УЦСБ SOC

УЦСБ

ЛАНДШАФТ КИБЕРУГРОЗ ЗА ПЕРВОЕ ПОЛУГОДИЕ 2026: ТРЕНДЫ, ИНЦИДЕНТЫ, УЯЗВИМОСТИ

сентябрь 2026 г.

soc.ussc.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В отчете представлен комплексный анализ инцидентов ИБ первого полугодия 2026 года, проведенный на базе экспертизы Threat Intelligence УЦСБ SOC и публичных источников. Рассмотрены наиболее критичные уязвимости, активно эксплуатировавшиеся в реальных атаках. А также приведены сведения о характере эксплуатации, уязвимых версиях ПО и рисках для ИТ-инфраструктур.

Перечислены наиболее значимые сообщения о взломах компаний различных секторов российской экономики, как публично раскрытые и опубликованные, так и выявленные в ходе мониторинга теневых каналов. Проведен ретроспективный анализ инцидентов ИБ с целью подтверждения или опровержения прогнозов на 2026 год, сделанных командой Threat Intelligence УЦСБ SOC в прошлом отчете «Ключевые тренды киберугроз 2025». Данные ведущих вендоров и исследовательских центров, зафиксированные кибератаки подтверждают заявленные тренды.

Цель отчета — не только проинформировать о выявленных инцидентах ИБ, но и предоставить данные, которые могут использоваться при выработке стратегических решений по защите ИТ-инфраструктуры в условиях высоких рисков компрометации и совершения атак.

ТОП-10 НАИБОЛЕЕ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ЗА ПЕРВОЕ ПОЛУГОДИЕ 2026 ГОДА

В первом полугодии 2026 года специалисты команды Threat Intelligence УЦСБ SOC зафиксировали значительный рост числа критических уязвимостей, эксплуатируемых в реальных атаках. Особую обеспокоенность вызывают 0-day-уязвимости в периметровом оборудовании (Palo Alto, Check Point, NGINX), уязвимости повышения привилегий в ядре Linux (Dirty Frag, Copy Fail, CVE-2026-23111), а также уязвимости в офисных приложениях (CVE-2026-21509, CVE-2026-34621). Раздел содержит анализ десяти наиболее опасных уязвимостей, выявленных в период с января по июнь 2026 года.

1. CVE-2026-0300 RCE в Palo Alto PAN-OS — переполнение буфера в User-ID Authentication Portal

Эксплуатация уязвимости вызывает переполнение буфера в сервисе User-ID Authentication Portal и позволяет неаутентифицированному атакующему выполнить произвольный код с правами суперпользователя на межсетевых экранах серии PA и VM путем отправки специально сформированных сетевых пакетов. Уязвимость присутствует только на устройствах, где Authentication Portal доступен из недоверенных сетей или интернета.

Эксплуатация зафиксирована как 0-day с 9 апреля 2026 г. — за четыре недели до публичного раскрытия. Группировка CL-STA-1132, квалифицированная как вероятный государственно-спонсируемый кластер, 16 апреля достигла успешного RCE и внедрила шеллкод в рабочий процесс nginx. Злоумышленники с правами суперпользователя использовали туннелирующие инструменты EarthWorm и ReverseSocks5, выполнили перечисление Active Directory с использованием учетных данных, извлеченных с самого межсетевого экрана, а затем системно удалили логи crash-дампов nginx и артефакты ядра. 29 апреля злоумышленники провели SAML-flood-атаку, которая спровоцировала HA-переключение на второе устройство, уже находившееся под их контролем. Ставка на общедоступный open-source-инструментарий намеренно снижала вероятность срабатывания сигнатурных средств детектирования.

В начале июня 2026 года в интернете было доступно более 135 тысяч межсетевых экранов с уязвимой версией PAN-OS.

2. CVE-2026-20963 RCE в Microsoft SharePoint — десериализация недоверенных данных

Уязвимость связана с ошибкой в механизме десериализации. Неавторизованный злоумышленник может написать произвольный код, внедрить его и удаленно выполнить на сервере SharePoint. В результате атакующий может получить конфиденциальные данные

и использовать доступ к скомпрометированному серверу для дальнейшего развития атаки. Затронуты SharePoint Server Subscription Edition 2019 и Enterprise Server 2016.

Агентство по кибербезопасности и защите инфраструктуры США (CISA) подтвердило факт активной эксплуатации данной уязвимости и внесло ее в свой каталог известных эксплуатируемых уязвимостей (KEV). SharePoint — ключевая платформа корпоративного документооборота в российском госсекторе и крупном бизнесе: ее компрометация открывает прямой доступ к корпоративным документам, учетным записям сотрудников и формирует плацдарм для развертывания шифровальщиков или шпионского ПО. После получения RCE атакующие устанавливают веб-шеллы и используют сервер для латерального перемещения по внутренней сети.

В 2025 году серверы SharePoint целенаправленно атаковались через 0-day-цепочку ToolShell (CVE-2025-53770/53771), в кампаниях принимали участие китайские кластеры Storm-2603, Linen Typhoon и Violet Typhoon.

3. CVE-2026-50751 Auth Bypass в Check Point VPN Remote Access / Mobile Access (IKEv1) — 0-day

Логическая ошибка в механизме проверки сертификатов при обмене ключами IKEv1 позволяет неаутентифицированному удаленному атакующему установить VPN-сессию без действительного пароля. Клиент манипулирует флагами аутентификации через кастомный VPNExtFeatures Vendor ID payload — шлюз пропускает проверку подписи сертификата и цепочки доверия. Затронуты Security Gateways, Mobile Access SSL VPN и Spark Firewall на устаревшем IKEv1. Уязвимость эксплуатировалась как 0-day с 7 мая 2026 г. Но только когда в начале июня интенсивность атак резко возросла, 8 июня 2026 г. был выпущен патч.

Как минимум один инцидент связан с аффилированным участником группировки Qilin, который использует ее вымогательское ПО для проведения собственных атак. Группировка работает по модели Ransomware-as-a-Service и также известна под названием Agenda. По всему миру зафиксировано более 1400 ее жертв, среди которых Nissan, Synnovis, Lee Enterprises. В ходе постэксплуатации применялся Rclone для кражи данных и, предположительно, протокол Tox для C2-коммуникации. Атакующая инфраструктура: VPS-серверы Kaupo Cloud HK, Shock Hosting, Vultr Holdings. Тот же актор параллельно эксплуатировал уязвимости VPN-решений других вендоров.

Для российских организаций угроза особенно высока: после 2022 года межсетевые экраны Check Point стали единственной западной продукцией этого сегмента, доступной к свободной покупке в РФ без технической поддержки вендора. По различным оценкам, их доля на российском рынке достигает 40–60%. Успешная эксплуатация открывает атакующему прямой туннель в корпоративную сеть без каких-либо ограничений периметра.

