или полной утрате инфраструктуры, сбоям в бизнес-процессах, а также к возможности проведения атак на клиентов и партнеров. Поэтому защита домена должна рассматриваться как одна из приоритетных задач информационной безопасности наряду с другими ключевыми системами, компрометация которых может повлечь реализацию недопустимых событий.

Во всех протестированных компаниях уровень защищенности от внутренних атак был низким либо ниже среднего. При этом каждый четвертый (24%) вектор получения контроля над доменом имел низкую сложность.

Рисунок 65. Сложность выявленных векторов получения контроля над доменом (доля векторов)



Показательно, что в 44% случаев для захвата максимальных привилегий в домене специалистам PT SWARM было достаточно менее 10 шагов.

Рисунок 66. Количество шагов в выявленных векторах получения контроля над доменом (доля векторов)

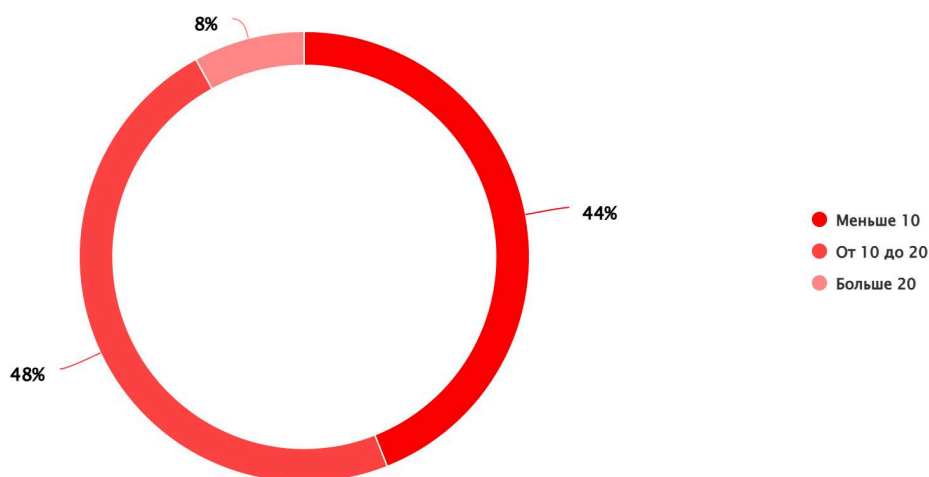
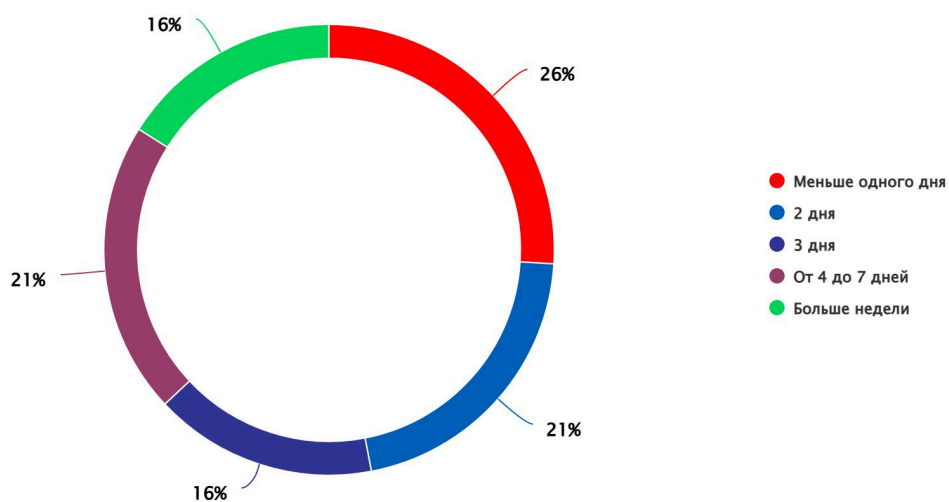


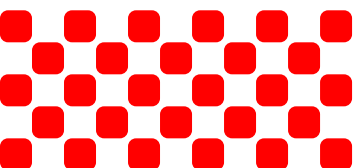
Рисунок 67. Количество дней до получения контроля над доменом при внутренних пентестах (доля проектов)



После получения контроля над доменом специалисты PT SWARM добивались реализации⁷ обозначенных недопустимых событий и дополнительных целей. К ним относятся:

- получение привилегированного доступа к целевым системам;
- нарушение работы информационных ресурсов с остановкой бизнес-процессов;
- искажение, уничтожение или утечка конфиденциальных данных;
- похищение финансовых средств.

⁷ Специалисты PT SWARM реализовывали согласованные с заказчиком критерии недопустимых событий, не причиняя ущерба системам и данным.



По итогам внутренних тестов на проникновение удалось реализовать 79% обозначенных недопустимых событий с минимальным временем достижения цели — 4 часа после получения контроля над доменом.

