УЦСБ SOC

УЦСБ

ЛАНДШАФТ КИБЕРУГРОЗ 2025: ТРЕНДЫ, АТАКИ, УЯЗВИМОСТИ

май 2026 г.

soc.ussc.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В отчете представлены ключевые тренды киберугроз 2025 года, повлиявшие на выстраивание процессов защиты. Специалистами команды Threat Intelligence УЦСБ SOC был отмечен комплексный характер атак (шифрование + кража + публикация) и использование DDoS-атак как инструмента вымогательства (Ransom DDoS), также описано использование цепочек поставок и подрядчиков как канала проникновения и целевых фишинговых рассылок.

На основе исследования проведенного экспертной командой Threat Intelligence УЦСБ SOC в документе представлена актуальная картина киберрисков, а также сформулированы конкретные меры для выстраивания противодействия и сдерживания угроз в 2026 году.

Для кого будет полезно:

- технические специалисты: аналитики TI, инженеры по управлению уязвимостями, аналитики SOC, специалисты по защите информации и реагированию на инциденты ИБ;
- руководители SOC и подразделений реагирования на инциденты;
- руководители и специалисты внутреннего ИБ;
- инженеры по эксплуатации средств защиты.

Из анализа событий, происходящих в киберпространстве в 2025 году эксперты Threat Intelligence УЦСБ SOC **выделили ключевые изменения в характере угроз и каналах атак**, которые необходимо учитывать при выстраивании мер противодействия.

1. **Угрозы для российских организаций в 2026 году станут комплексными.** Особого внимания при принятии мер противодействия и минимизации ущерба потребуют неизменяемые бэкапы и контроль публичного периметра.

2. **DDoS-атаки используют не только принцип «мощности»**, но и переходят к точечному давлению на бизнес-процессы. Основными мерами защиты становятся геофильтрация, rate-limit и профессиональные сервисы защиты.

3. **Цепочки поставок и подрядчики остаются главным вектором проникновения**. Требуется строгий контроль удаленного доступа, MFA и сегментация сети даже для доверенных партнеров.

4. **Социальная инженерия остается базовым вектором для множества атак**, включая компрометацию учетных данных, атаки на сотрудников и использование фишинговых ресурсов. Ключевыми мерами противодействия являются повышение киберграмотности персонала, регулярные фишинг-тесты, контроль доступа к чувствительным данным и дополнительные меры аутентификации для критичных ролей.

УЯЗВИМОСТИ, КОТОРЫЕ ЭКСПЛУАТИРОВАЛИСЬ В АТАКАХ В 2025 ГОДУ

В 2025 году из более чем 48 тысяч вновь опубликованных CVE для 21% уязвимостей были доступны публичные эксплойты, но реальная эксплуатация злоумышленниками подтверждена лишь для 1% по данным платформа кибербезопасности **VulnCheck**. Более половины уязвимостей, задействованных в атаках программ-вымогателей, относились к zero-day, что резко повышало риски для систем без своевременно принятых мер противодействия.

Глобальная платформа кибербезопасности **VulnCheck** в ежегодном отчете расширила свой каталог известных эксплуатируемых уязвимостей на 884 позиции на основе доказательств из 118 источников, где уязвимости 2025 года составили **47,7%** базы — это показывает ускорение атакующих в создании и применении эксплойтов. Также отмечен рост общего числа эксплойтов на 16,5% благодаря использованию искусственного интеллекта.

Особенный тренд смогла выделить команда Threat Intellengence УЦСБ SOC в ходе анализа атак с использованием уязвимостей — **рост атак через известные уязвимости**: в 2025 году число инцидентов, где злоумышленники получали первичный доступ через уже описанные CVE, увеличилось примерно на 30% по сравнению с предыдущим годом. Это означает, что старые, но неустановленные уязвимости все чаще становятся основным вектором первичного проникновения в инфраструктуру.

Специалистами команды Threat Intellengence УЦСБ SOC было выделено 65 трендовых уязвимостей, отнесенных к числу наиболее критичных и эксплуатируемых в российском сегменте. Все они выявлены в программных и аппаратных решениях, применяемых российскими организациями, включая операционные системы, прикладное ПО, сетевые устройства и другие компоненты инфраструктуры.

Большинство уязвимостей зафиксировано в сегменте операционных систем и рабочих станций — **44%**. Значительную долю занимают уязвимости сетевой инфраструктуры и сервисов — **27%**, а также прикладного ПО и библиотек — **23%**. Оставшиеся **6%** приходятся на корпоративные ИТ-платформы.

Более подробная информация со списком уязвимостей представлена в **Приложении «Детализированные списки трендовых уязвимостей 2025 года»**.

РАСПРЕДЕЛЕНИЕ ТРЕНДОВЫХ УЯЗВИМОСТЕЙ ПО ТИПАМ ИТ-РЕШЕНИЙ

Показательный пример перехода потенциального риска в реальную угрозу — уязвимости повышения привилегий в Hyper-V (CVE-2025-21333, CVE-2025-21334, CVE-2025-21335). Для CVE-2025-21333 были опубликованы публичные PoC-эксплойты, а также зафиксированы случаи эксплуатации в реальных атаках группировкой **DarkHydrus** в Юго-Восточной Азии.

Другой пример — уязвимость CVE-2025-33053, представляющая собой полноценный weaponized zero-day. Она использовалась APT-группой **Stealth Falcon** в целевых атаках еще до выхода патча. Эксплуатация реализовывалась через вредоносные .url-файлы и WebDAV, что делало ее особенно эффективной в фишинговых сценариях.

Также интересен пример кампании, связанной с цепочкой уязвимостей ToolShell, которую активно использовали для компрометации серверов Microsoft SharePoint. Эта цепочка объединяла несколько CVE-2025-53770 и CVE-2025-53771, что позволило атакующим получить удаленное выполнение кода в инстансах SharePoint, доступных из сети Интернет, без необходимости аутентификации. Группа, отслеживаемая как **Storm-2603**, наряду с другими китайскими операторами (например, Linen Typhoon и Violet Typhoon), использовала именно эту цепочку уязвимостей для вторжения в корпоративные сети и развертывания вредоносного ПО.

Также стоит отметить:

CVE-2025-8088 — WinRAR. Серьезный path traversal-баг в WinRAR, который эксплуатировался в реальных атаках для доставки зловредов и установки постоянных нагрузок. Видео и PoC-демки демонстрируют практический exploit-код, используемый в wild

(уязвимость не просто существует теоретически, а активно используется злоумышленниками в реальных атаках).

CVE-2025-55188 — 7-Zip. По этой уязвимости имеются подтверждения наличия PoC-эксплойтов на GitHub: публичные репозитории с PoC были опубликованы после раскрытия. Они демонстрируют возможность произвольной перезаписи файлов при извлечении архивов.

CVE-2025-55182 — React2Shell. Уязвимость представляет собой безавторизационный RCE в React Server Components/Next.js. После раскрытия появились публичные PoC-эксплойты и немедленно зафиксированы эксплуатации в реальных кампаниях со стороны нескольких китайских хакерских групп, связанных с государством, включая **Earth Lamia и Jackpot Panda**.

BDU-2025-10114, BDU-2025-10115, BDU-2025-10116 — TrueConf Server. Позволяет злоумышленникам обойти проверку доступа, прочитать произвольные файлы и выполнить произвольные команды на сервере при отсутствии актуальных обновлений, создавая в системе привилегированные учетные записи для дальнейшей эксплуатации. Исследователями УСЦБ SOC отмечалась волна подобных атак, приписываемая к группировке **Head Mare**, использующей данную цепочку уязвимостей для проникновения и постэксплуатации.

ОТСЛЕЖИВАНИЕ ПРОТИВНИКА: ОПЕРАЦИИ APT-ГРУППИРОВОК В 2025 ГОДУ

В 2025 году активность APT-группировок (Advanced Persistent Threat) против РФ-сегмента выросла на 25–30% по сравнению с 2024 годом — атаки стали более целенаправленными и интенсивными. При этом общий рост наблюдается не столько благодаря появлению новых игроков, сколько вследствие усиления и расширения активности уже известных группировок, а также их фокуса на более крупных и стратегически значимых секторах.

По данным отчета CrowdStrike 2025 Global Threat Report, атакующие сократили временной цикл между первичным проникновением и переходом к целевым операциям до 48 минут в среднем и до 51 секунды в самых быстрых случаях, все чаще используя искусственный интеллект, легитимные учетные записи, стандартные административные инструменты и уязвимые решения вендоров. В ряде случаев первичный доступ формируется не только через фишинг-рассылки, но и за счет компрометации организаций, выступающих в роли подрядчиков и интеграторов, что позволяет злоумышленникам масштабировать воздействие на целевые организации через цепочки поставок. Это повышает устойчивость кампаний, снижает их заметность и усложняет своевременное обнаружение даже при наличии устоявшихся механизмов мониторинга. По оценке команды Threat Intelligence УЦСБ SOC, основанной на анализе инцидентов за 2025 год, атаки через подрядчиков и интеграторов составляют не менее 30% от всех общеизвестных кибератак, что позволяет рассматривать данный вектор как один из ключевых трендов текущего периода.

Долгоиграющим трендом для APT-группировок, действующих на российском сегменте, остается применение **целевых рассылок**, как основного вектора первичного проникновения. Сценарии рассылок становятся более персонализированными, учитывают структуру организаций, роли сотрудников и используемые сервисы, что повышает их эффективность и устойчивость к стандартным методам защиты.

В течение всего 2025 года специалисты команды Threat Intelligence УЦСБ SOC вели тщательный мониторинг и глубокий анализ действий хакерских группировок, ориентированных на российский бизнес и госструктуры, что позволило составить профиль их активности для выстраивания эффективных стратегий противодействия. Ниже рассматриваются три самые активные APT-группировки, чьи действия в 2025 году оказали наибольшее практическое влияние на российский сегмент и наглядно иллюстрировали ключевые выявленные тренды. В качестве критериев отбора использовались характер и сложность атак, новизна тактик и масштаб их воздействия на критически важные инфраструктуры, что позволяет рассматривать их как представителей наиболее продвинутых и опасных угроз года.