4. CVE-2026-43284 + CVE-2026-43500 Dirty Frag — цепочка LPE в ядре Linux (все основные дистрибутивы)

Две уязвимости в подсистеме обработки кеша страниц ядра Linux, работающие в связке. Атакующий выбирает доступный вектор и гарантированно получает права суперпользователя независимо от конфигурации дистрибутива, цепочка закрывает слепые зоны каждого отдельного компонента. Затронуты Ubuntu, RHEL, Fedora, AlmaLinux, openSUSE, Astra Linux, РЕД ОС. Компенсирующая мера от предшественника Copy Fail (блокировка algif_aead) не защищает от Dirty Frag. Рабочий эксплойт опубликован публично 7 мая 2026 г.

Применяется как второй этап атаки после первоначального RCE-проникновения через периметровые уязвимости. Последовательность действий: эксплуатация сетевой уязвимости → Dirty Frag → полный контроль над хостом с правами root.

5. CVE-2026-34197 RCE в Apache ActiveMQ Classic — выполнение кода через Jolokia API

Выявлена уязвимость в брокере сообщений Apache ActiveMQ Classic. Аутентифицированный злоумышленник через веб-консоль Jolokia JMX-HTTP API вызывает операцию BrokerService.addNetworkConnector с URI, содержащим brokerConfig-параметр. Это инициирует загрузку удаленного Spring XML-контекста, что приводит к выполнению произвольного кода на уровне JVM-брокера.

В версиях 6.0.0–6.1.1 эксплуатация возможна без аутентификации. Более 7000 серверов оставались уязвимы, по данным Shadowserver. Реальные атаки зафиксированы с 13 апреля 2026 г.

6. CVE-2026-34621 RCE в Adobe Acrobat Reader — вредоносный PDF-документ

Ошибка некорректной обработки JavaScript-объектов в Adobe Acrobat Reader для Windows и macOS позволяет выполнить произвольный код при открытии специально созданного PDF-файла. Требует взаимодействия пользователя с документом. Эксплуатация подтверждена с ноября 2025 г., однако патч вышел только в июне 2026 г.

Обнаруженные вредоносные документы-приманки на русском языке с нефтегазовой тематикой являются прямым свидетельством целевых фишинговых кампаний против российских организаций ТЭК. Документы маскируются под отраслевые материалы, связанные с текущими событиями в российской нефтегазовой отрасли, что существенно повышает доверие получателей и вероятность открытия.

7. CVE-2026-21509 RCE в Microsoft 365 / Office 2016–2024 — обход OLE через вредоносный документ

Логическая ошибка при проверке входных данных в механизме OLE позволяет атакующему выполнить произвольный код с правами текущего пользователя при открытии специально созданного документа. Затронуты Office 2016 и 2019, LTSC 2021/2024 и Microsoft

365 Apps for Enterprise. Активная эксплуатация подтверждена вендором. Публичного PoC нет, уязвимость применяется в закрытых инструментариях.

В феврале 2026 года зафиксирована первая фишинговая атака на российские организации с использованием этой уязвимости. Группировка BO Team (также известная как Black Owl, Lifting Zmiy) распространяла RTF-документы, оформленные под служебную переписку федерального ведомства «Акт проверки транспортного средства» с формой пояснений по делу об административном правонарушении. Встроенный OLE-объект с CLSID Shell.Explorer.1 при открытии в уязвимом Office запускал загрузку LNK-файла через WebDAV и инициировал дальнейшую цепочку компрометации. Кроме BO Team, уязвимость применяла группировка PhantomCore, которая использует перехват COM-объектов для загрузки вредоносных DLL в контексте легитимных процессов. Атаки направлены преимущественно против российских государственных, промышленных и финансовых организаций.

8. CVE-2026-31431 Copy Fail — LPE в ядре Linux algif_aead (присутствует с 2017 года)

Логическая ошибка в криптографическом модуле algif_aead ядра Linux (присутствует с 2017 года): через сокет AF_ALG, доступный любому пользователю, атакующий перезаписывает 4 байта в кеше страниц читаемых файлов. Исследователи продемонстрировали повышение привилегий до root через отключение проверки пароля в /usr/bin/su, модификацию запущенных процессов, а в Kubernetes через выполнение кода в соседних подах или побег из контейнера. Уязвимость присутствовала в ядре около 9 лет до обнаружения. Затронуты Ubuntu, RHEL, WSL2 и все дистрибутивы с загруженным модулем algif_aead.

Применяется как инструмент постэксплуатации после первоначального RCE-проникновения. Факт эксплуатации до публичного раскрытия свидетельствует о присутствии в арсеналах акторов с закрытым инструментарием. Данная уязвимость — предшественник цепочки Dirty Frag (№4). При этом она особенно актуальна для российских организаций в условиях активного импортозамещения на отечественные Linux-дистрибутивы.

9. CVE-2026-23111 LPE в ядре Linux nf_tables

В подсистеме nf_tables ядра Linux выявлена уязвимость типа use-after-free. Причина — инвертированная проверка (лишний «!» в функции nft_map_catchall_activate). Это приводит к тому, что при отмене транзакции счетчик ссылок цепочки уменьшается без последующего восстановления, обнуляется, цепочка освобождается, а указатель на нее остается висеть. Непривилегированный локальный пользователь получает права root и может выйти из контейнера на хост-систему. Патч — одна строка кода, выпущен 5 февраля 2026 г. Эксплуатация подтверждена на Debian 12/13 и Ubuntu 22.04/24.04 LTS, включая обход AppArmor через профиль trinity.

Полный рабочий PoC опубликован в апреле 2026 г., а детальный технический разбор 8 июня 2026 г. Публично доступный рабочий эксплойт создает высокий риск применения в APT-атаках.

10. CVE-2026-42945 DoS/RCE в NGIN — переполнение буфера в модуле rewrite (NGINX Rift)

Переполнение буфера памяти в модуле ngx_http_rewrite_module затрагивает все версии NGINX Open Source и NGINX Plus с 0.6.27 по 1.30.0, фактически весь диапазон релизов за 18 лет. Уязвимость существует в кодовой базе с 2008 года и связана с несогласованной логикой экранирования внутри rewrite-движка. Неаутентифицированный атакующий может вызвать аварийное завершение worker-процессов, отправив специально сформированный HTTP-запрос к серверу с уязвимой rewrite-конфигурацией. Удаленное выполнение кода возможно при отключенном ASLR на целевой системе. По оценке исследователей, около 5,7 млн NGINX-серверов, доступных в интернете, работали на потенциально уязвимых версиях.