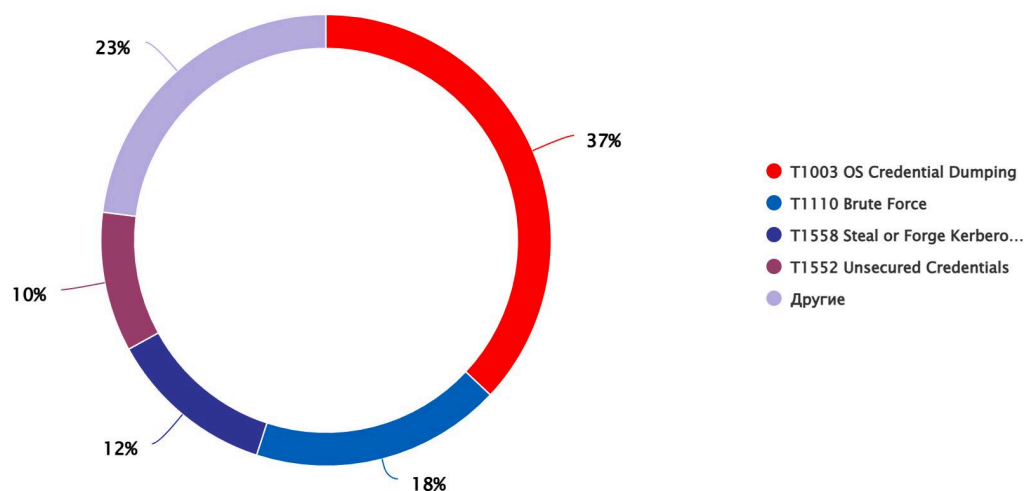
В ходе внутренних тестов на проникновение специалисты PT SWARM в основном эксплуатировали следующие проблемы безопасности: небезопасное хранение учетных данных, недостаточную защиту процессов аутентификации, недостатки в конфигурации системы сертификации Active Directory, использование слабых паролей, а также уязвимости в устаревшем программном обеспечении.

Учетные записи — ключ к взлому

В ходе внутренних тестов на проникновение специалисты PT SWARM регулярно получали учетные данные легитимных пользователей и сервисов, используя их для дальнейшего развития атаки. Техника T1078 Valid Accounts использовалась в 34% случаев применения тактики закрепления (Persistence) и в 39% случаев повышения привилегий (Privilege Escalation). Значимую роль также сыграла техника T1550 Use Alternate Authentication Material, включая подтехники T1550.002 Pass the Hash и T1550.003 Pass the Ticket: она использовалась при перемещении внутри сети (Lateral Movement) в 38% случаев и для предотвращения обнаружения (Defense Evasion) — в 24%.

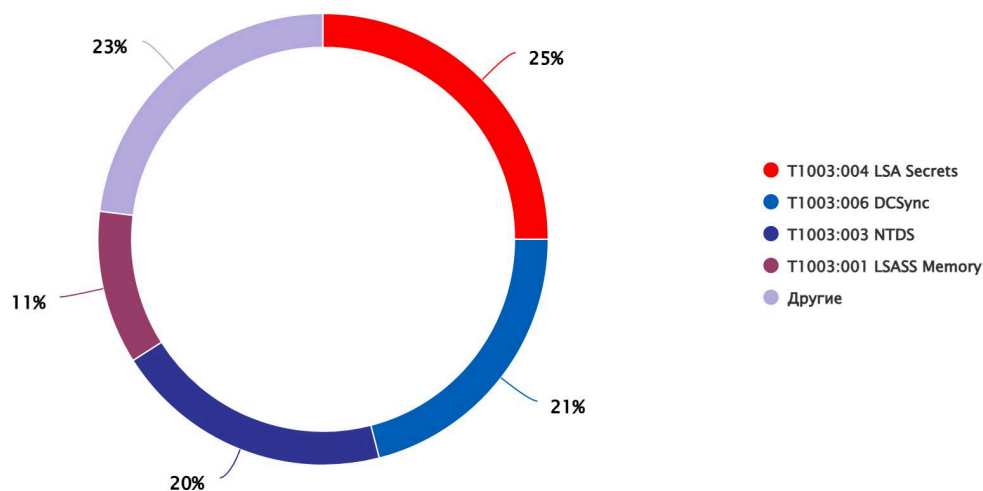
Для получения учетных данных применялись различные техники, в числе которых извлечение из памяти ОС (T1003 OS Credential Dumping), перебор «грубой силой» (T1110 Brute Force) и другие.