PhantomCore

Другие названия	Head Mare Rainbow Hyena Fairy Trickster
Инструменты	StatRAT, PhantomRShell, PhantomDL, PhantomPSUpload, PhantomJitter, PhantomTaskShell, PhantomProxyLite, PhantomCSLoader, PhantomSAgent, PhantomGoShell, PhantomPasswordDumper, LockBit, PhantomRAT, PhantomPyramid, PhantomCore.KscDL_trim, Babuk
География атак	Россия Беларусь
Атакуемые отрасли	Аэрокосмическая промышленность Военный сектор Государственный сектор Здравоохранение Исследовательские организации Логистические компании Медиа Производство Развлечения Розничная торговля Телекоммуникации Технологические компании Финансовый сектор Энергетика

На протяжении 2025 года данная группировка проявляла повышенную активность, при этом меняя инструменты и подходы к атакам.

Начальный вектор атак не изменился: преимущественно он осуществлялся через целевые рассылки с ZIP-архивами и LNK-ярлыками, а также через фишинговые страницы с fake CAPTCHA, принуждающие выполнить PowerShell-однострочник.

По данным **Kaspersky**, в марте 2025 исполняемая часть polyglot-файла представляла собой ранее неизвестный бэкдор PhantomPyramid, написанный на Python версии 3.8, который загружал легитимный MeshAgent из MeshCentral (утилита для удалённого администрирования, которая после запуска на целевом устройстве самостоятельно подключается к серверу MeshCentral, предоставляя оператору доступ к системе). Ранее такой агент был замечен у группы Awaken Likho.

На следующем этапе, уже летом 2025, злоумышленники обновили инструментарий, задействовав цепочку дополнительных бэкдоров — PhantomCSLoader и PhantomSAgent — для закрепления в системе. Эти вредоносные программы написаны на разных языках

программирования, применяют схожую модель взаимодействия с C&C-сервером, но отличаются внутренними механизмами работы — вероятно, чтобы при обнаружении одного компонента другой продолжал функционировать.

По данным **команды Threat Intellengence УЦСБ SOC**, к концу года злоумышленники отошли от привычных векторов атак, перейдя к целенаправленным ударам по организациям, использующим TrueConf Server. Киберпреступники активно эксплуатировали цепочку недавно исправленных уязвимостей в указанном ПО для видеоконференций, получая полный контроль над корпоративными серверами.

Атаки начинались с использования сервисов анонимизации, в частности, Proton VPN, что затрудняет отслеживание истинного источника угрозы. На первом этапе злоумышленники применяли связку двух уязвимостей, зарегистрированных в базе данных уязвимостей ФСТЭК России под идентификаторами BDU:2025-10114 и BDU:2025-10116. Первая представляет собой уязвимость типа Server-Side Request Forgery (подделка межсайтовых запросов), а вторая — Command Injection (внедрение команд), что в совокупности позволяло выполнять произвольные команды на целевом сервере.

Особую известность PhantomCore приобрела после атак на крупную транспортно-логистическую компанию в 2024 году.

Black Owl

Другие названия	BO Team Lifting Zmiy Hoody Hyena
Инструменты	BrockenDoor, Reverse SSH, DarkGate, Remcos, Babuk
География атак	Россия
Атакуемые отрасли	Государственные учреждения Здравоохранение Промышленный сектор Сельскохозяйственная промышленность Телекоммуникации Транспортные компании

По сравнению с аналогичным периодом 2024 года начальный вектор атак не изменился, для получения первоначального доступа использовались целевые фишинговые письма: злоумышленники представлялись поставщиками услуг страхования и банковскими организациями.

По данным **Kaspersky** от мая 2025 года, для получения первоначального доступа злоумышленники используют фишинговые рассылки, содержащие вредоносные вложения. Если пользователь открывает вложение, запускается цепочка компрометации, в результате которой в системе жертвы выполняется один из следующих бэкдоров:

- DarkGate;
- BrockenDoor;
- Remcos.

После компрометации целевых систем BO Team уничтожает резервные копии файлов и виртуальную инфраструктуру компании, а также удаляет данные с хостов с помощью популярной утилиты SDelete. В отдельных случаях злоумышленники дополнительно используют шифровальщик Babuk (версию для Windows), чтобы потребовать с жертвы выкуп.

В мае 2025 года командой **Threat Intelligence УЦСБ SOC** была зафиксирована новая волна хакерских атак группировки BO Team на российские компании. Злоумышленники рассылали письма с угрозами и требованиями перевода средств в биткоинах, сообщая, что ИТ-инфраструктура компании уже подверглась атаке. Преступники требовали выкуп, угрожая в противном случае нанести значительный ущерб бизнесу — вплоть до полной потери данных и вывода систем из строя.

В начале сентября 2025 года была обнаружена новая вредоносная рассылка группы BO Team с использованием запароленных RAR-архивов. В фишинговых письмах говорилось о проведении служебного расследования, связанного со злоупотреблением использования полисов ДМС. В ходе анализа было обнаружено, что BO Team обновила свой инструментарий: теперь атакующие рассылают новую версию бэкдора BrockenDoor, переписанную на C#, а также используют его для установки обновленной версии бэкдора ZeronetKit.

В конце 2025 года зафиксировано проведение совместных атак с группами 4BID и Red Likho, что отражает растущую тенденцию к координации усилий среди хактивистов. Такие группировки наносят одновременные удары по общим целям, существенно затрудняя атрибуцию: в единой инфраструктуре прослеживаются инструменты и TTP различных акторов.

Ключевым новым вектором стал шифровальщик Blackout Locker, реализованный на C/C++. Ранние версии функционировали как вайпер (wiper): они не сохраняли ключ шифрования, делая восстановление данных невозможным, а также перезаписывали MBR, блокируя загрузку ОС.

Дополнительно выявлены бэкдоры ZeronetKit (BO Team) и GoRed (Red Likho), указывающие на переход хактивистов от чистого вайпинга и вымогательства к кибершпионажу.

Атакующий арсенал дополнен кастомными инструментами, позволяющими:

- отключать устройства ввода (мыши и клавиатуры);
- создавать скрытые учетные записи администратора.

Данная группировка была замечена за атаками на компанию «Орион телеком» — одного из крупнейших интернет-провайдеров Красноярского края и других сибирских регионов. Также была произведена крупная атака на инфраструктуру российской компании в области беспилотных и роботизированных систем.

Киберпартизаны BY

Другие названия	Беларуские КиберПартызаны, Беларускія КіберПартызаны, CyberPartisans
Инструменты	FortiClient VPN, DNSCat2, Seekdns, Vasilek, Pryanik, Metasploit Framework, SharpSploit, Cobalt Strike, Mimikatz, Sliver, PowerSploit, TightVNC, Aspia Remote Desktop, PSExec, 3proxy, Gost, Evlx
География атак	Россия Беларусь
Атакуемые отрасли	Государственные учреждения Технологические компании Телекоммуникационные компании Промышленные предприятия Авиационная отрасль

Начальный вектор атак — фишинговое письмо, которое содержит инсталлятор. Этот инсталлятор устанавливает на систему легитимную программу FortiClient VPN, а также скрытно устанавливает утилиту DNSCat2, позволяющую злоумышленникам получить полный контроль над системой.

В своей деятельности группировка активно применяла бэкдор Vasilek. Особенность этого бэкдора заключается в том, что управление им (получение команд и отправка результатов их выполнения) осуществляется не через классический командный сервер (C&C), а через группу в мессенджере Telegram. По данным анализа группировки, удалось установить, что злоумышленники использовали Vasilek сразу в нескольких атаках.

Также обнаружено огромное количество утилит, применяемых для развития атаки (т.е. заражения других компьютеров в сети), из которых практически все, за редким исключением, являются утилитами с открытым исходным кодом и используются злоумышленниками «как есть», без каких-либо изменений. Эти утилиты можно условно разделить на несколько групп:

- полнофункциональные фреймворки постэксплуатации;
- инструменты для кражи учетных данных;
- средства удаленного доступа.

Из-за большого количества обнаруженных инструментов, а также их широкой распространенности представим в виде краткой справки: Metasploit, Mimikatz (с ReflectivePEInjection), PSExec, VNC, 3proxy/Gost для туннелирования, Evlx для логов.

По данным Forbes, одной из самых громких кибератак 2025 года стала совместная операция, проведенная группировкой Silent Crow и белорусской группировки «Киберпартизаны BY» против «Аэрофлота». По заявлению злоумышленников, она длилась

около года: хакеры поддерживали постоянный доступ к системам авиакомпании вплоть до финальной атаки.

DDoS-АТАКИ

По данным **Curator**, количество DDoS-атак на сетевых уровнях в 2025 году выросло на 24,18% по сравнению с 2024 годом. При этом атаки стали короче, но интенсивнее: самая мощная атака года достигла 1,57 Тбит/с (цель — букмекеры), превысив прошлогодний рекорд в 1,14 Тбит/с.

Чаще всего в 2025 году атаковали сегменты «Финтех» (21,73% атак), «Электронная коммерция» (15,95%) и «ИТ и Телеком» (9,02%). Доля промышленного сектора выросла на 357%, тогда как доля образовательных технологий (EdTech), входивших в топ-5 годом ранее, сократилась на 79%.

По оценкам команды Threat Intelligence УЦСБ SOC, основанным на анализе зафиксированных общедоступных инцидентов в 2025 году, в число наиболее активных DDoS-группировок, действовавших против российских организаций, входят IT Army of Ukraine, CyberSec (BadB), Himars DDOS и Киберкорпус.

Весомый вектор DDoS-атак в 2025 году приходился на российских телеком-провайдеров. В 2026 году следует ожидать сохранения высокой активности этих группировок, дальнейшего использования ботнетов на российских устройствах, а также усиления мощности атак и нацеленности на объекты критической инфраструктуры с целью не временного вывода сервисов из строя, а их долгосрочной деградации или уничтожения.