Активная эксплуатация зафиксирована 16 мая 2026 года, через три дня после публичного раскрытия. Специалисты VulnCheck обнаружили попытки атак в honeypot-сетях с использованием специально сформированных HTTP-запросов. Кластер атакующей активности исходил с китайского IP-адреса и применял кастомизированную реализацию ИИ-инструмента Vulnhuntr для автоматического обнаружения уязвимых установок с последующей установкой PHP веб-шелла. NGINX является одним из наиболее распространенных веб-серверов и реверс-прокси в российской корпоративной и государственной инфраструктуре. Аварийная остановка worker-процессов в результате DoS-атаки выводит из строя веб-сервисы и API-шлюзы организации. В конфигурациях с отключенным ASLR — открывает путь к полной компрометации сервера.

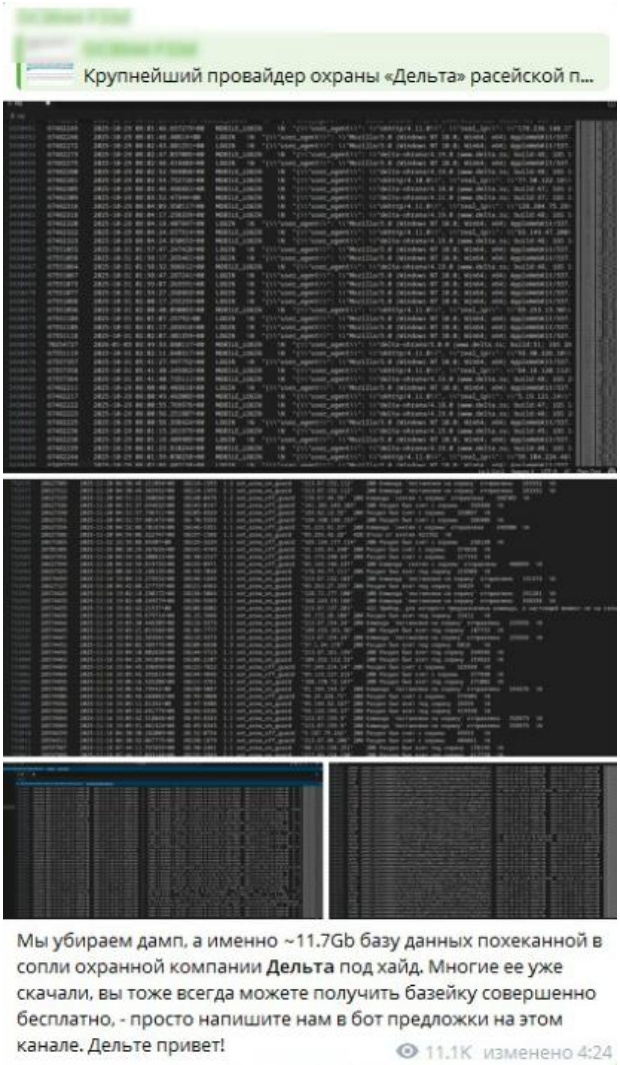
ПОЛУГОДОВОЙ АНАЛИЗ УТЕЧЕК: КТО И КАК ТЕРЯЛ ДАННЫЕ

Ниже представлены наиболее значимые 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. **«Дельта»**

В январе группировка «DC8044 F33d» заявила о компрометации охранной компании «Дельта». Хакеры утверждают, что база объемом 11 ГБ содержит логи входа в личные кабинеты, сообщения и другие данные, относящиеся к 167 000 физических лиц, 89 100 юридическим лицам и 138 000 индивидуальных предпринимателей, которые являются клиентами компании.

По данным РИА Новости, компания «Дельта» прокомментировала сообщение о масштабной внешней атаке на ее ИТ-инфраструктуру, направленной на нарушение работы сервисов.



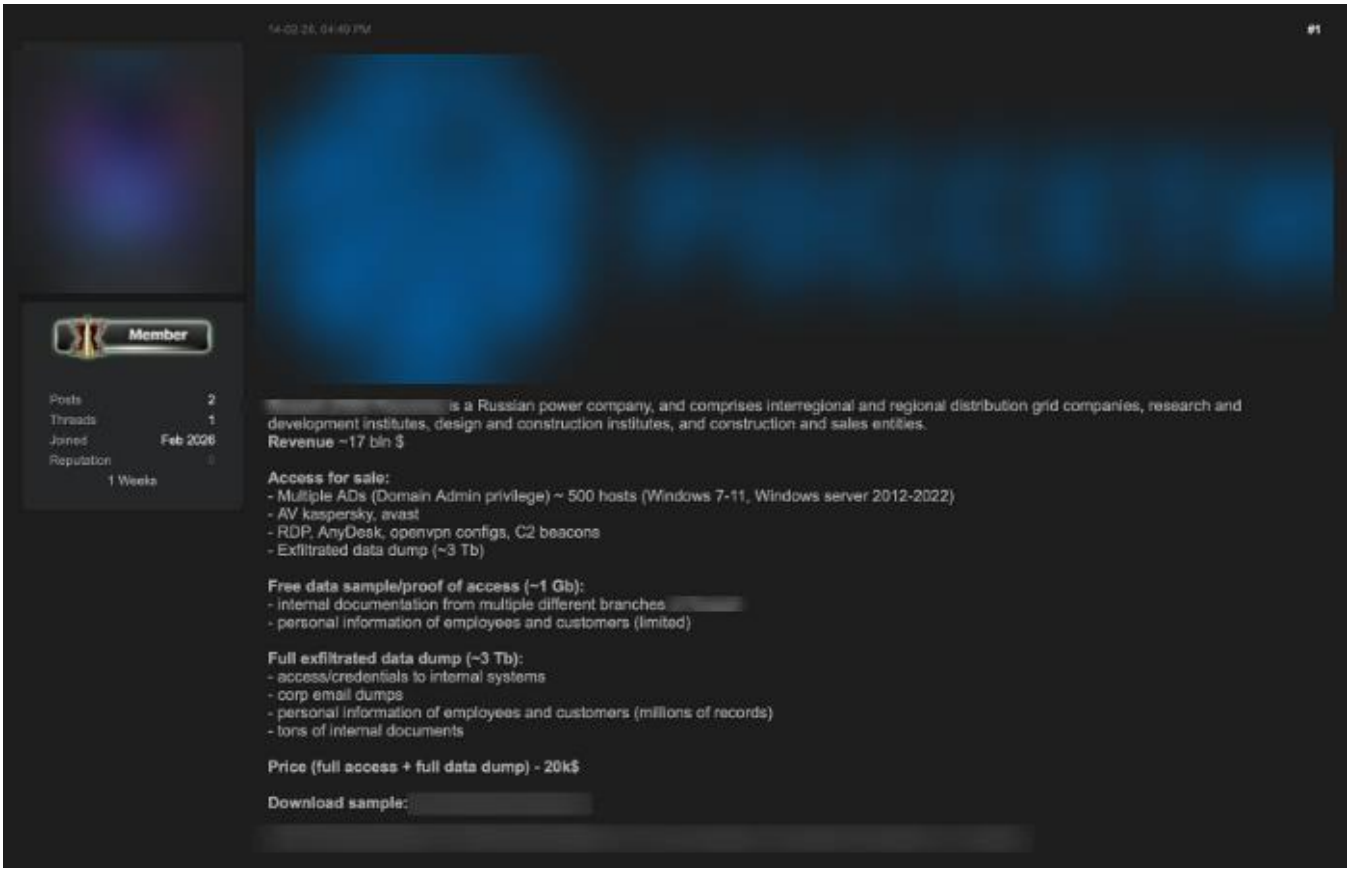
2. Российская энергетическая компания

В феврале злоумышленник выставил на продажу данные Active Directory объемом около 3 ТБ (500 хостов) российской энергетической компании.

