ЛАНДШАФТ КИБЕРУГРОЗ

за 2025 год

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

ЦЕЛЬ ОТЧЁТА

Целью документа является предоставление комплексного анализа текущих тенденций и угроз в области кибербезопасности. Отчет призван информировать организации о типах кибератак, наиболее используемых тактиках, техниках и процедурах злоумышленников (ТТП), а также об эксплуатируемых уязвимостях. Основной задачей является повышение осведомлённости и подготовленности безопасности инфраструктуры, с целью выработки компаниями эффективных стратегий защиты своих информационных систем.

АКТУАЛЬНОСТЬ ТЕМЫ

Цифровая трансформация охватывает всё больше сфер жизни, что ведёт к значительному увеличению киберугроз. С ростом числа сложных и целенаправленных атак бизнес и государственные структуры сталкиваются с новыми вызовами в обеспечении безопасности данных и непрерывности операций. Актуальность отчёта заключается в необходимости своевременно выявлять и анализировать новые методы атак, наиболее часто используемые злоумышленниками уязвимости и тенденции в киберугрозах, чтобы минимизировать риски и защитить критически важные информационные системы.

Методологией является анализ текущего ландшафта угроз, проведённый на основе внутренних данных АО «ПМ», отчётов внешних вендоров (F6, Kaspersky, Positive Technologies, BI`ZONE), а также официальных источников.

Целевой аудиторией отчёта являются руководители, специалисты по ИБ, ИТ-отделы, регуляторы.

Над отчётом работали сотрудники отдела исследований киберугроз АО «ПМ».

ТРЕНДЫ УХОДЯЩЕГО ГОДА

КЛЮЧЕВЫЕ ДРАЙВЕРЫ КИБЕРРИСКА 2025–2026

Четыре устойчивых драйвера формируют профиль риска в России в 2025-м году и определяют приоритеты на 2026-й.

1 Геополитический фактор и «гибридные» кампании.

Одновременно целевые атаки, криминальные группы и хактивисты. Всё чаще используются «комбинированные» сценарии: сначала запускают DDoS или бот-атаки, чтобы создать шум и отвлечь внимание, затем точечно взламывают уязвимые системы и вручную закрепляются в сети, после чего похищают данные и начинают вымогательство.

Индикаторы:

- Необычные всплески L7-трафика с низкой конверсией.
- Координированные инфоповоды вокруг бренда/отрасли.
- Всплеск фишинга/спуфинга доменов.

2 Цифровизация критичных услуг и зависимость от внешних поставщиков.

Рост (+23%) доли внешних SaaS/аутсорсеров (MDM/EDR-платформ, платёжных/телеком-шлюзов; расширение поверхности атаки и связности инцидентов).

Индикаторы:

- Компании всё чаще используют сторонние сервисы и неофициальные инструменты, которые подразделения ИТ не всегда контролируют. Появляется больше связей между системами.
- Недоступность внешних компонентов — каскадные отказы.

3 Импортонезависимость и технологические миграции.

Переезд на отечественные ОС/БД/СКЗИ/СЗИ, замена зарубежных библиотек и драйверов.

Индикаторы:

- «Смещение» сроков миграций, временные костыли интеграций.
- Дефицит квалификации, рост операционных ошибок.

4 Генеративный ИИ в руках атакующих и защитников.

Масштабирование фишинга (мультиязычность, голос/видео), ускоренная разработка скриптов пост-эксплуатации; с защитной стороны — авто-корреляция и детект.

Индикаторы:

- «Идеальные» письма без орфографических огрехов, локализованные под процессы.
- Рост дипфейк-сценариев BEC (голос/видео «руководителя»).

ГЕОПОЛИТИЧЕСКИЙ ФАКТОР И «ГИБРИДНЫЕ» КАМПАНИИ

В России по-прежнему отсутствует единая централизованная статистика, позволяющая напрямую сравнивать количество кибератак за период 2022–2025 годов. Существующие данные носят фрагментарный характер: большинство цифр в публичных отчётах формируется на основе ограниченных выборок — расследований инцидентов у клиентов, телеметрии систем защиты, данных о выявленных APT-атаках и сведений, публикуемых на теневых форумах.

Тем не менее, анализ совокупных источников позволяет проследить устойчивый рост интенсивности атак. Согласно информации, собранной специалистами АО «ПМ», с 2023 года фиксируется стабильное увеличение количества APT-инцидентов, отражающее общее повышение активности киберпреступных группировок и геополитически мотивированных акторов. За 2025 год Россию атаковали более 90 группировок.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Search Open Websites/Domains	Stage Capabilities	Exploit Public-Facing Application	Windows Management Instrumentation	Modify Registry	Exploitation for Privilege Escalation	Deobfuscate/Decode Files or Information	OS Credential Dumping	System Information Discovery	Lateral Tool Transfer	Data from Local System	Ingress Tool Transfer	Exfiltration Over C2 Channel	Data Encrypted for Impact
Active Scanning	Acquire Infrastructure	Valid Accounts	Native API	Valid Accounts	Valid Accounts	Modify Registry	Credentials from Password Stores	File and Directory Discovery	Exploitation of Remote Services	Screen Capture	Protocol Tunneling	Automated Exfiltration	Inhibit System Recovery
Gather Victim Host Information	Acquire Access	Trusted Relationship	Exploitation for Client Execution	External Remote Services	Process Injection	Obfuscated Files or Information	Input Capture	Process Discovery	Remote Services	Automated Collection	Non-Application Layer Protocol	Exfiltration Over Web Service	Data Destruction
Gather Victim Identity Information	Compromise Accounts	External Remote Services	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading	Steal Web Session Cookie	System Network Configuration Discovery	Replication Through Removable Media	Clipboard Data	Remote Access Tools	Data Transfer Size Limits	System Shutdown/Reboot
Gather Victim Network Information	Compromise Infrastructure	Drive-by Compromise	Shared Modules	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Valid Accounts	Unsecured Credentials	System Owner/User Discovery	Taint Shared Content	Archive Collected Data	Non-Standard Port	Scheduled Transfer	Service Stop
Gather Victim Org Information	Develop Capabilities	Phishing	Scheduled Task/Job	Hijack Execution Flow	Hijack Execution Flow	Process Injection	Adversary-in-the-Middle	Remote System Discovery	Software Deployment Tools	Data from Removable Media	Application Layer Protocol	Exfiltration Over Alternative Protocol	Resource Hijacking
Phishing for Information	Establish Accounts	Replication Through Removable Media	System Services	Account Manipulation	Access Token Manipulation	Indicator Removal	Brute Force	Network Service Discovery	Use Alternate Authentication Material	Video Capture	Data Encoding	Exfiltration Over Other Network Medium	Account Access Removal
Search Closed Sources	Obtain Capabilities	Content Injection	User Execution	BITS Jobs	Account Manipulation	Virtualization/Sandbox Evasion	Exploitation for Credential Access	System Network Connections Discovery	Internal Spearphishing	Input Capture	Encrypted Channel	Exfiltration Over Physical Medium	Defacement
Search Open Technical Databases		Hardware Additions	Software Deployment Tools	Create Account	Abuse Elevation Control Mechanism	Reflective Code Loading	Modify Authentication Process	Network Share Discovery	Remote Service Session Hijacking	Audio Capture	Fallback Channels	Transfer Data to Cloud Account	Financial Theft
Search Threat Vendor Data		Supply Chain Compromise	Cloud Administration Command	Modify Authentication Process	Boot or Logon Initialization Scripts	Hide Artifacts	Multi-Factor Authentication Interception	Query Registry		Browser Session Hijacking	Proxy		Data Manipulation
Search Victim-Owned Websites		Wi-Fi Networks	Container Administration Command	Boot or Logon Initialization Scripts	Create or Modify System Process	Hijack Execution Flow	Network Sniffing	Account Discovery		Data from Network Shared Drive	Dynamic Resolution		Disk Wipe
			Deploy Container	Cloud Application Integration	Domain or Tenant Policy Modification	System Binary Proxy Execution	Steal Application Access Token	Application Window Discovery		Adversary-in-the-Middle	Web Service		Email Bombing
			ESXi Administration Command	Compromise Host Software Binary	Escape to Host	Access Token Manipulation	Forced Authentication	Software Discovery		Email Collection	Data Obfuscation		Endpoint Denial of Service
			Input Injection	Create or Modify System Process	Event Triggered Execution	Execution Guardrails	Forge Web Credentials	System Time Discovery		Data from Information Repositories	Multi-Stage Channels		Firmware Corruption
			Inter-Process Communication	Event Triggered Execution		File and Directory Permissions Modification	Multi-Factor Authentication Request Generation	Virtualization/Sandbox Evasion		Data Staged	Communication Through Removable Media		Network Denial of Service
			Poisoned Pipeline Execution	Exclusive Control		Impair Defenses	Steal or Forge Authentication Certificates	Browser Information Discovery		Data from Cloud Storage	Content Injection		
			Serverless Execution	Implant Internal Image		Rootkit	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Data from Configuration Repository	Hide Infrastructure		
				Office Application Startup		Template Injection		System Location Discovery			Traffic Signaling		
				Power Settings		BITS Jobs		System Service Discovery					
				Pre-OS Boot		Debugger Evasion		Domain Trust Discovery					
				Server Software Component		Exploitation for Defense Evasion		Group Policy Discovery					
				Software Extensions		Indirect Command Execution		Debugger Evasion					
				Traffic Signaling		Modify Authentication Process		Local Storage Discovery					
						Use Alternate Authentication Material		Log Enumeration					
						XSL Script Processing		Network Sniffing					
						Abuse Elevation Control Mechanism		Cloud Infrastructure Discovery					
						Build Image on Host		Cloud Service Dashboard					
						Delay Execution		Cloud Service Discovery					
						Deploy Container		Cloud Storage Object Discovery					
						Direct Volume Access		Container and Resource Discovery					
						Domain or Tenant Policy Modification		Device Driver Discovery					
						Email Spoofing		Password Policy Discovery					
						Impersonation		Permission Groups Discovery					
						Modify Cloud Compute Infrastructure		Virtual Machine Discovery					
						Modify Cloud Resource Hierarchy							
						Modify System Image							
						Network Boundary Bridging							
						Plist File Modification							
						Pre-OS Boot							
						Rogue Domain Controller							
						Selective Exclusion							
						Subvert Trust Controls							
						System Script Proxy Execution							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused/Unsupported Cloud Regions							
						Weaken Encryption							