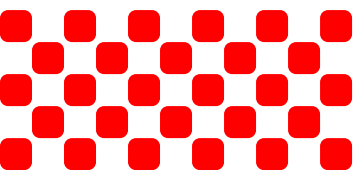
Рисунок 68. Техники Credential Access, применявшиеся во внутренних тестах на проникновение



Реализация подобных техник становится возможной вследствие распространенной проблемы небезопасного хранения конфиденциальных данных, выявленной в 85% протестированных компаний, использования одинаковых или схожих паролей для разных учетных записей, а также из-за недостаточной защиты от атак, направленных на кражу учетных данных, например техник принудительной аутентификации (PetitPotam, PrinterBug) или Kerberos Relay.

Рисунок 69. Подтехники Credential Dumping, применявшиеся во внутренних тестах на проникновение





Кейс из практики специалистов по тестированию на проникновение Positive Technologies (PT SWARM): получение контроля над доменом

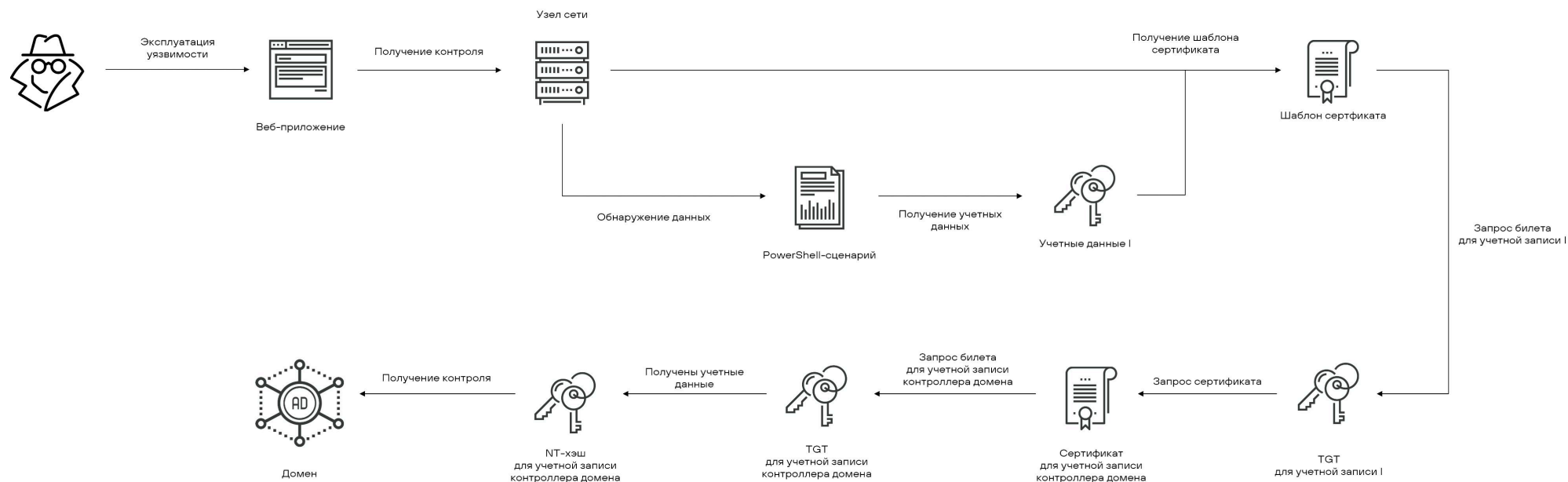
Для получения контроля над доменом специалисты PT SWARM выполнили следующие шаги:

1. Обнаружили веб-приложение с известной уязвимостью «Удаленное выполнение произвольного кода», проэксплуатировали ее и загрузили на узел сети интерпретатор командной строки.
2. На этом узле нашли PowerShell-сценарий с доменной учетной записью.
3. С помощью найденной учетной записи получили шаблон сертификатов Active Directory.
4. Проэксплуатировали уязвимость шаблона и запросили Ticket Granting Ticket (TGT) и сертификат для указанной учетной записи, установив в качестве альтернативного имени субъекта учетную запись контроллера домена.
5. С использованием полученного сертификата запросили TGT и NT-хеш учетной записи контроллера домена, после чего получили полный контроль над доменом.

Меры кибербезопасности, направленные на устранение возможного вектора:

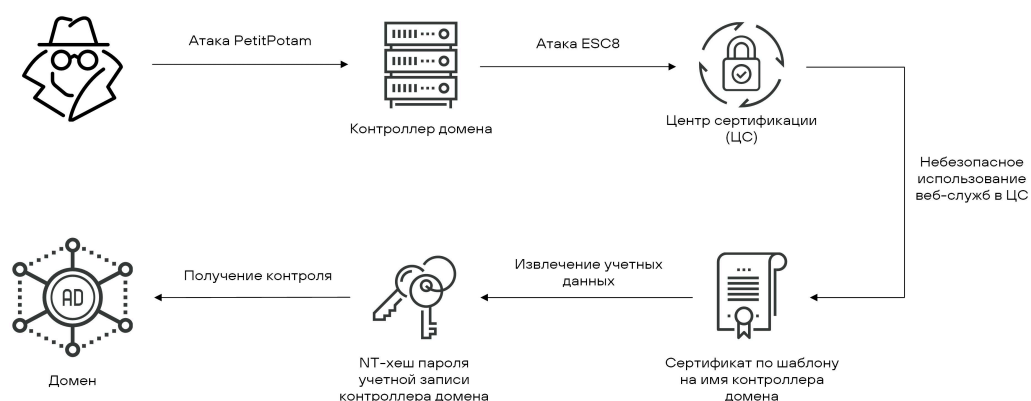
- обновить ПО на периметре инфраструктуры до актуальных версий;
- не допускать хранения конфиденциальной информации в открытом виде;
- по возможности отключить в шаблоне сертификата опцию получения альтернативного имени из запроса;
- устранить известные недостатки конфигурации в шаблонах сертификатов;
- реализовать рекомендованные меры по снижению риска атак, эксплуатирующих недостатки шаблонов сертификатов;
- проводить аудиты событий, связанных с обнаружением подозрительных запросов на получение сертификатов.

Схема получения доступа к корпоративной инфраструктуре из практики специалистов PT SWARM



Один из регулярно используемых способов повышения привилегий — атаки на службы сертификации Active Directory (так называемые ESC-атаки). Эксперты PT Cyber Analytics подробно рассматривали векторы всех ESC-атак, включая последний на момент публикации исследования — ESC16.

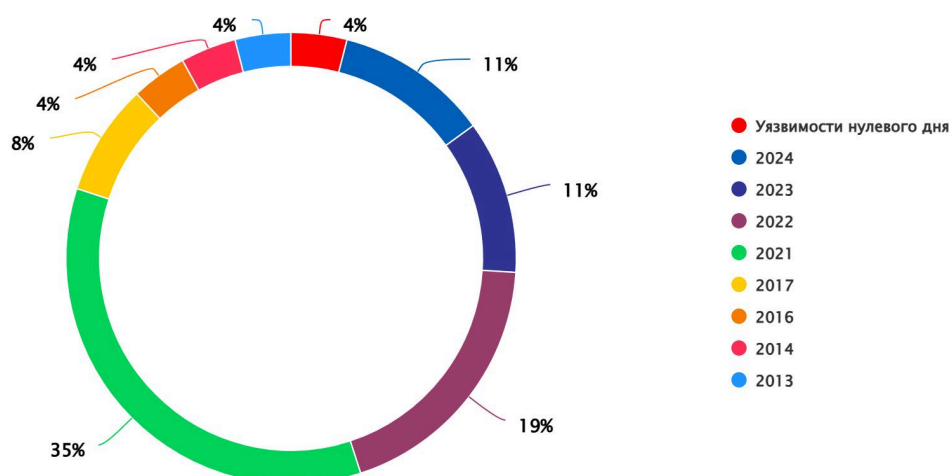
Рисунок 71. Возможный вектор получения контроля над доменом

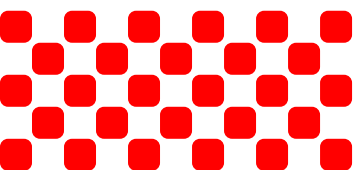


Дальше в домен — старше уязвимости

Специалисты PT SWARM выявили устаревшее программное обеспечение в каждой второй (48%) протестированной компании. При этом у 42% организаций такие уязвимости имели критический уровень риска. На долю устаревшего ПО пришлось около 9% всех проблем безопасности, выявленных во время внутренних тестов на проникновение. По сравнению с внешним тестированием специалистам потребовалось реже прибегать к эксплуатации уязвимостей нулевого дня, но при этом 8% выявленных уязвимостей оказались старше десяти лет.

Рисунок 72. Распределение выявленных в ходе внутренних тестов на проникновение уязвимостей по году обнаружения (доля уязвимостей)





Кейс из практики специалистов по тестированию на проникновение Positive Technologies (PT SWARM): получение контроля над доменом