В качестве подтверждения злоумышленник опубликовал архив объемом примерно 1 ГБ. Он содержал файлы с рабочих компьютеров сотрудников трех региональных филиалов энергокомпании: в Сибири, Южном и Северо-Кавказском регионах.

В опубликованных материалах злоумышленник отдельно отмечает наличие документов в формате DOCX с просьбами о возврате ранее изъятого майнингового оборудования, а также жалобы, связанной с непоставкой майнинговых устройств интернет-магазину. По их утверждению, указанные документы были найдены на одном из рабочих компьютеров сотрудника Северо-Кавказского филиала.

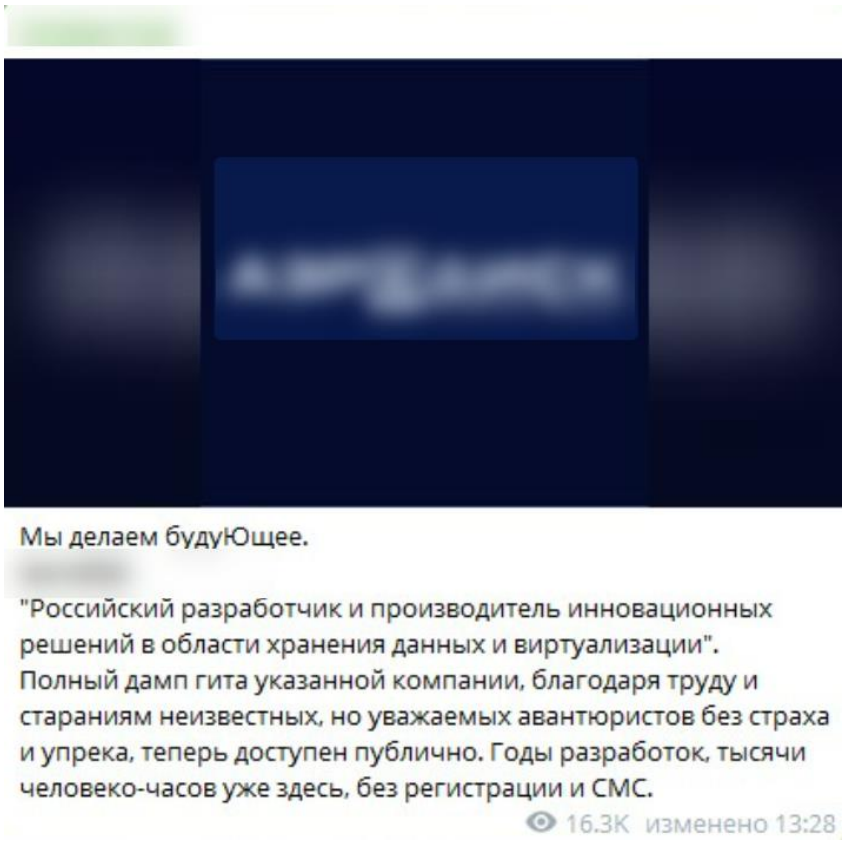
Злоумышленник утверждает, что в полном дампе содержатся данные корпоративной почты, персональные данные сотрудников и более 1 млн клиентов, а также значительный объем внутренних документов.



3. Российский разработчик систем хранения данных и систем виртуализации

В марте хакеры заявили о взломе компании-производителя СХД и решений для виртуализации, чьи продукты используются в критической инфраструктуре, включая Газпром, РЖД, Ростех и Россети. В качестве подтверждения злоумышленники опубликовали полный дамп Git-данных компании объемом около 112 ГБ.

Компрометация исходного кода создает прямую угрозу безопасности цепочек поставок для перечисленных организаций.

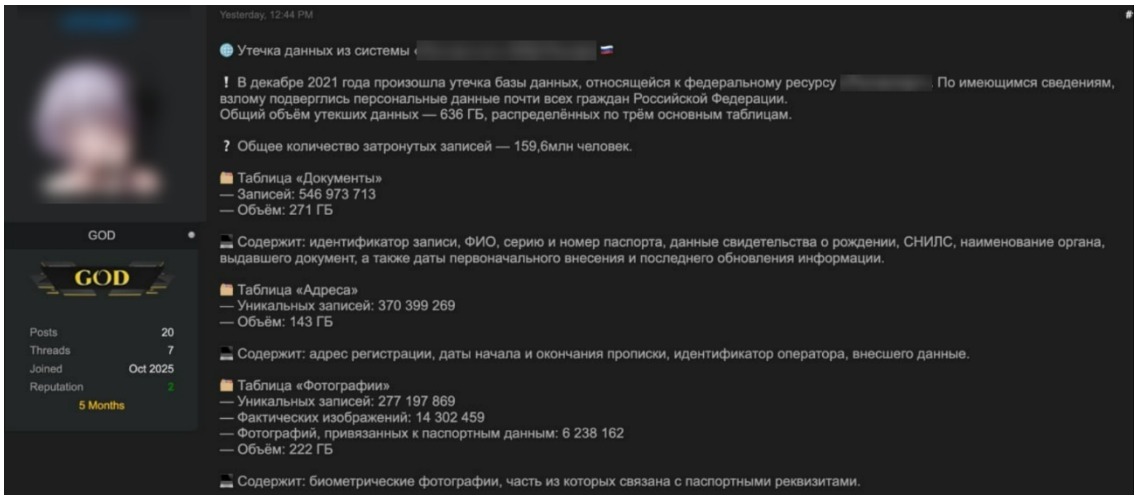


4. Федеральный ресурс

В апреле на одном из закрытых форумов был размещен пост о продаже крупного массива персональных данных, который, по утверждению продавцов, получен из Системы федерального ресурса. Злоумышленники предлагают приобрести архив объемом 636 ГБ за сумму 6000 долларов. В описании набор данных разделен на три логические таблицы:

- «Документы» — 547 млн записей, объем 271 ГБ;
- «Адреса» — 370 млн записей, объем 143 ГБ;
- «Фотографии» — 277 млн записей, 14 млн фотографий, объем 222 ГБ.