В 2025 году число инцидентов выросло ещё на 27% по сравнению с предыдущим периодом, что подтверждает рост целенаправленных кампаний против российских организаций в различных отраслях.

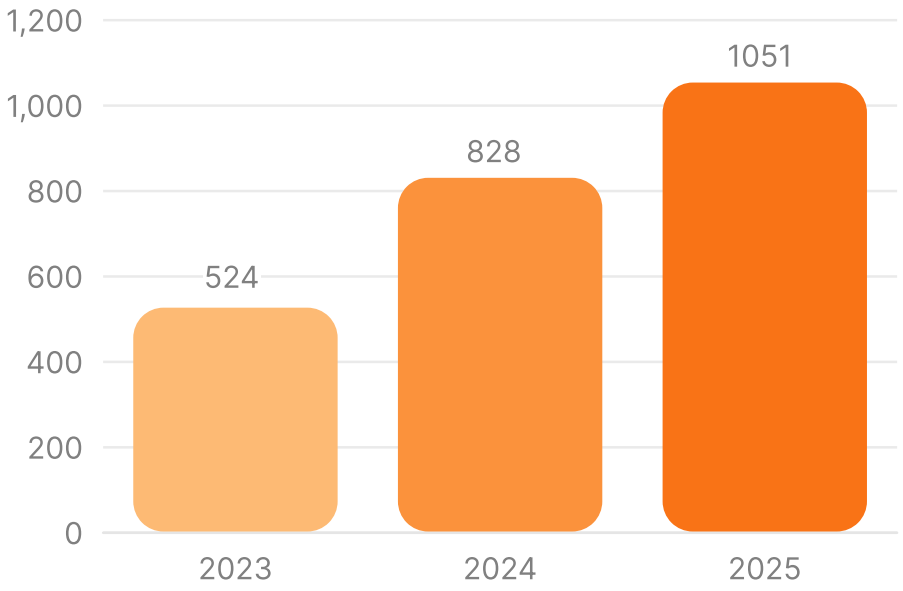


Диаграмма 1 - Общее число инцидентов

По данным открытых источников (отчёты крупных провайдеров DDoS-защиты, в т. ч. «Ростелеком-Солар» 1 и StormWall 2), в 2025 году фиксируется стабильно высокий уровень DDoS-нагрузки на российскую инфраструктуру.

За январь-сентябрь 2025 года по выборке одного из крупнейших провайдеров было отражено порядка 560 тыс. DDoS-атак, что соответствует в среднем ~60–65 тыс. атак в месяц.

В среднем на одну организацию приходилось порядка 1,2 тыс. DDoS-атак за 9 месяцев, то есть около 130 атак в месяц на компанию.

По другим провайдерам фиксируется годовой рост числа DDoS-атак на российские ресурсы порядка 40–80 % в зависимости от квартала и методики подсчёта.

Доля России в глобальном объёме DDoS-атак в 2025 году оценивается примерно в 10% (по отдельным заявлениям российских операторов — существенно выше, до «десятков процентов», что отражает различие методик учёта).

1 2

Наиболее заметные пики приходятся на месяцы, связанные с крупными политическими и общественно значимыми событиями (международные переговоры, юбилейные даты, выборы, крупные форумы).

Основной удар нацелен на критически важные отрасли — телеком, ИТ-провайдеров, финансовый сектор и государственный сектор, на которые суммарно приходится более половины зафиксированных атак. Типичная мощность атак измеряется единицами гигабит в секунду, но отдельные кампании достигают терабитного диапазона и могут продолжаться до нескольких суток, часто в многовекторном формате с активным использованием L7.

Ключевым фактором, поддерживающим высокий уровень угроз, остаётся геополитическая напряжённость, которая способствует совмещению трёх типов активности:

1. целенаправленные APT-операции, ориентированные на разведку и кражу данных;
2. криминальные кампании, преследующие финансовую выгоду;
3. хактивизм, выражающийся в символических или деструктивных атаках на публичные ресурсы.

При этом всё чаще отмечается, что классические разграничения между категориями злоумышленников стираются. Многие группировки сознательно не позиционируют себя как «хактивисты» или «APT», поскольку их деятельность носит гибридный характер — сочетает элементы киберпреступности, дезинформации и промышленного шпионажа. Такая трансформация отражает эволюцию угроз, при которой мотивы и методы атакующих выходят за рамки привычных шаблонов современной ИБ-среды России.

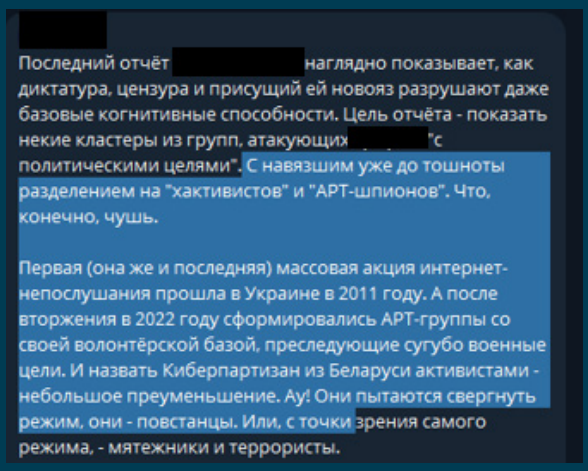


Рисунок 1 - Скриншот из чата группировки

ИМПОРТОЗАМЕЩЕНИЕ И ПЕРЕХОД К ТЕХНОЛОГИЧЕСКОМУ СУВЕРЕНИТЕТУ

Импортозамещение в сфере ИТ и кибербезопасности остаётся одним из ключевых направлений технологической политики России. В 2024–2025 годах наблюдается ускоренная миграция организаций на отечественные технологические стеки, что сопровождается временным ростом операционных рисков — нарушениями интеграций, кадровыми дефицитами и снижением совместимости решений. [3]

Сектор	Доля импортных решений в 2022 году	Доля импортных решений в 2025 году	Комментарий
Промышленность	~80%	~40%	Активная замена производственных и ИТ-систем отечественными аналогами; сохраняются зависимости от специализированных контроллеров и SCADA-платформ.
Информационная безопасность	~60%	~5% (95% замещения)	Высокие темпы перехода на отечественные SOC, SIEM и СЗИ; усиливается развитие экосистемы отечественных вендоров.
Критическая инфраструктура	~70%	~30–40%	Сохраняется зависимость от зарубежных промышленных ОС
Государственные компании и учреждения	~60%	~80–85% замещения	Лишь 15–20% компаний полностью выполнили нормативные требования по переходу на российское ПО.