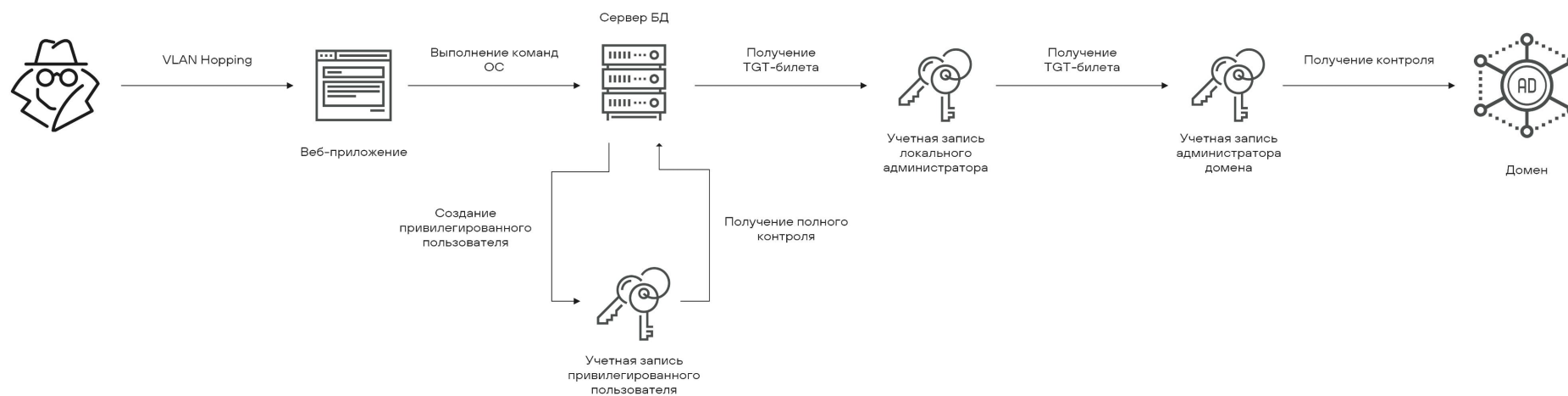
Для получения контроля над доменом специалисты PT SWARM выполнили следующие шаги:

- 1 Находясь в корпоративной инфраструктуре, провели атаку VLAN Hopping и обнаружили веб-приложение.
- 2 Проэксплуатировали уязвимость «Внедрение SQL-кода» в этом веб-приложении и создали привилегированную учетную запись на узле сети.
- 3 С помощью полученных прав сформировали TGT для пользователя с правами локального администратора.
- 4 Выявили активную сессию пользователя с правами администратора домена.
- 5 Скомпрометировали учетную запись администратора домена, получив ее TGT, и таким образом установили полный контроль над доменом.

Меры кибербезопасности, направленные на устранение возможного вектора:

- защита от атак VLAN Hopping: ограничение сетевой видимости; внедрение аутентификации для устройств, подключающихся к сети; регулярный мониторинг сетевого трафика;
- защита от внедрения SQL-кода: использование параметризованных SQL-запросов и «белых» списков значений параметров; применение принципа минимальных привилегий для веб-приложений при работе с базой данных; обязательная валидация поступающих от пользователя данных; рассмотрение возможности использования технологии Object Relational Mapping;
- разграничение прав доступа: реализация строгого разграничения прав доступа для пользователей в отношении объектов контроллера домена.

Схема получения доступа к корпоративной инфраструктуре из практики специалистов PT SWARM



Выводы и прогнозы

Многолетний опыт проведения тестов на проникновение показывает, что типовые проблемы кибербезопасности остаются актуальными для российских компаний из года в год. Специалисты PT SWARM ежегодно достигают целей как внешних, так и внутренних пентестов в подавляющем большинстве организаций. В 2026 году ситуация не поменяется, тестирование на проникновение вновь выявит традиционные слабые звенья защиты: простые пароли, отсутствие многофакторной аутентификации, небезопасное хранение данных, применение устаревшего ПО с известными уязвимостями, ошибки в разграничении доступа и недостаточную подготовку сотрудников к распознаванию атак методами социальной инженерии.

Повторяющаяся из года в год картина говорит о закономерности этих проблем для информационных систем. Тем не менее уязвимое состояние инфраструктуры не может считаться нормой. Обеспечение результативной безопасности необходимо выстраивать с учетом определенных для компании недопустимых событий, а также актуальных тенденций в киберпреступном мире.

Автоматические системы для оценки безопасности делают базовую киберзащиту доступной для всех. Уже сегодня базовые недостатки безопасности могут быть обнаружены сканерами уязвимостей в составе VM-решений и автопентестами. В 2026 году роль таких инструментов продолжит расти. Тем более, что благодаря формату автопентеста по подписке этот вариант остается доступен для организаций с различными бюджетами на информационную безопасность.

Результаты работы специалистов PT SWARM показывают, что для проникновения в корпоративную инфраструктуру 57% компаний достаточно вектора низкой сложности. Поэтому даже устранение базовых проблем с помощью автоматических пентестов поднимет уровень защищенности компании относительно среднего показателя. Это, в свою очередь, может стать важным фактором защиты от хактивистов и низкоквалифицированных финансово мотивированных киберпреступников, которые, как правило, выбирают наименее защищенные цели.