По заявлению злоумышленников, в совокупности массив затрагивает данные о 159,6 млн физических лиц.

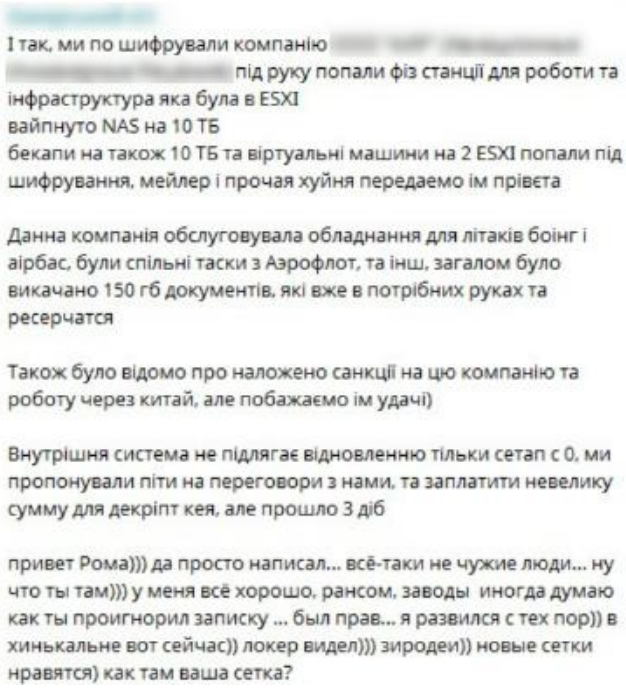


5. Компания, специализирующаяся на ремонте авиационных компонентов

В мае группировка «Хакерський кіт» заявила о взломе компании, которая обслуживала оборудование для самолетов Boeing и Airbus, а также имела совместные задачи с «Аэрофлотом» и другими организациями.

По утверждению злоумышленников, под шифрование попали рабочие станции, виртуальные машины на двух ESXi, почтовая инфраструктура и другие внутренние системы. Также заявлен вайп NAS и резервных копий суммарно примерно на 20 ТБ, а объем якобы выгруженных документов составил около 150 ГБ и передан третьим лицам для изучения.

В качестве доказательства злоумышленники предоставили около 215 учетных записей с паролями. Примерно 157 из них персональные и корпоративные: почта, AD, Outlook и VPN. Еще около 55–60 доступов инфраструктурные и сервисные: Wi-Fi, роутеры, NAS, серверы, Bitrix, хостинги, FTP/SSH, прокси и внешние кабинеты.



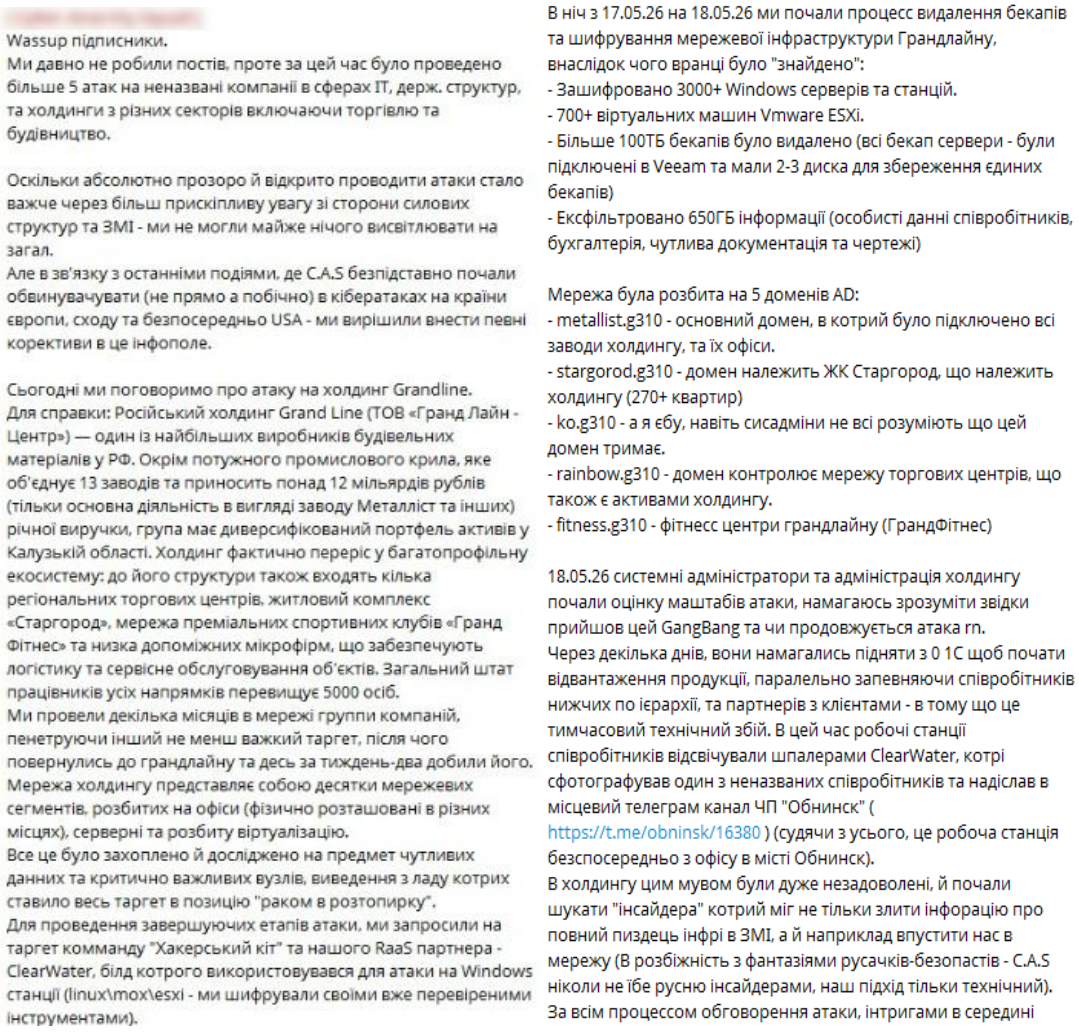
6. Grand Line

В июне группировка Cyber.Anarchy.Squad заявила о получении доступа к ИТ-инфраструктуре холдинга Grand Line — одного из крупнейших производителей строительных материалов в России.

Холдинг включает 13 заводов с общим штатом около 5000 человек. По утверждению хакеров, за несколько месяцев нахождения внутри инфраструктуры им удалось получить более 650 ГБ данных, включая персональные данные сотрудников и их фотографии, бухгалтерские документы, а также конфиденциальную документацию. Эти материалы были выложены в открытый доступ.