Таблица 1 - Доля импортозамещения в 2022-2025 г.

На фоне санкционных ограничений и геополитической турбулентности российские организации массово переходят на отечественные решения, особенно в сегментах ИБ и офисных платформ.

Россия фактически достигла технологического лидерства в области средств защиты: более 90% SOC и SIEM-платформ локализованы, растёт экспорт отечественных решений в дружественные страны.

3

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРАТАКАХ

Период 2024–2025 годов характеризуется массовым внедрением генеративных моделей ИИ в инструментарий злоумышленников. Если ранее ИИ применялся в основном для автоматизации технических процессов, то сегодня он активно используется для масштабирования фишинга, социоинженерии и ускорения пост-эксплуатации — от анализа артефактов до автоматического написания скриптов и PowerShell-команд.

Особенно стремительно развиваются голосовые дипфейк-атаки (вишинг) и синтетический медиа-фрод. По оценкам отраслевых источников, в 2024–2025 годах число подобных инцидентов выросло на сотни процентов, при этом отмечаются случаи компрометации корпоративных систем через имитацию звонков от руководителей и партнёров.

ИИ постепенно становится стандартным инструментом, интегрированным как в отдельные виды вредоносного ПО, так и в ключевые этапы всей цепочки атаки.

Одним из примеров является SpamGPT. Эта платформа предоставляет инструменты для создания индивидуализированных фишинговых писем, автоматизации массовых рассылок, управления SMTP-инфраструктурой и анализа эффективности кампаний.

Такой подход значительно снижает порог вхождения: злоумышленнику уже не требуются ни навыки социальной инженерии, ни техническая подготовка — всё делает готовая модель.

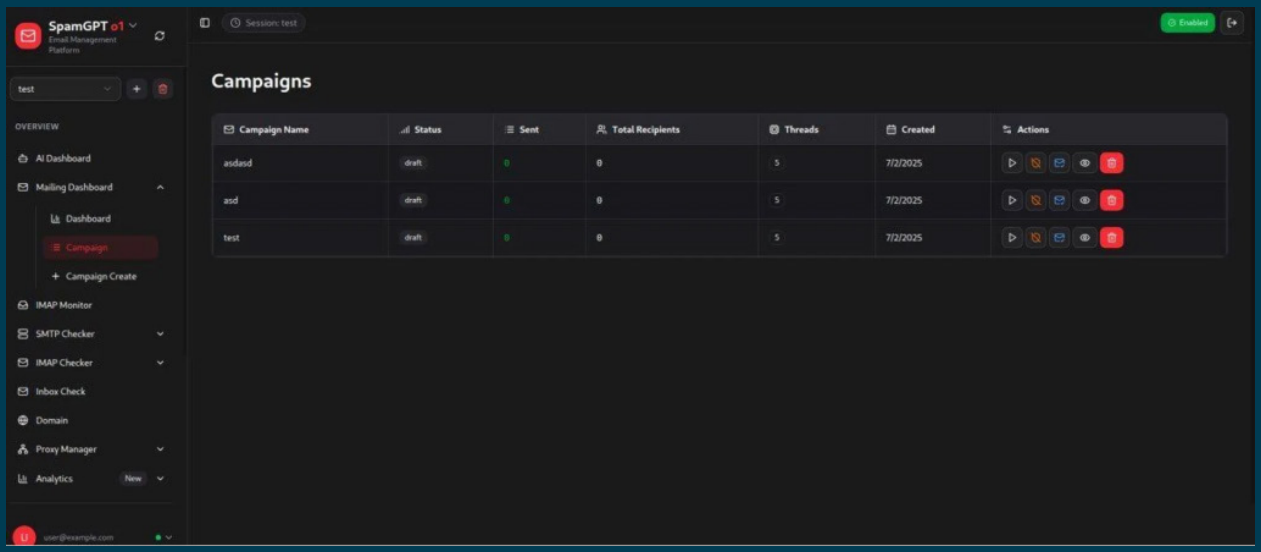


Рисунок 2 - Панель управления рассылками SpamGPT со статистикой

FraudGPT, DarkGPT и другие модели, построенные на модифицированных версиях GPT или LLaMA, сохраняют популярность. Однако на смену данным переработанным открытым моделям приходят полностью самостоятельно разработанные LLM, создаваемые специально под нужды киберпреступности. Одним из наиболее обсуждаемых примеров является Xanthorox AI. Данная языковая модель позиционируется как «универсальный помощник хакера». Она генерирует код, находит уязвимости, анализирует данные, работает с голосом и изображениями.

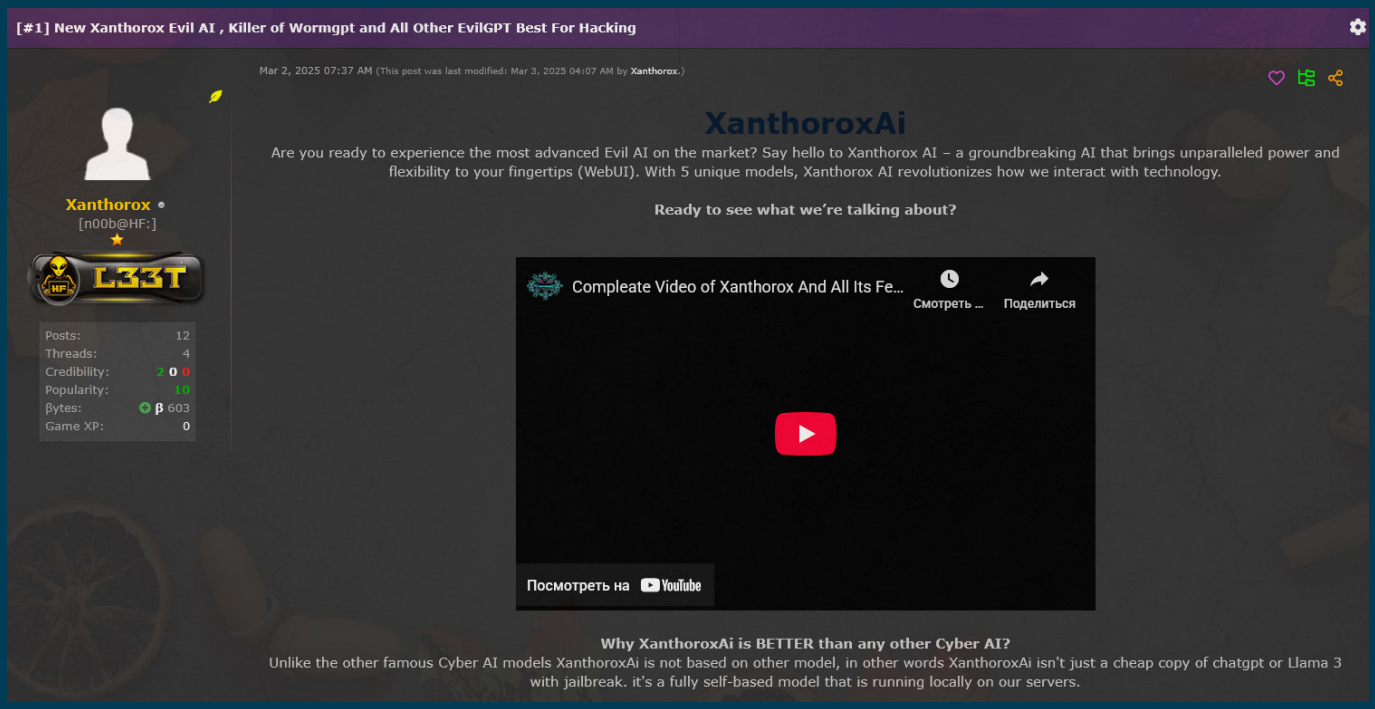


Рисунок 3 - Объявление о продаже Xanthorox AI

Основные направления атак, зафиксированные специалистами АО «ПМ»

1. Современные LLM-модели позволяют в реальном времени формировать высокореалистичные письма и сообщения, адаптированные под должность, стиль общения и контекст жертвы. Используется автоматический анализ открытых данных (соцсети, новости, корпоративные сайты) для точного выбора цели.