Роль крупных игроков рынка сервисов по анализу защищенности будет смещаться в сторону комплексных проектов. По мере того как базовые проблемы безопасности в инфраструктуре все чаще будут выявляться с помощью автоматизированных инструментов, задачи экспертных команд должны выйти за рамки стандартных тестов на проникновение. Высококласные специалисты сосредоточатся на проверке реализуемости недопустимых событий, проведении киберучений и оценке эффективности MDR-сервисов.

Полноценный red teaming от внешнего поставщика услуг не реже одного раза в год должен оставаться обязательной практикой для организаций со зрелыми процессами информационной безопасности, причем даже в тех случаях, когда значительная часть инфраструктуры компании проходит кибериспытания на платформах багбаунти.

Для надежной защиты приложения или сервиса нужен не только автоматизированный, но и экспертный ручной анализ. Как и в случае с инфраструктурой компании, для выявления сложных уязвимостей в приложениях и сервисах недостаточно полагаться исключительно на автоматизированные средства анализа защищенности. Сканеры кода и тестирование методом белого ящика позволяют выявлять типовые уязвимости, однако они не способны полноценно оценить корректность бизнес-логики и сценариев работы приложения. Поэтому перед размещением продукта на платформах багбаунти необходимо проводить ручное экспертное тестирование.

В 2026 году значимость таких проверок будет только возрастать на фоне масштабного применения ИИ-ассистентов для программирования и практики вайб-кодинга, которые ускоряют разработку, но одновременно с этим повышают риск появления недеklarированных возможностей и ошибок в логике работы приложений.

В центре шахматной партии: какие отрасли под особым прицелом



В последние годы Россия переживает заметные геополитические трансформации. На этом фоне цифровая среда страны активно развивается: внедряются современные, в том числе отечественные технологии, расширяются возможности сервисов, растет уровень цифровизации экономики и общества. Одновременно с этим существенно увеличивается число киберугроз. Доля атак на Россию из квартала в квартал остается высокой, ежегодно появляются новые киберпреступные группировки, что требует от бизнеса и государства системного укрепления защиты.

Рекомендации для государства



Региональное и международное сотрудничество

В условиях геополитической напряженности, санкционного давления и роста числа киберугроз стратегически важной задачей для России является региональное и международное сотрудничество в сфере кибербезопасности. Это позволит не только повысить устойчивость национальной цифровой инфраструктуры, но и укрепить имидж России как надежного и конструктивного партнера в цифровом взаимодействии.

Приоритетным направлением остается развитие партнерства в рамках СНГ и ОДКБ. Уже реализуются практические шаги: в мае 2025 года МВД России и Белоруссии договорились о синхронизации усилий в борьбе с киберпреступностью и обмене законодательными практиками. Следует инициировать механизмы оперативного обмена технической информацией об угрозах, включая индикаторы компрометации. Такой формат уже обсуждается на уровне СНГ, где планируется запуск общей платформы для обмена цифровыми следами преступлений между странами-участницами СНГ.

В рамках сотрудничества с Китаем следует активизировать совместные научно-технические проекты в сфере ИБ, включая разработку систем защиты от сложных целенаправленных атак и обмен технологиями устойчивой сетевой инфраструктуры. Россия и Китай ведут диалог по вопросам цифрового суверенитета и норм поведения в киберпространстве.

На глобальном уровне России необходимо укреплять свою роль в рамках ООН, БРИКС и ШОС. Первым шагом в данном направлении стало принятие разработанной по инициативе России Конвенции ООН против киберпреступности.

Подготовка кадров и образование

Развитие кадров в сфере информационной безопасности — один из ключевых факторов цифрового развития России: даже самые современные технологии защиты неэффективны без специалистов, способных их внедрять, сопровождать и совершенствовать. Проблема нехватки таких кадров стоит остро: в 2024 году количество вакансий выросло на 17–50%, тогда как число резюме снизилось на 6%.

Инвестиции в подготовку специалистов становятся приоритетной задачей для России. Необходимо совершенствовать и поддерживать в актуальном состоянии образовательные программы, а также развивать профильных педагогов. Еще одной важной задачей для государства является укрепление взаимодействия между ВУЗами и компаниями в сфере кибербезопасности — это позволит готовить специалистов с компетенциями, необходимыми на рынке труда.

Подобные инициативы формируют кадровый потенциал, необходимый для защиты цифрового суверенитета и построения устойчивой цифровой экономики.

Защита критической информационной инфраструктуры

В условиях обострения геополитической ситуации особое внимание должно уделяться защите критической информационной инфраструктуры, поскольку атаки на нее способны вызвать серьезные последствия для ключевых отраслей и национальной безопасности.

Фундаментом такой защиты является нормативная и законодательная база, требующая постоянной актуализации в ответ на изменения ландшафта киберугроз.

Ключевыми задачами в сфере защиты КИИ остаются обеспечение устойчивости резервных центров обработки данных и сетей электросвязи, проведение регулярных проверок планов аварийного восстановления, а также повышение внимания к безопасности цепочек поставок и подрядчиков. Последний аспект приобретает особую актуальность, так как атаки через сторонние компании становятся все более распространенными.