Отдельным трендом, меняющим ландшафт угроз, выступает конвергенция DDoS с ransomware. По данным анализа инцидентов 2025 года, операторы ПО для вымогательства все чаще используют DDoS-атаки как второй этап давления после шифрования данных. Это меняет саму природу угрозы — DDoS перестает быть просто атакой на доступность и становится инструментом переговоров о выкупе.

Мультипликатором угроз становятся технологии искусственного интеллекта: ИИ-алгоритмы позволяют генерировать адаптивный вредоносный трафик, обходить типовые средства защиты и достоверно имитировать человеческое поведение (включая голос и видео), делая атаки практически неотличимыми от легитимной активности.

Особый фокус хактивистских групп сохранится на государствах в зоне геополитической напряженности и транснациональных корпорациях, чья деятельность воспринимается как поддержка одной из сторон конфликта. Растущая взаимозависимость компаний в цифровых экосистемах создает риск каскадных эффектов: компрометация одного поставщика способна запустить цепную реакцию сбоев у его заказчиков и контрагентов, многократно усиливая последствия даже локальной атаки.

В этих условиях традиционные периметровые решения демонстрируют снижение эффективности. Основными мерами защиты становятся геофильтрация, rate-limit и профессиональные сервисы защиты, однако их применение требует постоянной адаптации:

алгоритмы DDoS-атак следующего поколения уже учатся обходить статические правила. Ключевым фактором успеха становится переход от реактивной модели («обнаружил — отразил») к проактивной — с непрерывным анализом телеметрии, поведенческими аномалиями на базе ИИ и распределенной архитектурой очистки трафика, способной выдерживать амплитудные атаки в десятки терабит в секунду без деградации сервиса для легитимных пользователей.

УТЕЧКИ ДАННЫХ

По данным **F6**, в 2025 году количество выявленных утечек баз данных российских компаний сократилось до 225 случаев против 455 годом ранее. Суммарно утечки российских компаний 2025 года содержали более 767 млн строк с данными пользователей. Основные публикации, как и прежде, приходятся на Telegram-каналы (187 из 225).

Собственные исследования УЦСБ SOC не только подтверждают эту динамику, но и позволяют детализировать портрет современной утечки. В ходе проведенного анализа по данным ЭАЦ InfoWatch пришли к выводу, что средний объем одной утечки персональных данных в России достиг 3,27 млн записей — на 26% больше, чем в 2024 году. В структуре утекшей информации преобладают персональные данные: 74% от общего объема. Telegram остается основным каналом распространения — 72% публикаций, доля даркнета и закрытых форумов — 26%.

По мнению команды Threat Intellegence УЦСБ SOC, официальная статистика утечек не отражает полного объема скомпрометированной информации. Значительная часть инцидентов в организациях, которые не обязаны отчитываться перед регуляторами об инцидентах, остается за рамками публичных источников, поэтому реальное число утечек может быть существенно выше зафиксированного.

Наиболее пострадавшими отраслями в 2025 году стали ретейл и интернет-магазины, государственный сектор, авиация, профессиональные услуги, здравоохранение и информационные технологии.

Инциденты стали более масштабными, а используемые злоумышленниками методы — более целенаправленными. Отдельные крупные утечки затрагивают сотни миллионов записей, что многократно повышает потенциальный ущерб и охват целевых групп. При рассмотрении статистики в разрезе отраслевой принадлежности организации за исключением единичных аномально крупных инцидентов видно, что за последние два года средний объем одной утечки в отрасли составляет около 1,8–1,9 млн записей, а совокупный объем скомпрометированных данных за год превышает 1,6 млрд, при этом доля инцидентов, затрагивающих более 10 миллионов записей, выросла в три раза.

Злоумышленники все чаще концентрируются на атаках против крупных централизованных хранилищ — государственных информационных систем, телеком-операторов, платформ электронной коммерции и медицинских сервисов — а не на разрозненных и относительно небольших базах. Именно на эти сектора приходится от 55 до 75% всех крупных инцидентов (свыше 1 млн записей). Такой подход делает инциденты более значимыми и сложными для ликвидации последствий, а скомпрометированные данные — долгосрочным ресурсом для злоумышленников: в 70% крупных утечек полное устранение последствий невозможно, а информация продолжает использоваться злоумышленниками на протяжении длительного времени после инцидента.

Полученные данные активно применяются в фишинговых рассылках, целевых сценариях социальной инженерии против сотрудников и атаках с вымогательством. Ускоренное распространение утечек в мессенджерах и закрытых каналах снижает управляемость последствиями и делает повторное использование данных практически необратимым, что повышает общую тяжесть и устойчивость рисков, связанных с утечками данных.

ТОП-10 УТЕЧЕК ДАННЫХ 2025 ГОДА

Ниже представлены наиболее значимые, по мнению команды Threat Intelligence УЦСБ SOC, инциденты с утечками данных — как публично раскрытые (из открытых источников и официальных уведомлений), так и непубличные, выявленные в ходе пассивного мониторинга теневых каналов утечек.

1. «Ростелеком»

В январе Silent Crow заявили о компрометации данных подрядчика, опубликовав 154 тыс. email-адресов и 101 тыс. номеров телефонов клиентов. Среди них — базы данных zakupki.rostelecom.ru и rt.ru, письма акционеров, номера телефонов, адреса и запросы в техническую поддержку.

Ростелеком прокомментировал утечку (по данным ТАСС МЕДИА), при этом заявив, что она произошла у подрядчика, обслуживавшего эти ресурсы.

2. Страховая компания

В январе Silent Crow выложили в сеть персональные данные примерно 500 тысяч клиентов российского страховщика.

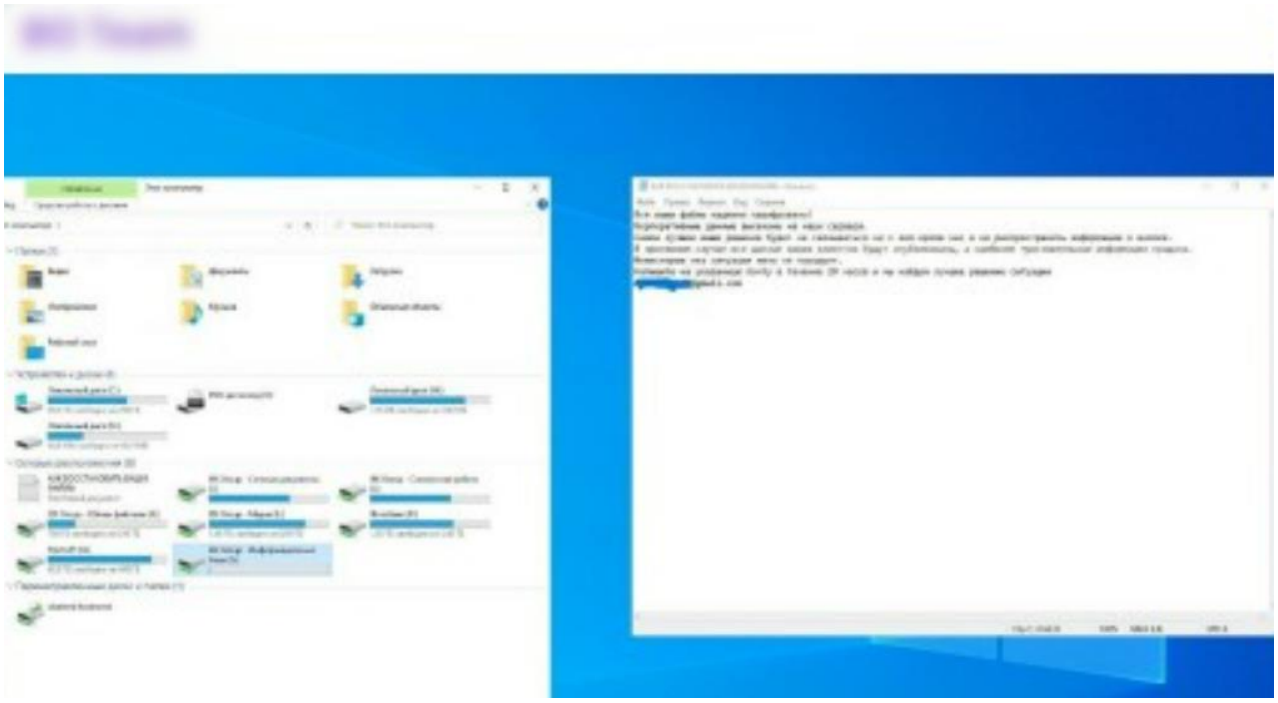
Среди прочего хакеры сообщили об утечке следующей информации: Ф.И.О., дата рождения, телефон (68 474 уник.), электронная почта (33 930 уник.), пароль в хэше, должность и место работы. Согласно заявлениям атакующих, данные базы актуальны на июнь 2024 года.

3. Крупнейший российский производитель и поставщик электротехнического и светотехнического оборудования

В апреле BO Team взломали российского производителя электротехнического оборудования и зашифровали его инфраструктуру.

Вход в систему осуществлен через фишинговую рассылку. Для расшифровки данных злоумышленники потребовали 50 000$ в BTC. После получения выкупа хакеры не восстановили доступ к данным.