2. Злоумышленники клонируют голоса руководителей или родственников, совершая звонки по схемам «фейк-босс» или «имитация чрезвычайной ситуации».

3. Генеративные инструменты позволяют создавать копии легитимных порталов с высоким уровнем визуальной точности, что снижает вероятность выявления фишинга пользователями.

4 Модели применяются для автоматического анализа инфраструктуры, поиска уязвимостей и формирования эксплойтов. Хотя их выводы требуют проверки, такие инструменты значительно ускоряют этапы разведки и перемещения внутри периметра.

5 Набирает популярность применение ИИ-инструментов для очистки изображений и видео от встроенных меток подлинности, что усложняет задачу атрибуции и идентификации источников дезинформации.

Повышение скорости и точности атак, обеспечиваемое применением генеративного ИИ и автоматизации, снижает эффективность традиционных средств защиты, основанных на сигнатурах.

Современные фишинговые и социоинженерные сценарии адаптируются под конкретного пользователя, его должность и поведенческие паттерны, что делает классические фильтры и системы корреляции менее результативными.

В краткосрочной перспективе критически важно внедрять многоуровневые механизмы проверки подлинности коммуникаций, включая:

1. многофакторную аутентификацию (MFA);
2. обучение сотрудников методам выявления фишинговых атак;
3. автоматизированные процессы проверки переводов и запросов с финансовыми последствиями.

По этой же причине вендоры стремятся не просто реагировать на инциденты, а спрогнозировать их — выявлять аномалии, подозрительную активность, паттерны, которые могут предшествовать атаке и блокировать их до реального ущерба, применяя LLM.

Для выявления новых, ранее неизвестных атак специалисты АО «ПМ» используют разработанную систему выявления и предупреждения атак на веб-ресурсы — AML Web Protection [4]. Система использует логи (журналы) веб-сервера для поведенческого анализа пользовательских запросов и выявления среди них атакующих сессий.

На основании анализа инцидентов специалисты АО «ПМ» отмечают, что социальная инженерия по-прежнему остаётся основным вектором первичного проникновения.

Именно через доверительные коммуникации злоумышленники получают доступ к инфраструктуре и учётным данным. Так, за 2025 год в 60% случаев в качестве первоначального доступа использовались различные методы фишинга, при которых пользователь самостоятельно открывает письмо, переходит по ссылке или скачивает вредоносное вложение, затем запускает его.

4

ПРОФИЛЬ АТАК В РОССИИ: МЕТОДЫ, ИНСТРУМЕНТЫ, УЯЗВИМОСТИ

ЭКОСИСТЕМА ДАРКВЕБА

Современный даркнет стал площадкой, где киберпреступность превратилась в организованный рынок с собственными продуктами, сервисами и поставщиками. Предложения на данном рынке охватывают весь цикл атаки — от первоначального доступа до монетизации похищенных данных.

Анализ объявлений на четырёх ведущих даркнет-площадках за 2025 год показал, что лидерами по количеству предложений о продаже стали стилеры (порядка 63 предложений). Немного отстают от них криптеры (60 предложений), замыкают тройку лидеров загрузчики с 50 предложениями о продаже.

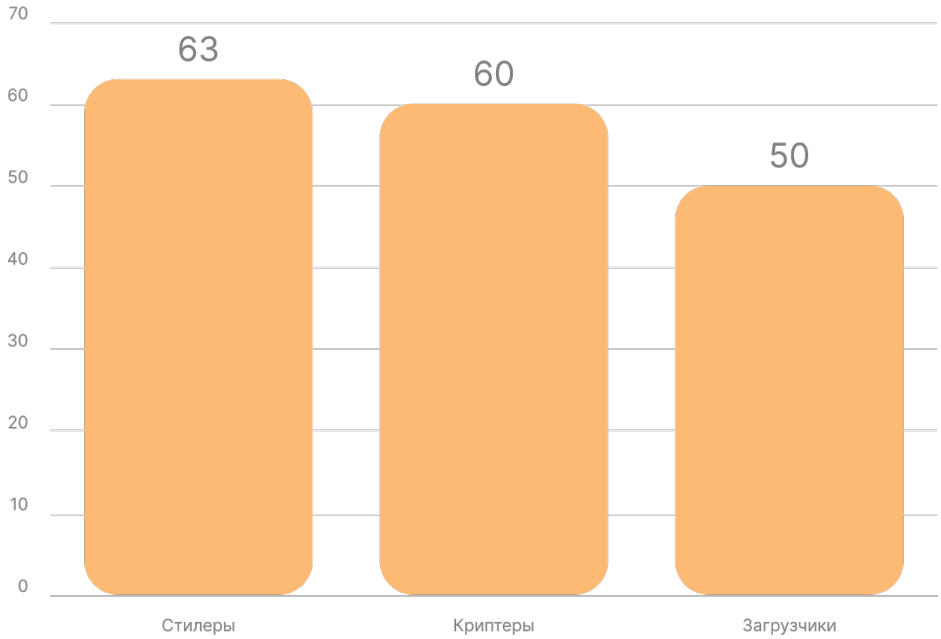


Диаграмма 2 - Статистика предложений о продаже ВПО на дарквеб-площадках за 2025 г.

Дарквеб сформировался в полноценную экосистему, где услуги и инструменты образуют взаимосвязанную инфраструктуру. Ниже представлена таблица с расценками на ВПО, собранная аналитиками АО «ПМ».

Категория	Примерная стоимость
Stealer	От $200 в месяц / от $3000 за полный код
Crypter	От $25 за 1 крипт
Loader	От $50 в месяц / от $10 за 1 билд
AV/EDR/XDR Killer	От $400 билд
RAT	От $50 в месяц
Drainer	20–30% от каждой украденной суммы
Ransomware as a Service	20–40% от каждой украденной суммы и первоначальный взнос за доступ к платформе ($1000–3000)
Miner	От $70 за 1 билд
DDoS	От $60/день
Initial Access	$50–5000+
0day / 1day exploit	$1000–1000000+

Таблица 2 - Расценка ВПО на дарквеб-площадках в 2025 году

В рамках экосистемы дарквеба различные группы и сервисы взаимодействуют между собой, образуя тесно связанную цепочку. Наиболее показательная модель: инфостилеры — брокеры доступа — шифровальщики. Стилеры играют роль первичной точки сбора данных, они массово собирают учётные записи, веб-сессии, cookies и другую цифровую информацию. Эти сведения (логи) становятся товаром на рынке, где их приобретают брокеры доступа. Брокеры сортируют, проверяют и агрегируют такие данные, превращая необработанные логи в доступы к корпоративным или индивидуальным системам.

Далее в цепочку вступают вымогатели. Они приобретают доступы и используют их как точки входа для последующих этапов атаки. Таким образом, даже простые и относительно дешёвые инструменты, такие как стилеры, оказывают прямое влияние на весь рынок, обеспечивая основу для более сложных и дорогостоящих операций.