Развитие и создание центров по реагированию на киберинциденты

На текущий момент в России существуют центры по реагированию на киберинциденты (CERT/CSIRT/CIRT), которые позволяют объединять усилия государственных органов и коммерческих организаций для эффективного урегулирования инцидентов, связанных с кибербезопасностью. Важной задачей остается их развитие, а также формирование специализированных центров, ориентированных на отдельные отрасли. Примером служит ФинЦЕРТ — специализированное подразделение Банка России, отвечающее за взаимодействие и реагирование в финансовом секторе. Создание отраслевых центров позволит противодействовать кибератакам и формировать перечень недопустимых событий с учетом отраслевого уровня, отслеживать и повышать уровень киберустойчивости всей отрасли.

Меры по защите граждан от киберпреступности

Согласно исследованию Международного союза электросвязи, 97% жителей России пользуется интернетом. Цифровые технологии активно проникают во все сферы жизни, однако вместе с этим растет уязвимость пользователей: во второй половине 2024-го и в первых трех кварталах 2025 года 26% всех успешных атак были направлены против частных лиц. Значительная их часть связана с мошенничеством: только в 2024 году россияне потеряли из-за него 168 млрд рублей.

Для защиты граждан государствам необходимо разрабатывать программы по противодействию мошенничеству, усиливать законодательство и повышать уровень цифровой грамотности населения. В качестве примера можно привести одну из мер, введенную с сентября 2025 года, включающую обязательную маркировку телефонных звонков.

Важным направлением борьбы с кибермошенничеством остается защита персональных данных, которые нередко используются злоумышленниками в противоправных целях. Пользователи должны быть информированы об утечке своих данных и осведомлены о порядке последующих действий. Также необходимо развитие механизмов компенсации ущерба пострадавшим от утечек пользователям. Например, в Казахстане для операторов, обрабатывающих более 1 млн персональных данных, вводится обязательное киберстрахование.

Такой подход стимулирует организации к более ответственному отношению к защите информации, снижает финансовые риски для пострадавших и способствует формированию зрелой системы управления киберрисками на национальном уровне.

Рекомендации для бизнеса



Укрепление IT-инфраструктуры

Во второй половине 2024-го и в первых трех кварталах 2025 года в 71% успешных кибератак на организации в России злоумышленники применяли вредоносное ПО. Анализ активности группировок, атакующих российские организации, показывает, что для его доставки используются различные каналы: фишинговые письма, сообщения в мессенджерах и соцсетях, поддельные сайты. Чтобы снизить риск успешных атак с применением ВПО, компаниям рекомендуется:

- использовать почтовые и веб-шлюзы, проверяющие вложения и ссылки в электронных письмах в режиме реального времени;
- внедрить NGFW и прокси-сервисы с функцией категоризации сайтов и фильтрацией трафика;
- контролировать каналы обмена файлами внутри организации, включая мессенджеры, где возможна доставка ВПО с использованием социальной инженерии;
- регулярно проверять эффективность настроек шлюзов и фильтров с помощью специализированных решений, имитирующих реальные сценарии распространения вредоносного ПО.

Важно учитывать, что эффективная защита IT-инфраструктуры невозможна без полного понимания всех активов и данных в ней. Под активами понимаются не только серверы, рабочие станции и сетевое оборудование, но и облачные сервисы, контейнеры, учетные записи сотрудников, базы данных, приложения. Согласно результатам нашего опроса, проведенного в конце 2024 года, целью которого было выяснить, как организации подходят к процессу управления активами, менее 15% респондентов ответили, что полностью отслеживают цифровые активы и владеют актуальной информацией по ним.

Компании, которые не знают полный перечень своих активов, оказываются в зоне повышенного риска. Злоумышленники используют «теневые» системы, забытые сервисы или устаревшие приложения как точки входа в инфраструктуру. Поэтому необходимо своевременно выявлять такие уязвимые элементы, обновлять их или исключать из эксплуатации, если они больше не нужны. Для этого рекомендуем использовать технологии asset management (AM).

В 28% успешных атак на организации в России злоумышленники эксплуатировали уязвимости, причем как трендовые, так и довольно старые. Своевременное обновление ПО и устранение уязвимостей — одна из обязательных для повышения киберустойчивости задач. Решения класса VM помогают не только выявлять уязвимости, но и расставлять приоритеты их устранения, а также автоматизировать процесс обновления. Для оперативного реагирования на угрозы необходимо ежедневно сканировать критически важные узлы инфраструктуры и ключевые системы на наличие уязвимостей. Однако, согласно результатам нашего опроса о готовности российских организаций противостоять атакам, такую практику применяют лишь 16% респондентов.