Злоумышленники заявили, что 18 мая 2026 г. было зашифровано более 3000 серверов и рабочих станций, 700 виртуальных машин, а также удалено более 100 ТБ резервных копий.

По данным SecPost, в компании подтвердили сбой в ряде сервисов.



Wassup підписники.
Ми давно не робили постів, проте за цей час було проведено більше 5 атак на неназвані компанії в сферах IT, держ. структур, та холдинги з різних секторів включаючи торгівлю та будівництво.

Оскільки абсолютно прозоро й відкрито проводити атаки стало важче через більш прискіпливу увагу зі сторони силових структур та ЗМІ - ми не могли майже нічого висвітлювати на загал.
Але в зв'язку з останніми подіями, де C.A.S безпідставно почали обвинувачувати (не прямо а побічно) в кібератаках на країни європи, сходу та безпосередньо USA - ми вирішили внести певні корективи в це інфополе.

Сьогодні ми поговоримо про атаку на холдинг Grandline.
Для справки: Російський холдинг Grand Line (ТОВ «Гранд Лайн - Центр») — один із найбільших виробників будівельних матеріалів у РФ. Окрім потужного промислового крила, яке об'єднує 13 заводів та приносить понад 12 мільярдів рублів (тільки основна діяльність в вигляді заводу Металліст та інших) річної виручки, група має диверсифікований портфель активів у Калузькій області. Холдинг фактично переріс у багатопрофільну екосистему: до його структури також входять кілька регіональних торгових центрів, житловий комплекс «Старгород», мережа преміальних спортивних клубів «Гранд Фітнес» та низка допоміжних мікрофірм, що забезпечують логістику та сервісне обслуговування об'єктів. Загальний штат працівників усіх напрямків перевищує 5000 осіб.
Ми провели декілька місяців в мережі группи компаній, пенетруючи інший не менш важкий таргет, після чого повернулись до грандлайну та десь за тиждень-два добили його.
Мережа холдингу представляє собою десятки мережевих сегментів, розбитих на офіси (фізично розташовані в різних місцях), серверні та розбиту віртуалізацію.
Все це було захоплено й досліджено на предмет чутливих данних та критично важливих вузлів, виведення з ладу котрих ставило весь таргет в позицію "раком в розтопирку".
Для проведення завершуючих етапів атаки, ми запросили на таргет комманду "Хакерський кіт" та нашого RaaS партнера - ClearWater, білд котрого використовувався для атаки на Windows станції (linux\mox\esxi - ми шифрували своїми вже перевіреними інструментами).

В ніч з 17.05.26 на 18.05.26 ми почали процесс видалення бекапів та шифрування мережевої інфраструктури Грандлайну, внаслідок чого вранці було "знайдено":
- Зашифровано 3000+ Windows серверів та станцій.
- 700+ віртуальних машин Vmware ESXi.
- Більше 100ТБ бекапів було видалено (всі бекап сервери - були підключені в Veeam та мали 2-3 диска для збереження єдиних бекапів)
- Ексфільтровано 650ГБ інформації (особисті данні співробітників, бухгалтерія, чутлива документація та чертежі)

Мережа була розбита на 5 доменів AD:
- metallist.g310 - основний домен, в котрий було підключено всі заводи холдингу, та їх офіси.
- stargorod.g310 - домен належить ЖК Старгород, що належить холдингу (270+ квартир)
- ko.g310 - а я єбу, навіть сисадміни не всі розуміють що цей домен тримає.
- rainbow.g310 - домен контролює мережу торгових центрів, що також є активами холдингу.
- fitness.g310 - фітнесс центри грандлайну (ГрандФітнес)

18.05.26 системні адміністратори та адміністрація холдингу почали оцінку маштабів атаки, намагаюсь зрозуміти звідки прийшов цей GangBang та чи продовжується атака rn.
Через декілька днів, вони намагались підняти з 0 1С щоб почати відвантаження продукції, паралельно запевняючи співробітників нижчих по ієрархії, та партнерів з клієнтами - в тому що це тимчасовий технічний збій. В цей час робочі станції співробітників відсвічували шпалерами ClearWater, котрі сфотографував один з неназваних співробітників та надіслав в місцевий телеграм канал ЧП "Обнинск" (https://t.me/obninsk/16380) (судячи з усього, це робоча станція безпосередньо з офісу в місті Обнинск).
В холдингу цим мувом були дуже незадоволені, й почали шукати "інсайдера" котрий міг не тільки злити інфорацію про повний пиздець інфрі в ЗМІ, а й наприклад впустити нас в мережу (В розбіжність з фантазіями русачків-безопастів - C.A.S ніколи не їбе русню інсайдерами, наш підхід тільки технічний).
За всім процессом обговорення атаки, інтригами в середині

ОТ ПРОГНОЗОВ К ФАКТАМ: ЧТО ПОДТВЕРДИЛОСЬ В ПЕРВОМ ПОЛУГОДИИ 2026 ГОДА

Основным прогнозом в годовом отчете «Ландшафт киберугроз 2025: тренды, атаки, уязвимости» Threat Intelligence УЦСБ SOC указывали трансформацию атак. Согласно оценке, атаки должны были перестать быть точечными и приобрести комплексный характер, затрагивающий операционные, репутационные и регуляторные аспекты бизнеса. Первое полугодие 2026 года полностью подтвердило этот прогноз.

Все заявленные тренды, а именно: переход к комплексным атакам, комбинирование шифрования с кражей данных и DDoS, использование ИИ, компрометация цепочек поставок стали доминирующими в ландшафте угроз для российских компаний. Анализ отчетов ведущих вендоров и исследовательских центров за январь — июнь 2026 года показывает, что прогнозные сценарии реализовались в полном объеме, а по ряду направлений даже превзошли ожидания.

Ниже представлены семь ключевых трендов, которые специалисты Threat Intelligence УЦСБ SOC прогнозировали на 2026 год и которые нашли фактическое подтверждение в первом полугодии.

1 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.

Согласно апрельскому отчету Positive Technologies CODE RED 2026, этот тренд уже получает эмпирическое подтверждение: эксперты фиксируют переход к многофункциональным троянам, объединяющим инфостилер, вайпер и шифровальщик. Именно такие инструменты делают атаки комплексными. Они не только блокируют доступ к данным, но и обеспечивают систематическую кражу информации для последующего шантажа, что ведет к остановке бизнес-процессов и репутационным рискам.

Особую тревогу вызывает распространение этой модели на промышленный сектор: Kaspersky ICS CERT за первый квартал 2026 года зафиксировал рост доли компьютеров АСУ, атакованных шифровальщиками, **в 2,3 раза** чаще по сравнению с предыдущим периодом. Промышленные объекты все чаще становятся жертвами двойного вымогательства: киберпреступники одновременно требуют выкуп за восстановление доступа к данным и угрожают утечкой украденной коммерческой или технологической информации, если их требования не будут выполнены.