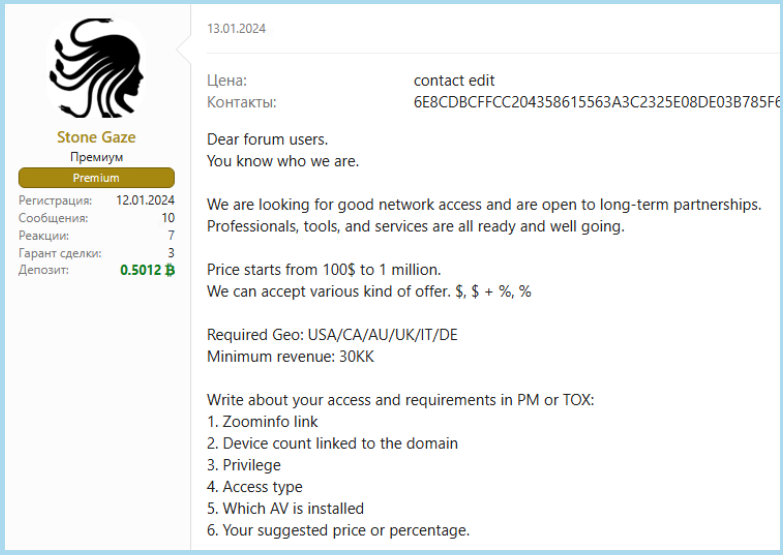
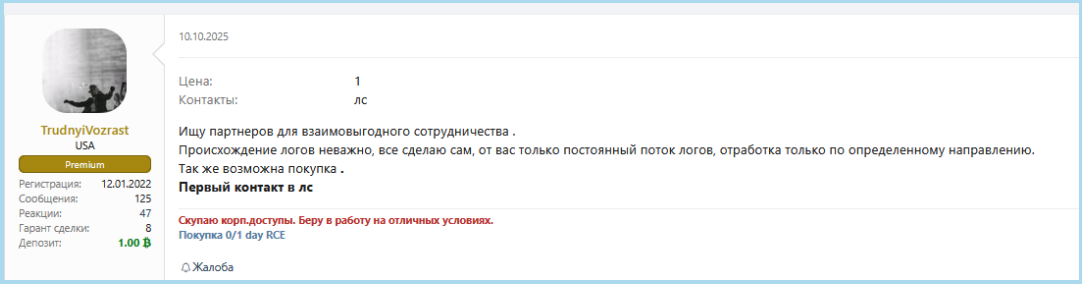


Рисунок 4 - Объявление Meduza Ransomware о поиске брокеров доступа



10.10.2025

Цена: 1
Контакты: лс

TrudnyiVozrast
USA
Premium
Регистрация: 12.01.2022
Сообщения: 125
Реакции: 47
Гарант сделки: 8
Депозит: 1.00 ₿

Ищу партнеров для взаимовыгодного сотрудничества .
Происхождение логов неважно, все сделаю сам, от вас только постоянный поток логов, отработка только по определенному направлению.
Так же возможна покупка .
Первый контакт в лс

Скупаю корп.доступы. Беру в работу на отличных условиях.
Покупка 0/1 day RCE

Жалоба

Рисунок 5 - Предложение о покупке логов для их обработки

Также на рынке распространены комплексные решения ВПО: один из участников преступного форума, например, предлагает по одной подписке сразу несколько решений- Botnet, HVNC, HCDP, Keylogger, Stealer, Clipper, Resident Loader и RAT.

Ценовая политика / Pricing policy

Название тарифа / Tariff name	Доступные модули / Available modules	Цена за неделю / Price per week	Цена за две недели / Price for two weeks	Цена за месяц / Price per month
Стандартный / Standard	Все стандартные / All standard	300$	500$	800$
Профессионал / Professional	Все стандартные + Стиллер + Лоадер / All standard + Stealer + Loader + API	500$	800$	1200$
Корпоративный / Entrerprise	Все стандартные + Стиллер + Лоадер + HVNC + HCDP / All standard + Stealer + Loader + HVNC + HCDP + API	850$	1200$	2000$

Пожизненные (lifetime) лицензии не предусмотрены!
Lifetime licenses are not provided!

Рисунок 6 - Предложение о покупке логов для их обработки

Теневые площадки демонстрируют устойчивый сдвиг к сервисным моделям: вредоносные инструменты и сопутствующие услуги всё чаще предлагаются не как разовые продукты, а как полнофункциональные сервисы по подписке или в формате партнёрских программ. Это формирует устойчивую модель взаимодействия между разработчиками и их клиентами: операторы получают предсказуемый денежный поток, а пользователи — регулярные обновления, техническую поддержку и доступ к готовой инфраструктуре.

Тенденция перехода к сервисной модели затрагивает не только ВПО, но и рынок эксплойтов. Если ранее злоумышленники преимущественно продавали сам код, эксплуатирующий уязвимость, то сейчас набирает популярность формат exploit-as-a-service: киберпреступник упаковывает эксплойт в удобный для развертывания модуль или скрипт и предоставляет его в аренду.

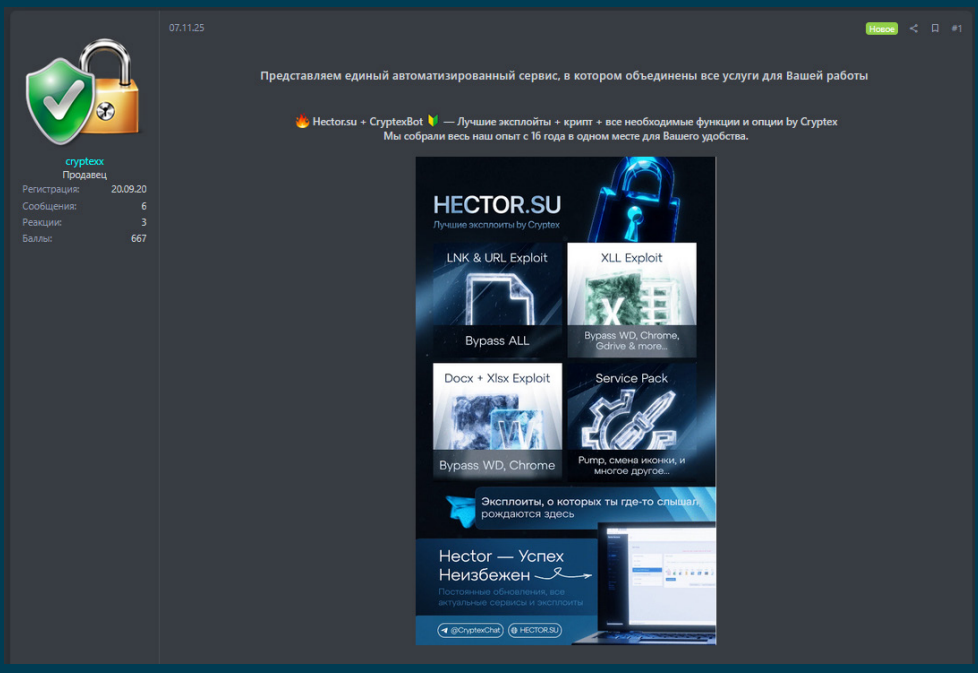


Рисунок 7 - Пример EaaS

РОЛЬ INITIAL ACCESS BROKERS В ЭКОСИСТЕМЕ АТАК

В 2025 году специалисты АО «ПМ» отмечают существенный рост активности Initial Access Brokers (IAB) — субъектов киберугроз, специализирующихся на несанкционированном получении доступа к корпоративным сетям и системам с последующей продажей этого доступа злоумышленникам, в том числе пользователям программ-вымогателей.

По сути, IAB выступают как «высокомаржинальные посредники», предоставляющие модель access-as-a-service: они монетизируют успешный взлом, минимизируя собственные риски за счёт отказа от участия в финальных стадиях атаки.

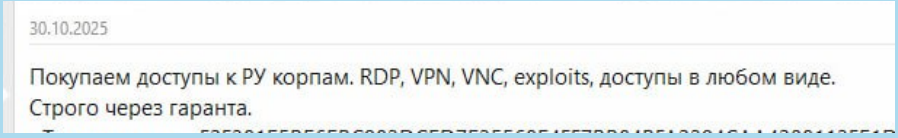


Рисунок 8 - Предложение о покупке доступа

Такая модель посредничества органично встраивается в экосистему ransomware-as-a-service (RaaS), позволяя злоумышленникам обходить трудоёмкий и длительный этап первоначального проникновения.

В рамках RaaS именно IAB специализируются на поиске и эксплуатации уязвимостей, формируя устойчивые точки присутствия в сетях жертвы и продавая готовый доступ операторам шифровальщиков, которые сразу переходят к развёртыванию полезной нагрузки.