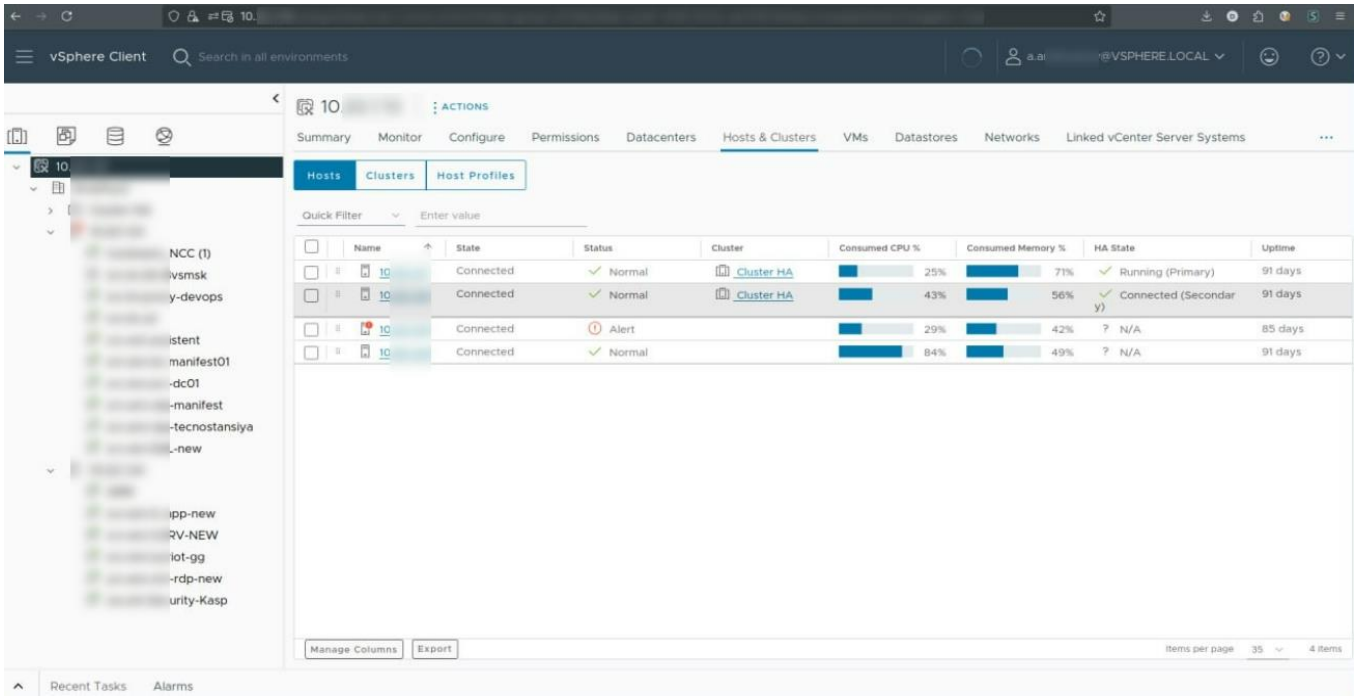
По заявлению хакеров, они смогли уничтожить:
200 виртуальных машин, 55 серверов, 18 ТБ резервных копий.



Всего удалось зашифровать более 1000 хостов - рабочих станций, на которых находилось более 300 ТБ ценных данных.

4. Российская компания в области беспилотных и роботизированных систем

В июле Ukrainian Cyber Alliance и BO Team заявили об атаке на компанию, хищении ее данных о разработках БПЛА и выводе инфраструктуры из строя. Злоумышленники утверждали, что украли терабайты документов, включая почту, чертежи, техдокументацию, исходный код, бухгалтерию и договора. В качестве доказательств они опубликовали скриншоты панелей управления, переписки сотрудников и образцы внутренних документов.



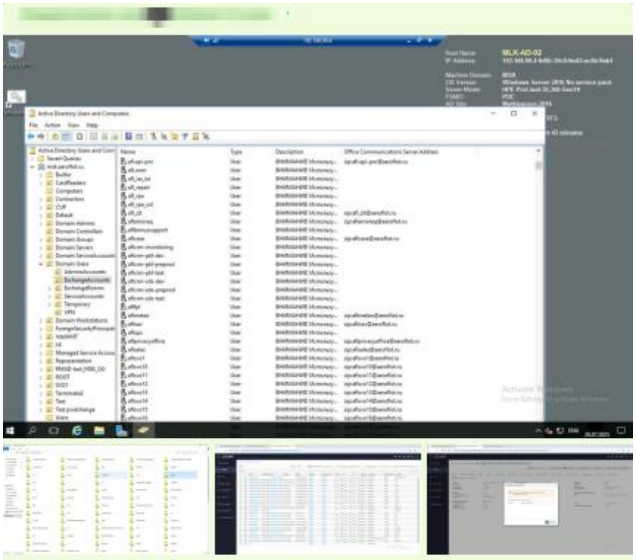
5. ПАО «Аэрофлот»

Группировки «Киберпартизаны BY» и Silent Crow в июле заявили об уничтожении ИТ-инфраструктуры компании и хищении персональных и медицинских данных сотрудников.

По заявлению злоумышленников, им удалось получить и выгрузить полный массив баз данных истории перелетов, скомпрометировать все критические корпоративные системы, включая CREW, Sabre, SharePoint, Exchange, КАСУД, Sirax, CRM, ERP, 1С, DLP и другие, а также получить контроль над персональными компьютерами сотрудников, включая высшее руководство. Кроме того, они скопировали данные с серверов прослушки, включая аудиозаписи телефонных разговоров и перехваченные коммуникации, и извлекли данные из систем наблюдения и контроля за персоналом.

В заявлении также указывалось, что хакеры получили доступ к 122 гипервизорам, 43 инсталляциям виртуализации ZVIRT, около сотни iLO-интерфейсов для управления серверами и четырем кластерам Proxmox. В результате их действий было уничтожено около 7 000 серверов — физических и виртуальных. Объем полученной информации составил 12 ТБ баз данных, 8 ТБ файлов с Windows Share и 2 ТБ корпоративной почты.

По информации из СМИ, причиной масштабного сбоя в работе крупной авиакомпании стала хакерская атака. Факт атаки подтвердили в Генпрокуратуре, где возбуждено уголовное дело по ч. 4 ст. 272 УК РФ (неправомерный доступ к компьютерной информации).



Вместе с коллегами из Киберпартизаны BY, заявляем об успешном проведении продолжительной и масштабной операции, в результате которой была полностью скомпрометирована и уничтожена внутренняя IT-инфраструктура "Аэрофлот — российские авиалинии".

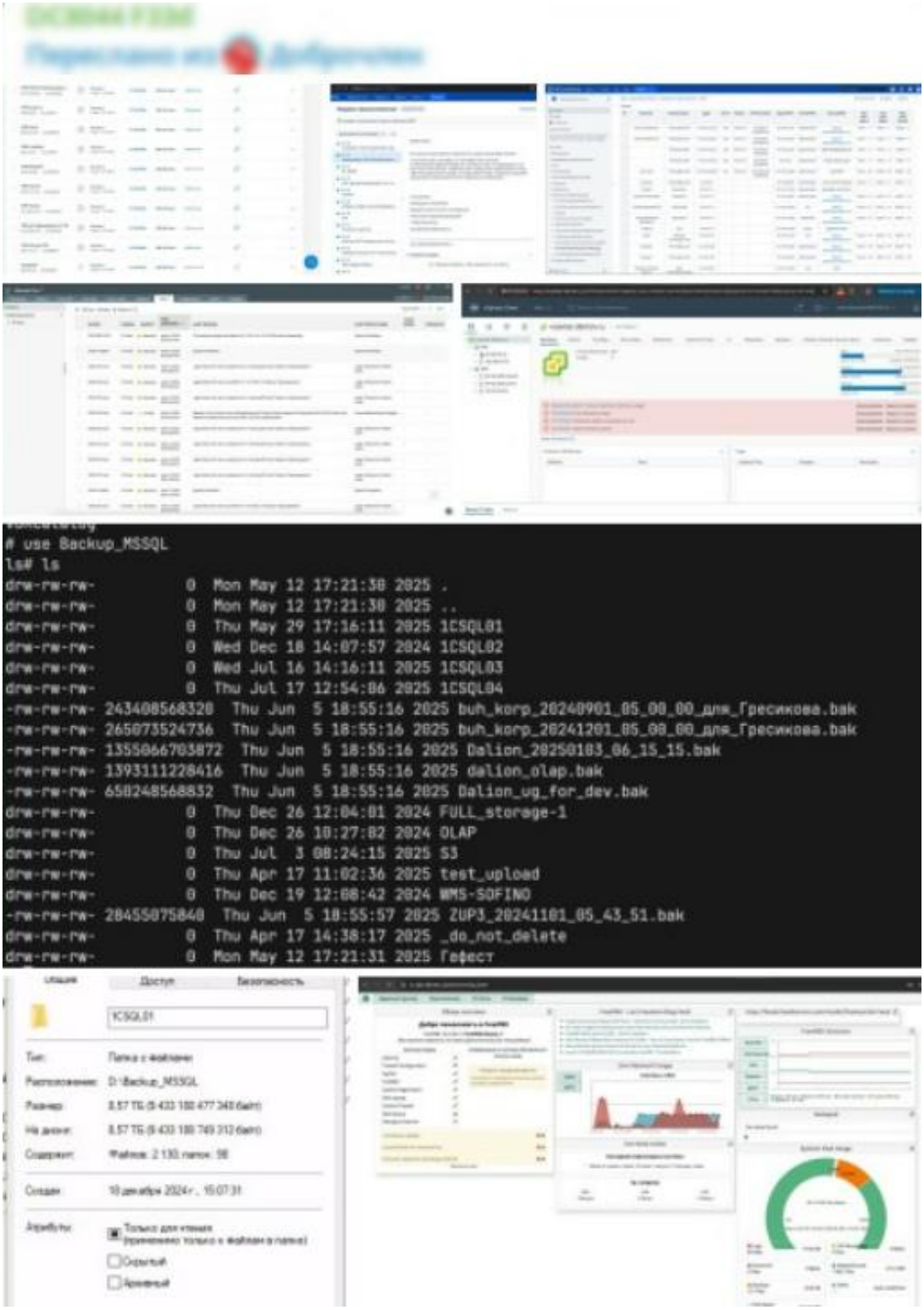
На протяжении года мы находились внутри их корпоративной сети, методично развивая доступ, углубляясь до самого ядра инфраструктуры — Tier0. Нам удалось:

Получить и выгрузить полный массив баз данных истории перелетов. Скомпрометировать все критические корпоративные системы, включая: **CREW**, **Sabre**, **SharePoint**, **Exchange**, **КАСУД**, **Sirax**, **CRM**, **ERP**, **1C**, **DLP** и другие.
Получить контроль над персональными компьютерами сотрудников, включая высшее руководство.
Скопировать данные с серверов прослушки, включая аудиозаписи телефонных разговоров и перехваченные коммуникации. Извлечь данные из систем наблюдения и контроля за персоналом.