2 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.

В первом квартале 2026 года Kaspersky ICS CERT зафиксировал блокировку вредоносных объектов **на 16% компьютеров АСУ в России**. Этот показатель оказался выше, чем в третьем и четвертом кварталах 2025 года. Основным источником угроз является цифровая трансформация промышленности, сопровождающаяся расширением подключений АСУ к глобальной сети. Это создает дополнительные каналы для доставки вредоносного ПО, что подтверждается статистикой отчета: на биометрических системах, традиционно имеющих доступ в интернет, зафиксирована максимальная доля заражений на 26,4%. Вместе с тем негативное влияние оказывают использование устаревших OT-систем, не адаптированных к современным угрозам, а также увеличение поверхности атаки за счет интеграции с партнерскими сетями и цепочками поставок. Совокупность перечисленных факторов способствует дальнейшему росту уязвимости АСУ перед внешними угрозами.

3 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, например в форме Ransom-DDoS.

По данным Kaspersky DDoS Protection, за период с января по май 2026 года число DDoS-атак в России и странах СНГ увеличилось **на 27%** по сравнению с аналогичным периодом 2025 года. В январе число массовых автоматизированных атак выросло на 54%. Злоумышленники применяют многовекторные схемы, ИИ-инструменты для генерации трафика и арендованную облачную инфраструктуру. Специалисты StormWall в отчете по итогам майских праздников 2026 года отмечают, что в начале года чаще всего применялись многовекторные атаки, импульсные атаки и так называемые ковровые бомбардировки. В I квартале 2026 года в России впервые были выявлены DDoS-атаки мощностью свыше 3 Тбит/с. Большинство таких атак было направлено на телеком-сферу и финансовую отрасль. Мощнейшие атаки вызвали неполадки в работе ИТ-инфраструктуры компаний, что привело к простоям бизнеса и значительному финансовому ущербу.

Аналитика Ideco за апрель показывает, что доля многовекторных DDoS-атак достигла **52% от общего числа инцидентов** — это более чем двукратный рост по сравнению с 2024 годом (25%). При этом 8 из 10 атак приходились на уровень L7 (уровень приложений), что подтверждает прикладной характер угрозы и требует защиты на уровне WAF, а не только на уровне межсетевых экранов.

4 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.

По данным RED Security, **треть всех расследованных случаев** компрометации инфраструктуры российских компаний связана с атаками через подрядчиков. Годом ранее

доля таких атак не превышала 10%. 94% внутренних тестов на проникновение завершились полным захватом корпоративной сети.

Исследование «Кросс технолоджис» показывает, что атаки на цепочки поставок выросли **на 90% в 2025 году.** Их доля от общего числа инцидентов составляет 25–30%. При этом рост сохранится и в 2026 г., его темпы могут составить 35–40%. Чаще всего атаки на цепочки поставок реализуются через логистический бизнес — более 50% инцидентов.

А целью таких атак чаще всего становятся: 40% случаев промышленность, 30% ретейл, медицина и образование — по 10%.

Яркая иллюстрация этого тренда — атака на DAEMON Tools, о которой «Лаборатория Касперского» сообщила на ПМЭФ-2026. С начала апреля через официальный сайт разработчика распространялась версия программы с бэкдором внутри. В результате зафиксировано **свыше 2000 заражений** более чем в 100 странах, при этом 20% пострадавших устройств находились в России. Атаки на цепочки поставок ПО выделены как один из ключевых трендов первого полугодия 2026 года.

На этом фоне регулятор постепенно ужесточает требования. С 1 марта 2026 года требования по информационной безопасности стали обязательным условием договоров с подрядчиками значимых объектов КИИ. Государство сформировало системный контур защиты цепочек поставок: обязательное отслеживание и реагирование через ГосСОПКА, расширенные требования к подрядчикам, сертификация отечественных СЗИ.

5 Параллельно серьезной угрозой останется фишинг, который за счет массового применения LLM-инструментов становится одновременно более дешевым и более прицельным. Генерация корректных, стилистически выверенных писем снижает порог распознавания таких атак пользователями.

Согласно данным ЦАСИ, в первом квартале 2026 года зафиксирован рост кибермошенничества через мессенджеры. Все цифровые угрозы для брендов демонстрируют **высокую степень автоматизации и использования генеративных моделей** для наполнения мошеннических страниц фейковым контентом. Ключевым активом атакующего становится не технология взлома, а умение управлять доверием пользователя.

По данным BI.ZONE Mail Security, только за последнюю неделю мая 2026 года злоумышленники разослали более 1000 фишинговых писем сотрудникам российских компаний, спекулируя на теме пассивного дохода и инвестиций. Факт подтверждает массовый и стабильный характер фишинговых кампаний. А популярность применения данного инструмента, в свою очередь, свидетельствует о его эффективности.

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

Эксперты Anti-Malware в февральском анализе констатируют: «2026 год окончательно стирает грань между технической ошибкой и преступной халатностью в сфере ИБ». Руководители несут персональную ответственность сразу по нескольким направлениям: дисциплинарную, административную, субсидиарную (взыскание долгов с личного имущества) и уголовную — по статьям о халатности или **статье 274.1 УК РФ.** Основанием для привлечения становятся подписанные акты о вводе незащищенных систем, неисполнение предписаний регулятора.

В 2026 году уже есть прецеденты. В марте суд оштрафовал онлайн-школу Ukids за утечку 300–500 тыс. записей клиентов по новым, ужесточенным нормам. Формально компании грозил штраф от 10 млн рублей, но, как микропредприятию, ей назначили 400 тыс. рублей. При этом в замене на предупреждение отказали из-за нарушения сроков уведомления Роскомнадзора.

Еще один показательный пример — дело Минтруда, дошедшее до Верховного Суда РФ. Ведомство пыталось оспорить штраф в 100 тыс. рублей за утечку 1400 записей сотрудников (с паспортами и реквизитами карт), ссылаясь на вину подрядчика. Верховный Суд РФ подтвердил, что именно Минтруд является оператором персональных данных и несет полную ответственность за их защиту, включая контроль за действиями подрядчиков.

Также эксперты фиксируют неожиданный эффект ужесточения законодательства: новые штрафы создали для злоумышленников четкий «прайс-лист». Часть хакерских групп переходит от публичных сливов к модели **«тихого урегулирования»**: предлагает компании выкуп за неразглашение инцидента регулятору. Особенно уязвимы компании среднего размера, для которых один оборотный штраф может означать банкротство.

7 Привычные схемы проникновения останутся основным инструментом злоумышленников. Невысокая сложность подготовки, минимальные затраты и стабильная результативность обеспечивают базовым векторам лидирующие позиции. Совокупно они формируют 70–80% от общего объема расследуемых инцидентов.