TTP Initial Access Brokers

Технический профиль IAB и смежных сервисов можно связать с MITRE ATT&CK:

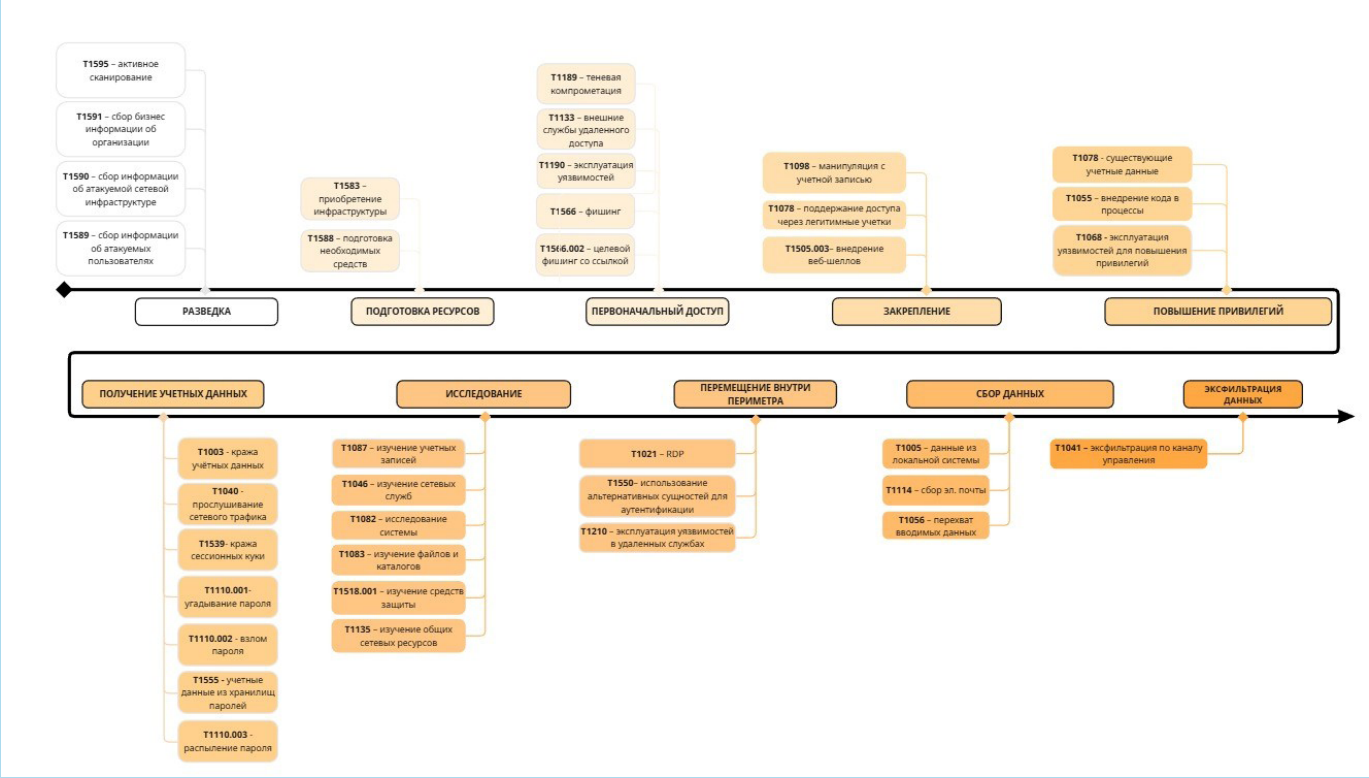


Рисунок 9 - Технический профиль атак

Рынок IAB к 2025 году фактически представляет собой сформированную B2B-платформу внутри криминальной экосистемы:

- типовые лоты: доступ к RDP/VPN, доменным контроллерам, e-mail-инфраструктуре, облачным аккаунтам, VDI (инфраструктура виртуальных рабочих столов), панелям администрирования отраслевых систем;
- в объявлениях стандартизируются метрики: отрасль, выручка/размер компании, страна, уровень доступа (user/admin/domain admin), наличие и тип средств защиты (EDR/XDR, SIEM, WAF), сетевой сегмент (корпоративный/OT/облако);
- ценник привязывается к качеству и «монетизируемости» актива: доступ к крупной компании без современного EDR оценивается значительно выше;
- развивается практика предоставления эксклюзивности на доступ (продажа в одни руки) либо, напротив, массовой перепродажи менее критичных активов.

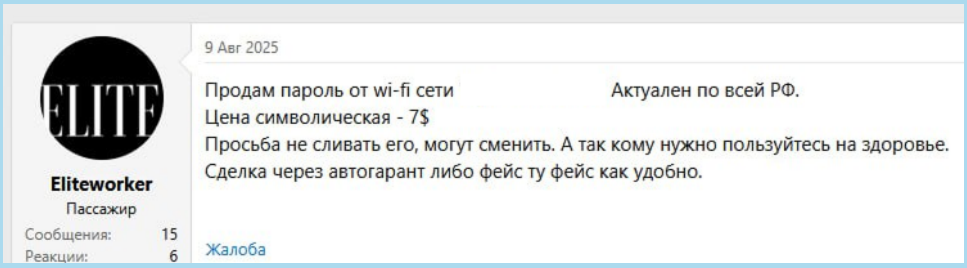


Рисунок 10 - Пример продажи с форума

Это формирует для защитной стороны важный риск: успешная компрометация необязательно приводит к немедленной финальной атаке — доступ может «выдерживаться» и продаваться, что увеличивает окно скрытого присутствия в сети.

Связь IAB с ростом ВПО и фрагментацией RaaS

- группировки всё чаще специализируются на финальных стадиях (развёртывание, шифрование, извлечение (кража), переговоры по выкупу), не тратя ресурсы на первичное проникновение и разведку;
- значительная доля успешных атак с шифрованием организуется через заранее купленный доступ;
- экосистема кибератак фрагментируется: отдельно стоят поставщики доступа (IAB), операторы инфраструктуры (абузоустойчивый хостинг (bulletproof-хостинг), прокси), разработчики ВПО и криптеров, специалисты по отмыванию средств, переговорщики.

Для организаций это означает ускорение всего цикла атаки: между первичной компрометацией и запуском шифровальщика может проходить существенно меньше времени, особенно если доступ продаётся «под конкретного» оператора.

5

6

7

Premier Pass-as-a-Service и операционные альянсы

Отдельно стоит выделить переход к модели premier pass-as-a-service [5] [6] — расширенному варианту «доступа как услуги», при котором акторы передают не просто первичный вход, а прямой доступ к уже контролируемым и подготовленным активам.

Такой подход смещает фокус с классических брокеров первоначального доступа на операционные альянсы между APT-группами и киберпреступными формированиями:

- одна группа специализируется на разведке, первичном доступе и закреплении в стратегически важных сетях;
- другая использует этот доступ для шпионажа, саботажа или финансово мотивированных операций;
- инфраструктура и опорные точки могут использоваться многократно и несколькими акторами, что существенно усложняет атрибуцию.

По данным Trend Micro [7], можно выделить четыре уровня такой кооперации: от эпизодического пересечения интересов до предоставления партнёрам полностью готовой инфраструктуры («операционного бокса»). Наиболее продвинутый сценарий предполагает использование облачных сервисов (например, VS Code Remote Tunnel) в качестве устойчивого RAT-канала для скрытого удалённого управления.

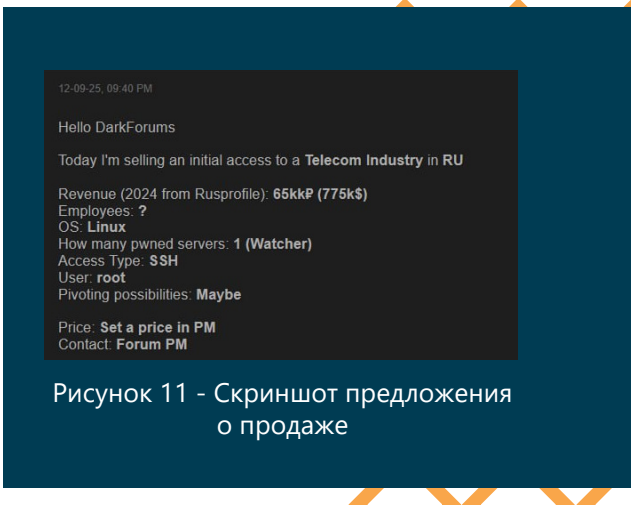


Рисунок 11 - Скриншот предложения о продаже

ВРЕДОНОСНОЕ ПО И ИНСТРУМЕНТАРИЙ

По данным специалистов АО «ПМ» в 2025 году вредоносное ПО используется примерно в 2/3 успешных атак на российские организации, причём чаще всего в роли средства закрепления в инфраструктуре или финальной фазы атаки выступают шифровальщики.