6. Крупнейшая федеральная розничная сеть магазинов

В июне хакеры скомпрометировали сеть магазинов: выгрузили базы данных и уничтожили серверы. В открытый доступ попали персональные данные клиентов. Среди опубликованных материалов — снимки внутренней переписки сотрудников, корпоративной почты, ИТ-инфраструктуры, а также кадры с камер видеонаблюдения торговых точек и складов.

В качестве семпла злоумышленниками был предоставлен файл на 10 000 строк, который, по утверждению хакеров, содержит персональные данные покупателей.

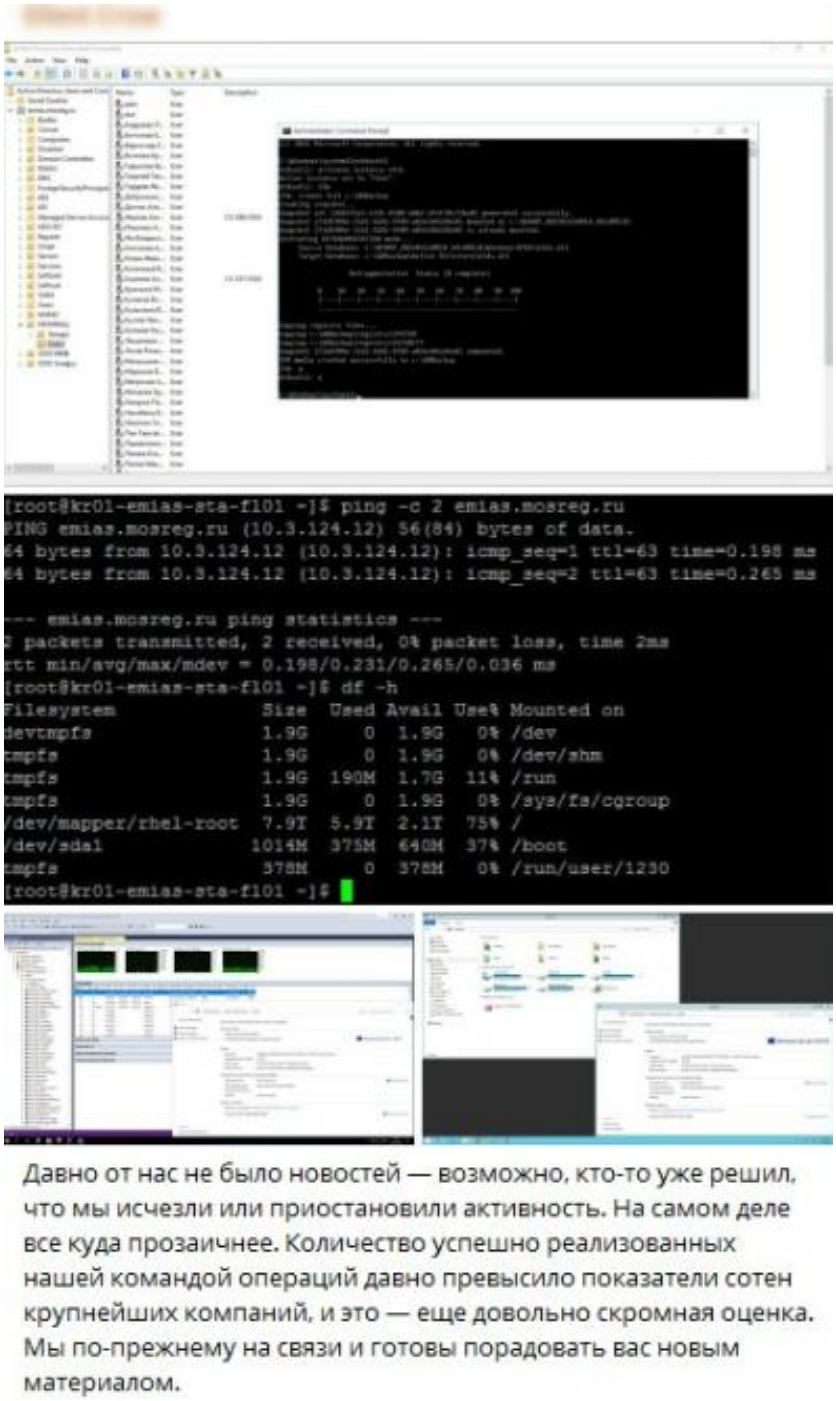


```
# use Backup_MSSQL
ls# ls
drw-rw-rw-          0  Mon May 12 17:21:30 2025 .
drw-rw-rw-          0  Mon May 12 17:21:30 2025 ..
drw-rw-rw-          0  Thu May 29 17:16:11 2025 1CSQL01
drw-rw-rw-          0  Wed Dec 18 14:07:57 2024 1CSQL02
drw-rw-rw-          0  Wed Jul 16 14:16:11 2025 1CSQL03
drw-rw-rw-          0  Thu Jul 17 12:54:06 2025 1CSQL04
-rw-rw-rw- 243408568328  Thu Jun  5 18:55:16 2025 buh_korp_20240901_05_00_00_для_Гресикова.bak
-rw-rw-rw- 265073524736  Thu Jun  5 18:55:16 2025 buh_korp_20241201_05_00_00_для_Гресикова.bak
-rw-rw-rw- 1355066703872  Thu Jun  5 18:55:16 2025 Dalion_20250103_06_15_15.bak
-rw-rw-rw- 1393111228416  Thu Jun  5 18:55:16 2025 dalion_olap.bak
-rw-rw-rw- 658248568832  Thu Jun  5 18:55:16 2025 Dalion_ug_for_dev.bak
drw-rw-rw-          0  Thu Dec 26 12:04:01 2024 FULL_storage-1
drw-rw-rw-          0  Thu Dec 26 10:27:02 2024 OLAP
drw-rw-rw-          0  Thu Jul  3 08:24:15 2025 S3
drw-rw-rw-          0  Thu Apr 17 11:02:36 2025 test_upload
drw-rw-rw-          0  Thu Dec 19 12:08:42 2024 WMS-SOFINO
-rw-rw-rw- 28455075840  Thu Jun  5 18:55:57 2025 ZUP3_20241101_05_43_51.bak
drw-rw-rw-          0  Thu Apr 17 14:38:17 2025 _do_not_delete
drw-rw-rw-          0  Mon May 12 17:21:31 2025 Гефест
```

7. Медицинская информационная система

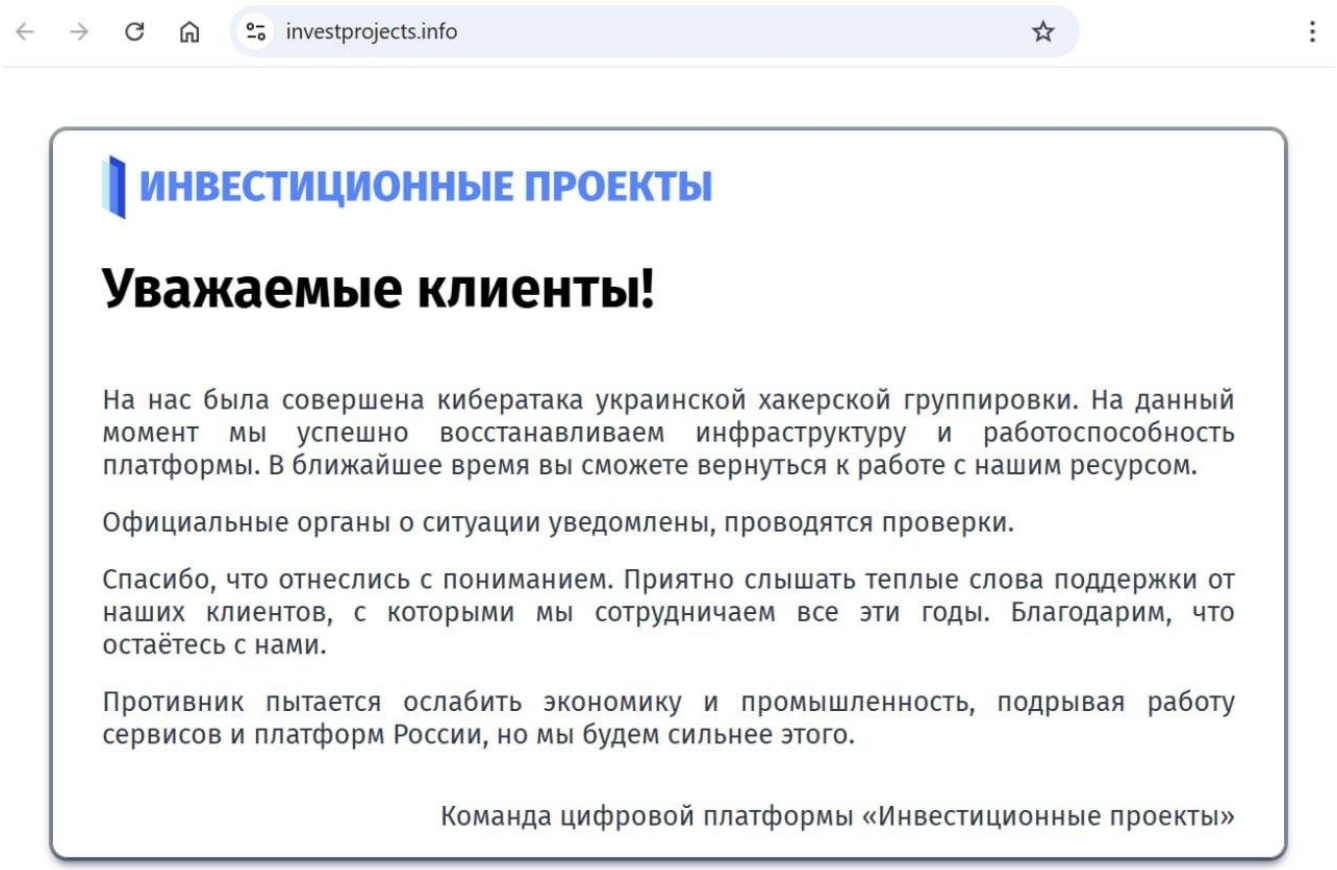
В июле хакеры получили полный доступ к внутренней инфраструктуре медицинской информационной системы, включая контроллер домена, базы данных и внутреннюю документацию.