По данным «Информзащиты», за I квартал 2026 года распределение по типам инцидентов выглядит так: фишинг — **68%**, шифровальщики — **21%**, атаки через подрядчиков — **26%**. В рамках одной атаки нередко комбинируются разные векторы, поэтому суммарные доли превышают **100%.**

Исследование «Бастиона» выявило критический разрыв в осведомленности персонала: только **1% сотрудников** сообщает о потенциально фишинговых письмах в службу безопасности, тогда как **16% переходят по вредоносным ссылкам**. Это также подтверждает тезис о стабильной результативности базовых векторов.

«Информзащита» в апрельском отчете указывает, что **53%** всех ransomware-инцидентов в начале 2026 года начинаются с компрометации учетных данных через инфостилеры: злоумышленники просто покупают готовый доступ вместо того, чтобы искать уязвимости. Однако в 31% случаев злоумышленники по-прежнему используют уязвимости веб-

приложений. Именно они зачастую служат первоначальной точкой внедрения для тех же инфостилеров или фишинговых атак.

ИТОГОВЫЕ ВЫВОДЫ

1. Прогнозы подтвердились и останутся актуальными во втором полугодии 2026 г.

Сформулированные в прошлом отчете прогнозы, нашли фактическое подтверждение в независимых источниках по итогам первого полугодия. Это доказывает корректность выбранной методологии оценки угроз и своевременность сделанных ранее предупреждений. Важно, что эти тенденции не являются краткосрочными: специалисты команды Threat Intelligence УЦСБ SOC прогнозируют сохранение их актуальности и влияния на ландшафт угроз до конца 2026 года.

2. Рост атак по цепочкам поставок продолжается

Наиболее чувствительным к прогнозированию оказался вектор атак через цепочки поставок: доля таких инцидентов за год выросла с 10 до 30–33%, что практически совпало с прогнозным диапазоном. Рост на 90% за 2025 год и сохранение восходящего тренда в 2026-м подтверждают системный характер угрозы, требующей пересмотра договорных и технических отношений с подрядчиками.

3. LLM-угрозы перешли из теории в практику

Использование генеративных моделей злоумышленниками перестало быть гипотетическим сценарием: автоматизация фишинга с применением LLM-инструментов зафиксирована в реальных кампаниях. Снижение порога распознавания таких атак и рост их массовости подтверждают, что человеческий фактор становится главной уязвимостью даже при формально выстроенной защите.

4. Рост кибератак на АСУ ТП в России

Промышленный сектор и автоматизированные системы управления технологическими процессами вышли на первое место по числу атак в России, что полностью подтверждает прогноз расширения угрозы за пределы традиционной ИТ-инфраструктуры. Число зараженных компьютеров АСУ выросло в 2,3 раза. При этом в первом квартале 2026 года доля зараженных систем достигла 16%. Поэтому защита АСУ ТП должна быть важным приоритетом, обеспечения непрерывности и устойчивости работы предприятия.

5. Устойчивость базовых векторов сохраняется

Несмотря на появление сложных многофакторных атак, фишинг, кража учетных данных и эксплуатация веб-уязвимостей сохраняют долю 70–80% в структуре инцидентов. Инвестиции в базовую гигиену информационной безопасности остаются наиболее эффективными с точки зрения снижения рисков. Пренебрежение элементарными правилами информационной безопасности продолжает иметь место в реальных инфраструктурах, несмотря на широкую осведомленность в сфере. При этом даже при соблюдении базовой

гигиены компании зачастую не способны вовремя обнаружить атакующего: известны случаи, когда злоумышленник оставался незамеченным в инфраструктуре месяцами, что указывает на незрелость мониторинга ИБ. В следующем разделе отчета приведены практические примеры, предоставленные специалистами направления пентестов Центра кибербезопасности УЦСБ.

ПРАКТИЧЕСКИЙ ВЗГЛЯД КОМАНДЫ ПЕНТЕСТЕРОВ: АНАЛИЗ ПРОЕКТОВ, ТРЕНДЫ И ПРОГНОЗ РАЗВИТИЯ УГРОЗ

В дополнение к аналитической части приводим наблюдения пентестеров Центра кибербезопасности УЦСБ. Выводы основаны на результатах проектов по оценке защищенности, выполненных в первом полугодии 2026 года.

Распространенной остается комбинация двух основных проблем, хорошо известных по прошлому году. Первая из них связана с недостаточным соблюдением парольной политики внутри компании: использование слабых паролей на критических серверах, хранение их в незашифрованном виде на внутренних ресурсах (как на личных АРМ, так и на сетевых папках или внутри конфигурационных файлов), эксплуатация системных средств для хранения УЗ (DPAPI, браузеры и т.п.). Эти и другие уязвимости используются атакующим для сбора УЗ, необходимых для продвижения по сети.

Вторая проблема связана с недостатками конфигурации компонентов доменных сред, таких как ADCS или SCCM. После получения необходимых доступов и вводных именно эти методы чаще всего используются атакующим для компрометации внутренней инфраструктуры. Например, службы сертификации Active Directory остаются одной из самых опасных точек инфраструктуры. Ошибки конфигурации, такие как избыточные права на шаблоны сертификатов, устраняются, но со временем появляются снова. Проблема дополнительно усугубляется появлением новых техник атак, таких как ESC16 и CVE-2026-54121.

Стоит отметить, что многие компании до сих пор используют западное ПО, обновление которого в текущих реалиях либо невозможно легально, либо требует обходных путей по его установке, и это зачастую усложняет его эксплуатацию. Переход же на отечественные аналоги иногда связан с дополнительными рисками и трудозатратами, на которые компании не всегда готовы. В связи с этим на проектах мы часто находим какие-либо серверы, предоставляющие доступ к жизненно важному, но устаревшему ПО, для которого уже давно выявлены известные уязвимости. Оно остается в инфраструктуре по принципу «работает — не трогай».

2026 год начался и проходит под эгидой повсеместного внедрения систем на базе ИИ. В ИБ этот тренд также становится одним из ключевых, наибольшие риски к 2027 году будут связаны с дальнейшим развитием ИИ. Уже сейчас существует множество открытого ПО, которое в разы ускоряет процесс компрометации систем и приложений. Оно одинаково эффективно как для опытных атакующих, автоматизирующих рутинные проверки с помощью MCP-агентов, так и для некомпетентных злоумышленников, использующих готовые комплексы, которые выполняют все шаги атаки автоматически. Применение ИИ-инструментов сильно снижает порог входа для менее квалифицированных участников

и повышает эффективность и мощность кибератак. Наряду с явлением вайбкодинга активно зарождается и развивается аналогичное направление в ИБ — вайбпентестинг. Это может принести дополнительные трудности для команды защиты, связанные со значительным увеличением количества атак.