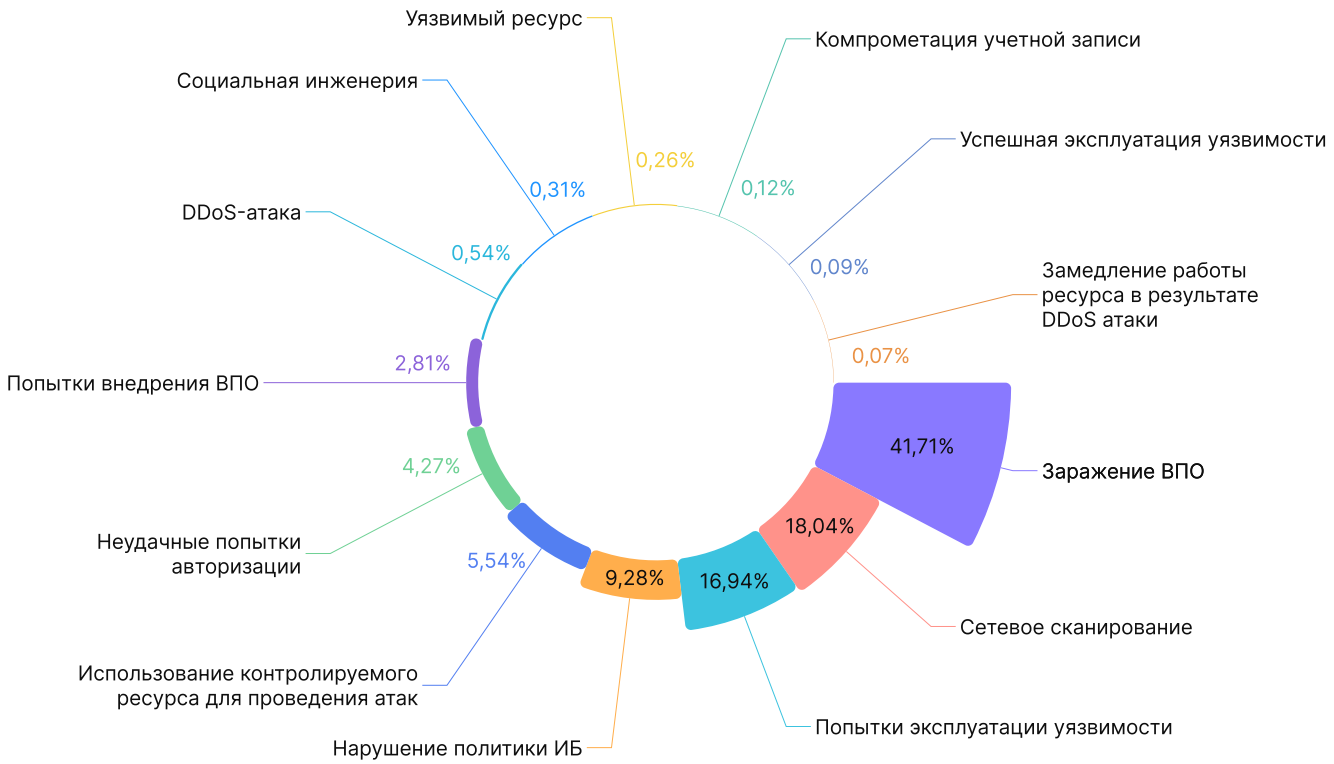


Диаграмма 3 - Статистика инцидентов по данным АО «ПМ»

Анализ статистики по инцидентам и открытым данным показывает, что в 2025 году атаки на российскую инфраструктуру базируются прежде всего на массово доступном ВПО.

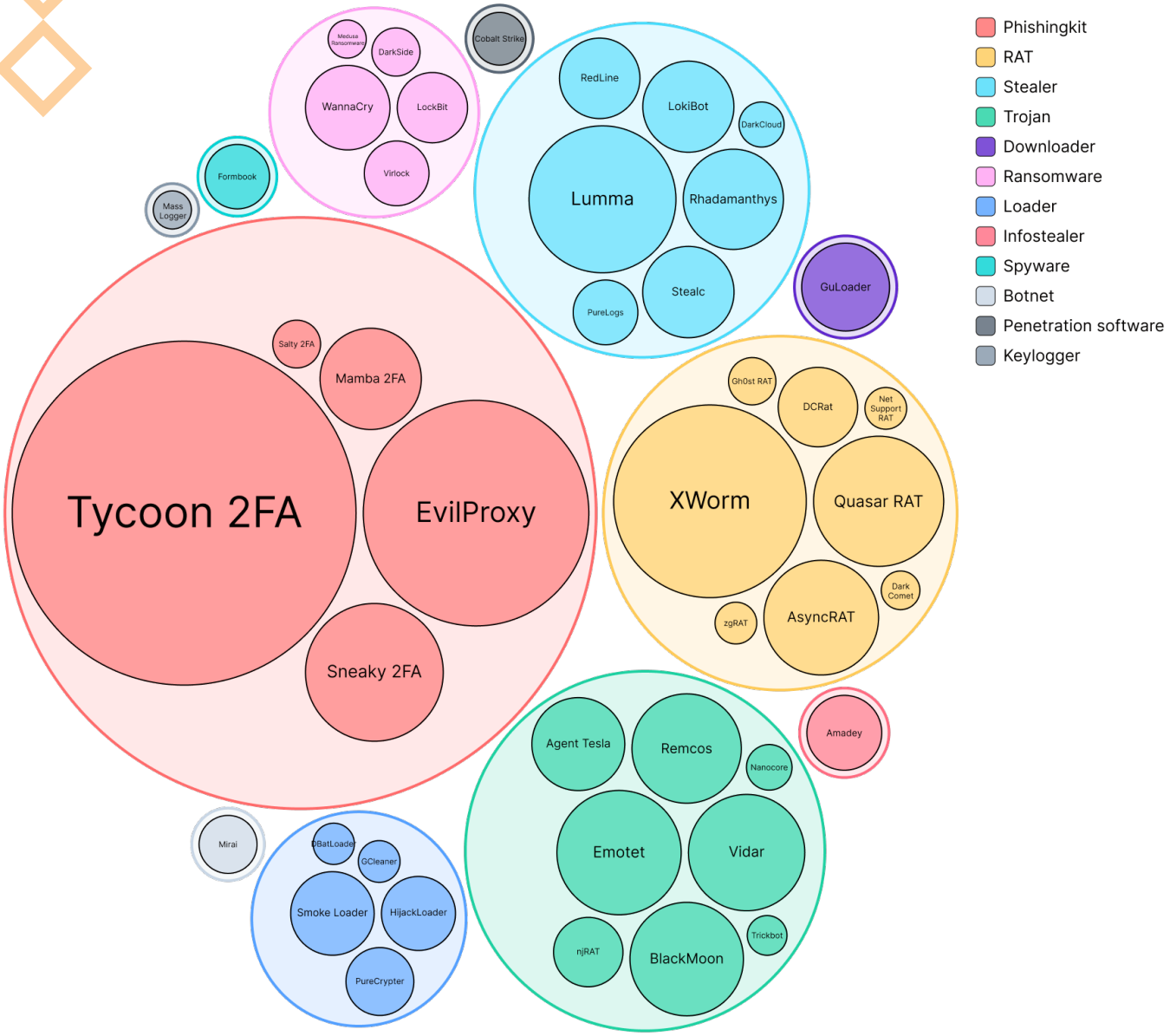


Диаграмма 4 - Используемое в 2025 году ВПО

Ключевую роль играют фишинг-киты (Tycoon 2FA, EvilProxy и др.), обеспечивающие кражу учётных записей, а также многофункциональные трояны и RAT (XWorm, QuasarRAT, AsyncRAT, Emotet, Remcos, Agent Tesla), которые используются для закрепления в сети и дальнейшего управления.