Для обеспечения соблюдения политик безопасности на уровне хостов, сетевых ресурсов и учетных записей рекомендуется использовать решения Host Compliance Control (HCC), Network Compliance Control (NCC) и User Compliance Control (UCC):

- HCC обеспечивает контроль соответствия активов требованиям к парольным политикам, ведению журналов значимых системных событий и защите от сетевых атак;
- NCC отвечает за безопасность сетевых ресурсов, а именно за конфигурацию сетевых устройств в соответствии с политиками безопасности, сегментацию сети, использование защищенных протоколов;
- UCC предназначен для защиты учетных записей пользователей, предотвращения компрометации учетных данных и контроля доступа к информационным системам.

Для прогнозирования сценариев продвижения злоумышленников в инфраструктуре и своевременного реагирования на угрозы рекомендуется использовать комплексные системы, объединяющие функциональность всех перечисленных продуктов.

Учитывая, что в 56% успешных атак на организации происходили утечки конфиденциальной информации, особое внимание следует уделять защите данных. Мы рекомендуем делать это с помощью решений класса data security platform (DSP), обеспечивающих полную видимость инфраструктуры хранения и обработки.

Мониторинг и своевременное реагирование

Чтобы эффективно противостоять кибератакам, необходимо своевременно выявлять подозрительные активности и быстро реагировать на них. При этом наибольшую ценность в определении легитимности действий и детальном анализе активности в инфраструктуре имеет полнота данных мониторинга. Для этого организациям рекомендуется использовать комплекс решений:

- системы управления информацией и событиями безопасности (security information and event management, SIEM);
- решения для обнаружения и реагирования на события, связанные с вредоносной активностью на конечных узлах (endpoint detection and response, EDR);
- изолированные среды для анализа вредоносных объектов (sandbox, «песочницы»);
- системы поведенческого анализа сетевого трафика (network traffic analysis, NTA);
- для промышленных предприятий — системы обеспечения киберустойчивости промышленных инфраструктур.

Человеческий фактор

В 60% успешных атак на организации ключевую роль сыграли методы социальной инженерии, поэтому обучение сотрудников — критически важная часть защиты. По данным Fortinet, 89% компаний отметили улучшение уровня безопасности после внедрения образовательных программ. Регулярные тренировки существенно повышают осведомленность: так, по данным Hoxhunt, через полгода обучения 50% сотрудников уже способны самостоятельно выявлять фишинг. Для специалистов по ИБ рекомендуется регулярное совершенствование навыков, например на онлайн-полигонах.

Оценка уровня защищенности

Поддержание киберустойчивости требует регулярных проверок безопасности инфраструктуры с формированием планов устранения выявленных проблем. В зависимости от целей, зрелости ИБ-процессов и сферы работы компании могут применяться специализированные услуги по оценке устойчивости организаций к кибератакам, ретроспективный анализ событий ИБ, тестирование на проникновение, в том числе автоматизированное, и киберучения.

Подтверждение высокого уровня киберустойчивости

Чтобы быть уверенными в защищенности ИТ-инфраструктуры, компаниям необходимо поддерживать перечень недопустимых событий в актуальном состоянии и регулярно проверять эффективность применяемых мер защиты. В дополнение к классическим методам оценки киберустойчивости полезно участвовать в кибериспытаниях: они позволяют определить возможность реализации недопустимых событий, наносящих критический ущерб, и выразить уровень защищенности в денежной оценке. Также рекомендуем размещать свои программы на платформах багбаунти, которые дают возможность выявить и устранить уязвимости до того, как ими воспользуются злоумышленники. Так, по результатам работы платформы Standoff Bug Bounty на ноябрь 2024 года, 31% обнаруженных уязвимостей имели высокий или критический уровень опасности, что подтверждает значимость подобных инициатив для практической проверки безопасности.

В условиях стремительной цифровизации, внедрения новых технологий и постоянно расширяющейся поверхности атак кибербезопасность государства и российского бизнеса становится ключевой фигурой на шахматной доске цифрового будущего. Как и в шахматах, где успех определяется не только силой отдельных фигур, но и продуманной стратегией, устойчивое развитие страны возможно лишь при комплексном подходе — модернизации нормативно-правовой базы, укреплении регионального и международного взаимодействия, подготовке квалифицированных кадров, внедрении передовых технологий защиты и регулярной оценке уровня киберустойчивости.

Каждое решение в этой партии должно быть выверенным ходом, направленным на предупреждение угроз и укрепление обороны. Только действуя согласованно, как единая команда, государство и бизнес смогут выстроить надежную защиту, сохранить цифровой суверенитет и обеспечить безопасное пространство для экономического и социального развития — доведя партию за цифровую стабильность до уверенного шаха и мата современным киберугрозам.



Узнать больше
об исследованиях
Positive Technologies