По заявлению злоумышленников, произошла утечка данных медицинских работников и пациентов, обслуживаемых в Москве и Московской области. Общий объем выгруженных данных составил около 17 ТБ. В них содержатся не только персональные данные, но и медицинская информация, включая диагнозы и схемы лечения.



8. Платформа «Инвестиционные проекты»

В августе Cyber Anarchy Squad совершила кибератаку на платформу, агрегирующую информацию об инвестпроектах в России и странах ЕАЭС. В ходе атаки злоумышленниками было заявлено о частичном уничтожении инфраструктуры, краже внутренней документации и переписок сотрудников в Telegram. Кроме того, CAS опубликовала часть якобы похищенных данных с целью создать повод для штрафа за утечку. После восстановления сайта всем пользователям в целях безопасности сбросили пароли.

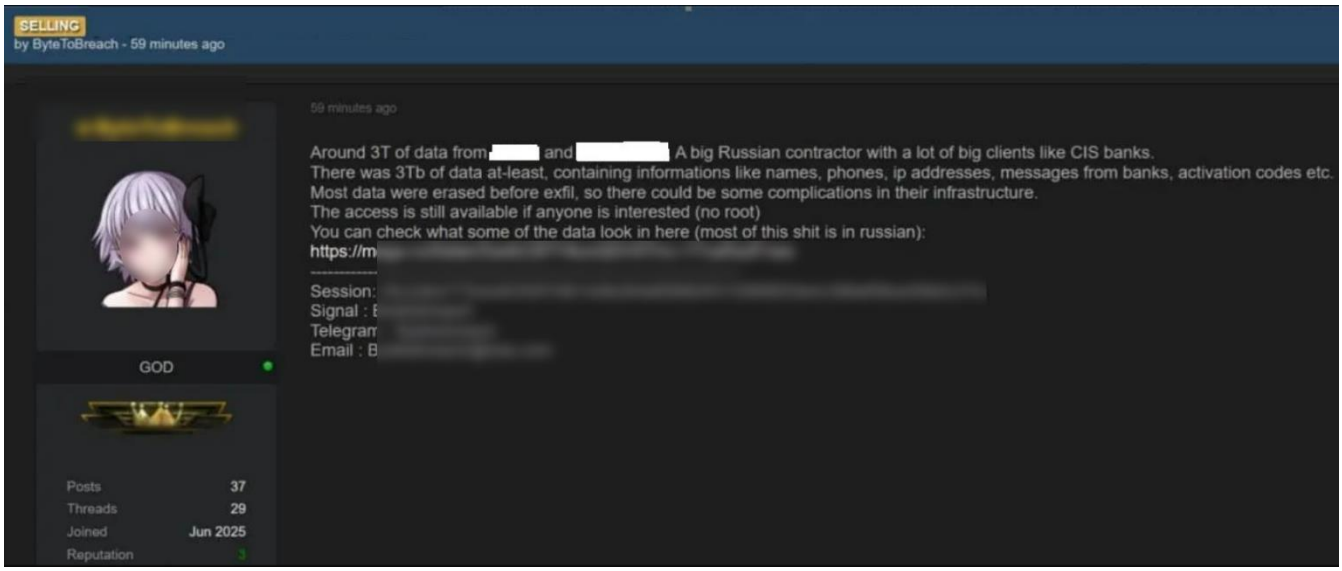


9. Профессиональные сервисы массовых рассылок для среднего и крупного бизнеса

В октябре злоумышленник опубликовал данные о взломе крупных российских подрядчиков, обслуживающих множество клиентов из банковского сектора СНГ.

Объем утечки составил не менее 3 ТБ, включая имена, номера телефонов, IP-адреса, банковские SMS-сообщения, коды активации и прочие чувствительные данные. Источники: поддомены компании, MongoDB (несколько хостов по сервисам), Redis (сессии) и ElasticSearch (сканирование сетевых источников).

Большая часть данных была удалена до эксфильтрации.



10. ИТ-компания, специализирующаяся на разработке ПО, автоматизации бизнес-процессов и государственных систем

В декабре анонимная группировка заявила о взломе одной ИТ-компании — в сеть были выложены технические данные и внутренняя переписка.

По словам злоумышленников, им удалось в течение нескольких месяцев находиться во внутренней инфраструктуре, получить доступ к исходному коду, технической документации и рабочей переписке.

Злоумышленники заявили, что все полученные данные планируют передать журналистам и правозащитным организациям, а также выложить в открытый доступ.

Отдельно упоминалось о 30 млн учетных записей, в качестве доказательства был опубликован скриншот внутреннего созвона, размещенный в официальных социальных сетях компании.

ЭВОЛЮЦИЯ УГРОЗ. ТРЕНДЫ

На основе массива данных, собранных и проанализированных командой Threat Intelligence УЦСБ SOC в течение 2025 года, а также с учетом текущих наблюдений за действиями злоумышленников, мы выделяем устойчивые закономерности в эволюции киберугроз для российского сегмента. Ниже приведены ключевые тренды по категориям уязвимостей, активности APT-группировок и утечек данных, а также сформированный на их основе прогноз на 2026 год, который позволяет скорректировать стратегии защиты с учетом прогнозируемых векторов атак.

Уязвимости

Анализ ландшафта уязвимостей за 2025 год выявил смещение фокуса атакующих и изменение структуры рисков для корпоративного сектора:

- **Рост числа инцидентов, связанных с отечественным ПО**. В условиях активной миграции на локальные решения злоумышленники переориентировались на поиск уязвимостей в российском стеке технологий. Наиболее показательны случаи с цепочками RCE в TrueConf Server (BDU:2025-10114...10116), эксплуатировавшимися группой Head Mare, а также критическая уязвимость в Kaspersky Endpoint Security (BDU:2025-09471), требующая повышенного внимания к обновлениям защитного ПО.
- **Доминирование уязвимостей в продуктах Microsoft**. Уязвимости в продуктах Microsoft составляют порядка 43% среди всех уязвимостей, активно используемых злоумышленниками в текущих атаках. Ключевой категорией остаются уязвимости повышения привилегий (EoP) в компонентах ядра Windows и Hyper-V (CVE-2025-21333 и др.), используемые для закрепления и развития атак после первоначального проникновения.
- **Атаки на инфраструктурный периметр**. Уязвимости в сетевом оборудовании и средствах защиты (Fortinet, Cisco) позволяют нивелировать защиту периметра, предоставляя атакующим прямой доступ во внутренние сегменты сети.
- **Сокращение окна экспозиции (Zero-Day → Wild)**. Наблюдается тренд на сверхбыструю интеграцию уязвимостей в арсенал APT-групп после публикации PoC. Примеры:
  - CVE-2025-33053: Weaponized zero-day, эксплуатировавшийся группировкой Stealth Falcon до выхода патча через WebDAV и .url файлы.
  - CVE-2025-55182 (React2Shell): Появление публичного PoC привело к немедленным атакам со стороны государственных хакерских групп (Earth Lamia), что подтверждает необходимость проактивной защиты веб-фреймворков.

Анализ трендовых уязвимостей 2025 года показывает устойчивый рост числа критических инцидентов как в отечественном, так и в зарубежном ПО. Основные риски связаны с уязвимостями удаленного выполнения кода (RCE), повышения привилегий (EoP) и обхода периметровой защиты. В условиях, когда оперативное обновление проблемных компонентов невозможно, требуется реализация комплекса компенсирующих мер.

APT-группировки

Основные тренды включают рост активности APT-группировок на государственный и промышленный сектор, а также рост консолидации хактивистких группировок стран СНГ.

Согласно аналитике команды Threat Intelligence УЦСБ SOC, по итогам 2025 года зафиксировано следующее количество APT-группировок, проявлявших активность в отношении секторов экономики:

В 2025 году российский государственный сектор оставался приоритетной целью APT-группировок. По результатам анализа открытых источников командой Threat Intelligence УЦСБ SOC зафиксировано сохранение ключевых трендов 2023–2024 годов: кибершпионаж, саботаж инфраструктуры и эксфильтрация данных. Количество APT-инцидентов выросло на 25-30%, при этом основным фокусом оставались геополитически мотивированные операции.

Наиболее заметный тренд 2025 года — атаки через доверительные отношения. Доля инцидентов, начинавшихся с компрометации подрядчика, увеличилась в 4 раза по сравнению с 2024 годом, достигнув 30%. Одновременно доля атак через уязвимости веб-приложений

снизилась на 15 процентных пунктов — до 31%. Еще 30% сложных инцидентов связаны со скомпрометированными сервисами или учетными записями сотрудников, 15% — с фишингом.

Эти данные подтверждают необходимость усиления защиты: сегментация сети, соблюдение принципа минимальных привилегий, мониторинг событий ИБ, повышения осведомленности сотрудников при работе с электронной почтой, строгого соблюдения парольной политики и своевременного обновления программного обеспечения.

Утечки данных

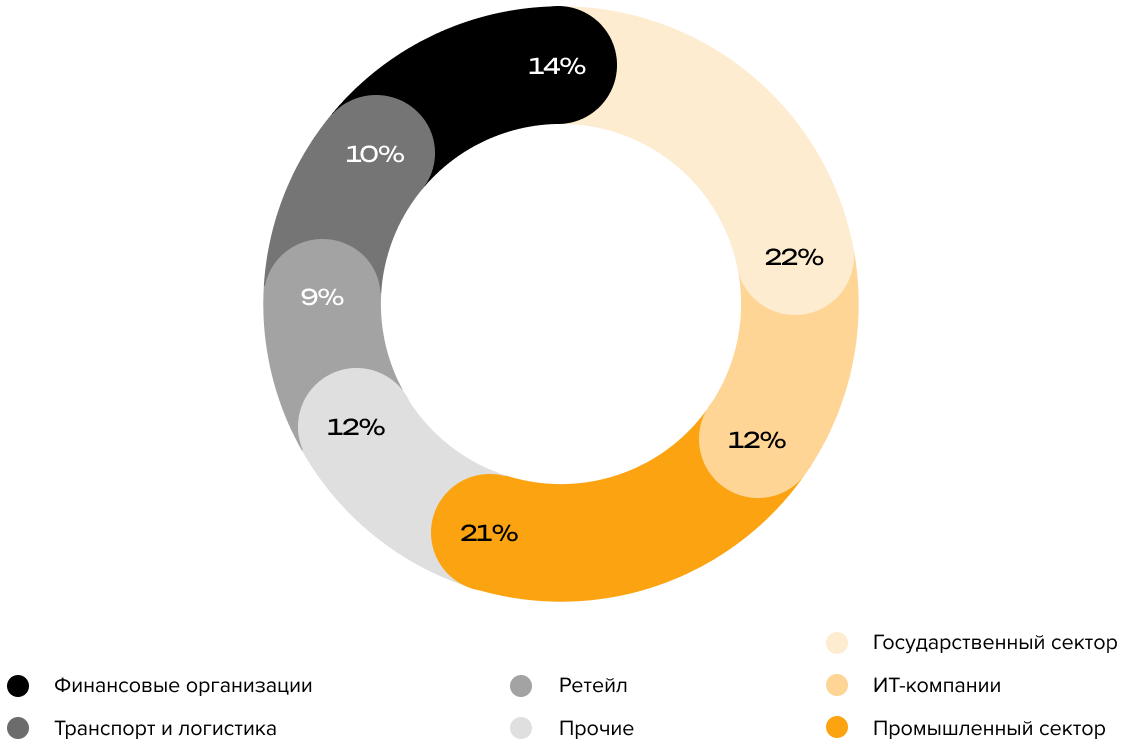
Утечки данных в 2026 году остаются одним из главных трендов в кибербезопасности, демонстрируя устойчивый рост масштабов и числа инцидентов. Глобально фиксируется увеличение количества атак, направленных на компрометацию персональной и корпоративной информации.

В России в 2025 году число утечек сократилось на 13–18%, однако объем скомпрометированных данных вырос. Усиление рисков связано с появлением новых каналов распространения украденной информации, включая вторичный рынок на даркнете.

Основные публикации по-прежнему приходятся на Telegram-каналы, несмотря на блокировки, а масштабные утечки данных продолжают усиливать угрозу повторного использования скомпрометированной информации в фишинговых и ransomware-атаках. Лишь в половине случаев хакеры публикуют реальные данные, в то время как около трети утечек из госорганов оказались фейковыми — компиляциями старых баз и общедоступной информации. Фейковые публикации киберпреступники используют для повышения репутации на хакерских форумах, манипуляции общественным мнением, провокации паники и даже разведки: они изучают реакцию компаний для точечных фишинговых атак или социальной инженерии.

Согласно данным анализа инцидентов из открытых источников, проведенного специалистами команды Threat Intelligence УЦСБ SOC, лидирующую позицию в «группе риска» занимает государственный сектор (22% инцидентов, обусловлено высокой концентрацией чувствительных данных и активной цифровизацией госуслуг), промышленность (21%, за счет сложных производственных цепочек и множества подрядчиков), финансовые организации (14%, сохраняют привлекательность для финансово мотивированных группировок), ИТ-компании (12%, как поставщики услуг и носители доступа к инфраструктуре клиентов), транспорт и логистика (10%), ретейл (9%), а также прочие сектора (12%). Данные из утечек активно используются для фишинга: в 2025 году количество исследуемых фейковых онлайн-ресурсов выросло в 1,5 раза.

РАСПРЕДЕЛЕНИЕ ДОЛИ ИНЦИДЕНТОВ ПО КЛЮЧЕВЫМ СЕКТОРАМ ЭКОНОМИКИ



ОЖИДАЕМЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ И ПРОГНОЗНЫЕ ОЦЕНКИ НА 2026 ГОД

В 2026 году кибератаки на российские компании все чаще будут приводить к комплексному ущербу: помимо блокировки доступа к данным через шифрование, хакеры систематически крадут информацию для последующего вымогательства или угроз публикацией. Такие инциденты парализуют ключевые операции и подрывают репутацию.

По мере развития цифровизации под угрозой окажутся промышленные системы управления, IoT-оборудование и смарт-датчики — их сбой спровоцирует простои на производстве и нарушения в критической инфраструктуре. Ключевой тенденцией станет не рост «мощности» DDoS-атак, а их усложнение и переход к прикладному характеру как инструменту давления. Такие атаки будут чаще использоваться с целью получения выкупа за их прекращение — например, в форме Ransom-DDoS, когда злоумышленники сочетают DDoS с угрозами утечки данных или блокировкой сервисов до оплаты.

Рост атак через цепочки поставок усугубит риски: злоумышленники будут использовать уязвимости подрядчиков и ИТ-сервис провайдеров для проникновения в корпоративные сети, что чревато масштабными последствиями. Параллельно серьезной угрозой останется фишинг, который за счет массового применения LLM-инструментов становится одновременно более дешевым и более прицельным. Генерация корректных, стилистически выверенных писем на нужном языке и контексте снижает порог распознавания таких атак пользователями и превращает фишинг в стабильный и эффективный инструмент первичного доступа.

Наконец, регуляторные санкции усилят давление: жертвы утечек столкнутся с крупными штрафами по законам о персональных данных и ИБ, а топ-менеджеры рискуют уголовным преследованием.

Привычные схемы проникновения останутся основным инструментом злоумышленников в 2026 году. Невысокая сложность подготовки, минимальные затраты и стабильная результативность обеспечивают базовым векторам лидирующие позиции в статистике инцидентов. Среди преобладающих техник выделяются:

- социальная инженерия через электронную почту и мессенджеры с целью перехода на поддельные страницы аутентификации либо запуска вложенного кода;
- подбор и повторное применение учетных данных, извлеченных из публичных утечек, в первую очередь для атак на сервисы удаленного доступа (RDP, корпоративные VPN-шлюзы, веб-интерфейсы почтовых систем OWA);
- выявление на периметре организаций известных, но не устраненных уязвимостей в сетевом оборудовании, веб-приложениях и системах публикации документов;

- применение штатных утилит самой операционной системы и легальных средств удаленного администрирования, включая PowerShell и AnyDesk, для продвижения внутри скомпрометированной сети.

В совокупности указанные методы формируют до 70-80% от общего объема расследуемых инцидентов в корпоративном сегменте, что выводит на первый план задачи по усилению контроля учетных записей, своевременному устранению уязвимостей на внешнем периметре и развитию поведенческого анализа на конечных устройствах.

Семь киберугроз 2026 года и рекомендации по противодействию

На основе анализа ландшафта киберугроз 2025 года эксперты Threat Intelligence УЦСБ SOC разработали практический комплекс мер противодействия для российских организаций. Рекомендации охватывают защиту ИТ-инфраструктуры, промышленных систем и цепочек поставок от наиболее актуальных векторов атак.

1. В 2026 году угроза для российских организаций останется комплексной: шифрование и дальнейшая кража, и угрозы, связанные с публикацией данных.
    - Внедрить систему резервного копирования с поддержкой защитного преобразования, обеспечивающую создание неизменяемых снимков данных. Такие копии должны храниться в режиме «только для чтения» на уровне файловой системы или хранилища с блокировкой на удаление и модификацию в течение заданного периода (от нескольких часов до месяцев). Это гарантирует сохранность данных при атаках вирусов-шифровальщиков и позволяет восстановить работоспособность без выплаты выкупа.
    - Проводить регулярное обновление программного обеспечения, включая операционные системы, прикладные и серверные решения, для своевременного закрытия известных уязвимостей, используемых злоумышленниками.
    - Внедрять и поддерживать современные антивирусные и endpoint-защитные решения, способные обнаруживать подозрительную активность и блокировать вредоносные программы на ранних этапах.
    - Ограничивать сетевой доступ за счет закрытия неиспользуемых портов, разрешения только необходимых протоколов и сервисов и применения строгой фильтрации трафика на уровне межсетевых экранов.
    - Контролировать и минимизировать удаленный доступ, обеспечивая его только через защищенные каналы и только для утвержденных сценариев использования.
    - Использовать VPN с обязательной аутентификацией для всех удаленных подключений, включая доступы сотрудников и внешних подрядчиков, а также фиксировать и мониторить все удаленные сессии.

- Внедрять сегментацию сети, разделяя инфраструктуру на изолированные сегменты для снижения риска горизонтального распространения вирусов и других угроз внутри корпоративной среды.
- Организовать строгую политику управления паролями и многофакторной аутентификацией, включая требование сложных и уникальных паролей, их регулярную смену и обязательное применение MFA на критических системах и сервисах.
- Усиливать защиту электронной почты за счет внедрения фильтров, sandbox-анализа вложений, url-фильтрации и контроля подозрительных сообщений, чтобы снизить вероятность попадания зараженных программ и фишинговых ссылок в инфраструктуру.
- Регулярно обучать сотрудников основам информационной безопасности, включая распознавание фишинга, недопущение открытия подозрительных вложений и ссылок, а также практики безопасного хранения учетных данных, использования многофакторной аутентификации и разграничения доступа к ресурсам.

2. Угрозы расширятся за пределы ИТ-инфраструктуры: критические уязвимости промышленных систем управления, IoT и смарт-датчиков.
   - Настроить WAF и NGFW/IPS на блокирование эксплуатационных запросов для выявленных критических уязвимостей без остановки сервисов.
   - Изолировать критически важные и уязвимые серверы в отдельных VLAN с ограничением доступа только через доверенные административные узлы и VPN с MFA.
   - Организовать регулярное управление уязвимостями и патч-менеджмент, включая своевременное обновление операционных систем, прикладного программного обеспечения и middleware, а также отключение или изоляцию компонентов без поддержки и с известными уязвимостями.
3. DDoS-атаки продолжат движение к целевой и прикладной модели (Ransom-DDoS, давление на бизнес-процессы).
   - Фильтровать входящий трафик по геолокации, блокировать обращения к веб-ресурсам из зарубежных стран.
   - Заблокировать IP-адреса, принадлежащие хостинг-провайдерам, предоставляющим услуги аренды VPS-серверов и выделенных proxy-серверов.
   - Настроить блокировку запросов к веб-ресурсам, в которых HTTP-заголовок Referer содержит адреса и/или ключевые слова атакующих доменов.
   - Настроить ограничение по количеству запросов в секунду с одного IP-адреса (rate-limit) к целевым веб-ресурсам.

- Инициировать обращение к профильным поставщикам с последующей установкой решения по защите web-ресурсов от DDoS-атак.

4. Цепочки поставок и подрядчики станут одним из ключевых каналов проникновения в корпоративные сети.
    - Организовать разделение информационных сред так, чтобы данные Заказчика были физически и логически отделены от собственных данных подрядчика с отдельным сетевым сегментом и строгим контролем доступа между ними.
    - Обеспечить контролируемый удаленный доступ, при котором все подключения к инфраструктуре заказчика осуществляются исключительно через VPN с обязательной многофакторной аутентификацией (MFA) и использованием системы управления привилегированным доступом (PAM).
    - Оснастить рабочие места сотрудников средствами защиты конечных точек, установив и поддерживая антивирусные решения и средства класса EDR на всех устройствах, имеющих доступ к инфраструктуре заказчика.
    - Внедрить системное управление уязвимостями путем регулярного обновления операционных систем и прикладного программного обеспечения, а также оперативного устранения известных уязвимостей на критических компонентах.
    - Применить принцип наименьших привилегий не только для своих сотрудников, но и для учетных записей подрядчиков, предоставляя доступ только к тем данным и системам, которые необходимы для выполнения конкретной задачи, и исключив административные права в стандартной пользовательской деятельности.
    - Установить и контролировать стандарты управления паролями: использовать сложные и уникальные пароли для каждого сервиса и регулярно их менять в соответствии с политикой безопасности организации.
    - Обеспечить безопасный обмен конфиденциальной информацией, передавая данные заказчика только по защищенным каналам связи с применением криптографического шифрования и контроля целостности.
    - Запретить использование несанкционированных устройств и каналов связи, включая подключение личных USB-накопителей и использование личных мессенджеров и некорпоративных сервисов для передачи рабочих и конфиденциальных документов.
    - Организовать мониторинг и оперативное реагирование на инциденты, включая постоянный контроль сети и конечных точек. В частности, можно использовать сервис мониторинга от УЦСБ SOC, обеспечивающий круглосуточное выявление аномальной активности, оперативную блокировку атак, а также полное сопровождение цикла реагирования — от обнаружения и анализа инцидента до нейтрализации, устранения последствий и внедрения мер, исключающих повторное возникновение угроз.

5. Фишинг и социальная инженерия, усиленные LLM-инструментами, останутся самым эффективным и устойчивым вектором первичного доступа.
    - 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.
6. Регуляторное давление и риск уголовной ответственности топ-менеджмента увеличат стоимость утечек и атак.
    - Внедрить систему автоматизированного контроля соответствия требованиям ИБ и НПА, в частности, можно использовать платформу CheckU от УЦСБ для организации централизованного внутреннего аудита ИБ. CheckU обеспечивает единые методики проверок по требованиям КИИ, ПДн (152-ФЗ), 187-ФЗ, отраслевым и корпоративным стандартам, автоматизацию сбора и анализа свидетельств, формирование регуляторных отчетов и контроль выполнения мероприятий по устранению несоответствий, что снижает вероятность крупных штрафов и уголовных претензий к руководству.
7. Большинство киберинцидентов обусловлено базовыми векторами: социальной инженерией, компрометацией учетных данных, устаревшими CVE и злоупотреблением инструментами.
    - Внедрить и поддерживать многофакторную аутентификацию для всех критически значимых систем, удаленных шлюзов и облачных сервисов, чтобы снизить риск компрометации учетных данных.
    - Организовать регулярное управление уязвимостями и патч-менеджмент, включая своевременное обновление операционных систем, прикладного программного обеспечения и middleware, а также отключение или изоляцию компонентов без поддержки и с известными уязвимостями.
    - Настроить WAF и NGFW/IPS на блокирование эксплуатационных запросов для выявленных критических уязвимостей без остановки сервисов.
    - Ужесточить контроль доступа на основе принципа наименьших привилегий, ограничив права пользователей и сервисных аккаунтов до минимально необходимого набора привилегий.

- Внедрить и настроить решения класса EDR/XDR на конечных точках и ключевых серверах с поведенческим анализом и обнаружением аномалий, включая признаки эскалации привилегий, запуск нестандартных оболочек и подозрительных скриптов.
- Ограничить и контролировать использование административных и служебных инструментов (powerShell, wmi, psExec, любые удаленные средства администрирования), запретив их применение в типовых сценариях и введя механизм аудита и одобрения.
- Внедрить и поддерживать технологии защиты от фишинга и социальной инженерии: filter-шлюзы, sandbox-анализ вложений, url-фильтрацию, блокировку подозрительных ресурсов и принудительную отложенную доставку рискованных писем.
- Организовать регулярное обучение для повышения осведомленности сотрудников с акцентом на распознавание фишинга, социальной инженерии и сценариев компрометации учетных данных, а также проводить внутренние симуляции атак.
- Внедрить централизованный мониторинг и корреляцию событий безопасности, обеспечивающий оперативное выявление и реагирование на типовые векторы атак на уровне сети, конечных точек и периметра, например, с использованием сервиса УЦСБ SOC, который обеспечивает сбор и корреляцию событий с сети, конечных точек и периметра, автоматизирует процессы реагирования с применением SOAR и реализует оперативную автоматизированную блокировку атак.

Выполнение указанных мер позволит минимизировать риски компрометации и обеспечить приемлемый уровень безопасности.

ПРИЛОЖЕНИЕ «ДЕТАЛИЗИРОВАННЫЕ СПИСКИ ТРЕНДОВЫХ УЯЗВИМОСТЕЙ 2025 ГОДА»

Ниже представлены детализированные списки уязвимостей, сгруппированные по категориям: операционные системы, сетевая инфраструктура, прикладное ПО и другие. Материал предназначен для технических специалистов — аналитиков SOC, инженеров по управлению уязвимостями и экспертов по реагированию на инциденты. В таблице ниже вы найдете идентификаторы CVE и информацию о затронутых компонентах, что позволит оперативно оценить актуальность угроз для своей инфраструктуры.

Операционные системы и рабочие станции

Продукт/Компонент	CVE
Windows Hyper-V NT Kernel Integration VSP	CVE-2025-21333 CVE-2025-21334 CVE-2025-21335
Windows Common Log File System Driver	CVE-2025-29824 CVE-2025-32701 CVE-2025-32706
Microsoft DWM Core Library	CVE-2025-30400
Windows Ancillary Function Driver for WinSock	CVE-2025-21418
Windows Storage	CVE-2025-21391
Windows Win32 Kernel Subsystem	CVE-2025-24983
Windows Cloud Files Mini Filter Driver	CVE-2024-30085 CVE-2025-62221
Windows Process Activation	CVE-2025-21204
Windows SMB Client	CVE-2025-33073
Windows Agere Modem Driver	CVE-2025-24990
Windows Update Service	CVE-2025-48799

Windows Remote Access Connection Manager	CVE-2025-59230
Windows Kernel	CVE-2025-62215
Windows Server Update Service	CVE-2025-59287
Internet Shortcut Files	CVE-2025-33053
Windows NTFS	CVE-2025-24993
Windows OLE	CVE-2025-21298
Windows Fast FAT File System Driver	CVE-2025-24985
Windows NTLM	CVE-2025-24054
Microsoft Windows File Explorer	CVE-2025-24071
Microsoft Management Console	CVE-2025-26633
Sudo	CVE-2025-32463
Linux Kernel	CVE-2025-38001

Сетевая инфраструктура и сервисы

Продукт/Компонент	CVE
Fortinet FortiWeb	CVE-2025-64446
Cisco ASA & FTD	CVE-2025-20363 CVE-2025-24472 CVE-2025-20362 CVE-2025-20333
CommuniGate Pro	BDU-2025-01331
TrueConf Server	BDU-2025-10114 BDU-2025-10115 BDU-2025-10116
Roundcube	CVE-2025-49113

XWiki Platform	CVE-2025-24893
Control Web Panel	CVE-2025-48703
Redis	CVE-2025-49844
Erlang/OTP	CVE-2025-32433
FortiOS	CVE-2024-55591
PAN-OS	CVE-2025-0108

Корпоративные платформы и инфраструктура

Продукт/Компонент	CVE
Microsoft SharePoint	CVE-2025-53770 CVE-2025-53771
VMware ESXi	CVE-2025-22224 CVE-2025-22225 CVE-2025-22226
Kubernetes	CVE-2025-1974

Прикладное ПО и библиотеки

Продукт/Компонент	CVE
WinRAR	CVE-2025-6218 CVE-2025-8088
7-Zip	BDU:2025-01793 CVE-2025-0411 CVE-2025-55188
Apache HTTP Server	CVE-2024-38475
Apache Tomcat	CVE-2025-24813
MongoDB	CVE-2025-14847

React Server Components	CVE-2025-55182
expr-eval	CVE-2025-12735
MDaemon Email Server	CVE-2024-11182
Zimbra Collaboration	CVE-2024-27443 CVE-2025-27915
Kaspersky Endpoint Security	BDU:2025-09471