Рисунок 12 - Предложение о продаже Tycoono продаже

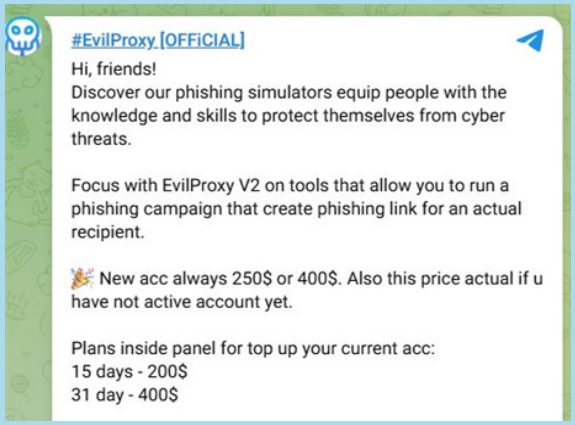


Рисунок 13 - Предложение о продаже EvilProxy

Tycoon 2FA отличается развитой панелью управления, которая в реальном времени отображает ключевые метрики атаки: количество успешных входов, перехваченных учетных данных, а также эффективность блокировки автоматических сканеров и систем анализа.

Платформа EvilProxy, в свою очередь, делает ставку на устойчивость инфраструктуры, интегрируя IP-прокси для маскировки исходного хостинг-провайдера и усложнения отслеживания. Для дополнительной маскировки трафика многие из этих решений по умолчанию используют CAPTCHA, которая отфильтровывает ботов и усложняет автоматизированный анализ их фишинговых страниц.

Фишинг-киты больше направлены на новичков, желающих присоединиться к цифровому преступному миру.

В подавляющем большинстве результативных цепочек атак фиксируется применение инфостилеров (Lumma, RedLine, Stealc, LokiBot, Rhadamanthys, Raccoon и др.), выполняющих автоматизированный сбор и эксфильтрацию учётных данных, а также загрузчиков (GuLoader, Smoke Loader и т.п.), формирующих дополнительный обфускационный слой между этапом эксплуатации уязвимости и доставкой основной вредоносной полезной нагрузки.

В качестве финальной стадии нередко применяются шифровальщики (WannaCry-подобные, LockBit, Babuk, DarkSide, REvil, BlackMatter и др.) и ботнет-компоненты (Mirai, Tofsee, HEH IoT), что позволяет злоумышленникам либо монетизировать атаку, либо нарушать работоспособность сервисов через DDoS и шифрование ресурсов.

Указанное свидетельствует, что при проведении атак на информационную инфраструктуру, ключевую роль играют не некие «экзотические» образцы ВПО, а массово доступные фишинг-киты и коммодити-вредоносное программное обеспечение (в первую очередь средства удалённого доступа), предназначенные для хищения учётных данных и формирования плацдарма для последующего развертывания шифровальщиков, либо осуществления деструктивных (саботажных) действий.

Наиболее часто встречающимися последствиями успешно проведённых атак на организации являются утечки информации (конфиденциальной, ПДн и т.д.)

Роскомнадзор в 2025 году зафиксировал 103 утечки ПДн (~50 млн записей), что меньше 2024 года (135 утечек, 710 млн записей).

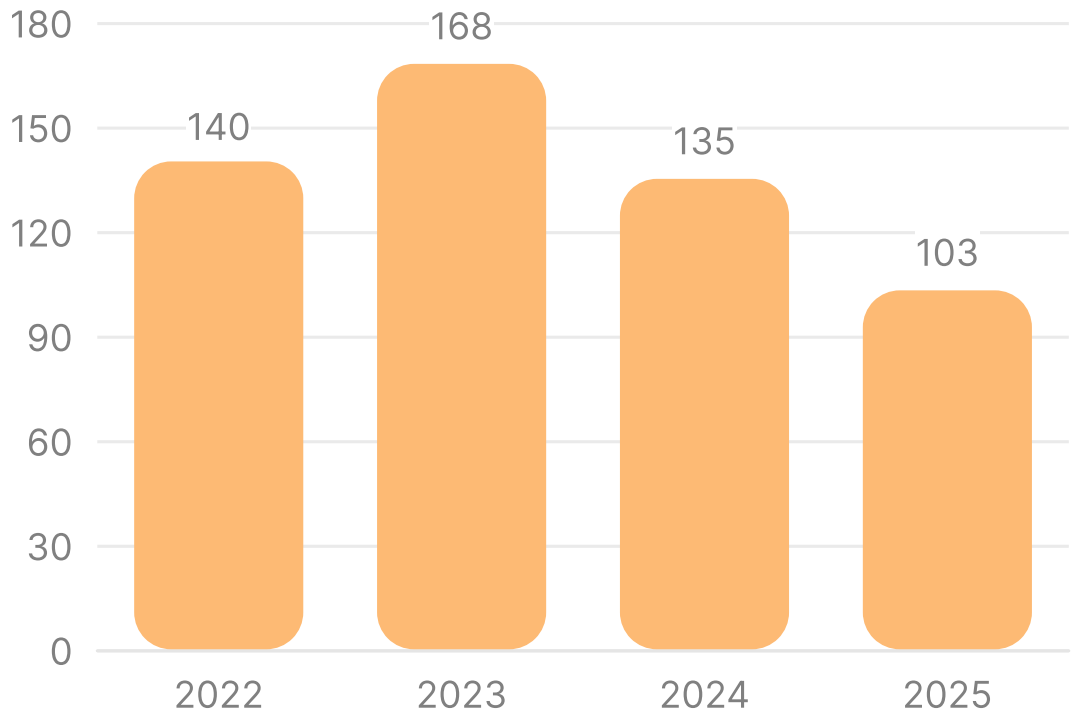


Диаграмма 5 - Количество утечек по данным Роскомнадзора

[8]

Специалисты Solar отмечают рост объёма утечек в 2025 году в 138 раз по сравнению с 2024 годом. Объём утекших данных составил 748 терабайт [8].

Согласно данным АО «ПМ» за 2025 год зафиксировано 1,6 млрд записей.

Диаграмма 6 - Утечки информации за 2025 год по данным АО «ПМ»

1 Государственный сектор занимает первое место — 497 млн. записей. Несмотря на повышенные меры защиты, инциденты в органах власти и муниципальных структурах часто связаны с человеческим фактором (ошибки операторов, несанкционированные выгрузки из реестров).

2 Коммерческий сектор — основной источник утечек (более 450 млн записей). Это отражает высокий уровень цифровизации и слабый контроль над внутренними системами хранения данных, особенно у e-commerce, маркетплейсов.

3 Медицинские организации — третий по объёму сегмент утечек (302 млн записей). Это подтверждает уязвимость МИС и лабораторных сервисов, где хранятся персональные и биометрические данные. Медицинские базы остаются одними из самых ценных на теневых форумах.

4 Онлайн-платформы и соцсети обеспечили более 267 млн утечек вместе, что указывает на высокий риск в сегменте пользовательских данных (аккаунты, токены, контактные цепочки). Эта сфера часто становится мишенью для фишинговых кампаний и спама.

5 Финансовый сектор (15 млн записей) демонстрирует относительно низкий объём утечек, но высокую чувствительность данных. Даже единичные инциденты приводят к серьёзным репутационным и юридическим последствиям.

Следует учитывать, что представленные количественные оценки могут варьироваться в зависимости от источника и методики сбора данных:

- официальная статистика формируется на основе обязательной отчётности организаций, уведомляющих государственные органы о киберинцидентах;
- неполнота данных возможна из-за того, что компании не всегда публично сообщают об утечках или атаках, опасаясь репутационных и правовых рисков;
- оценки вендоров и исследовательских центров зачастую шире, так как включают результаты проактивного мониторинга и анализа теневых площадок, где фиксируются инциденты, не попавшие в официальные сводки;
- хронологический сдвиг также влияет на статистику: утечки, опубликованные в 2025 году, могут относиться к компрометациям, произошедшим ещё в 2022–2023 годах.

Таким образом, выделим общие тенденции:

- смещение фокуса атакующих на массовые пользовательские базы, а не на точечные целевые атаки;
- рост вторичных утечек — публикации старых баз (например, взлом 2022 г. — слив 2025 г.);
- переоценка роли аутсорсеров и подрядчиков: часть утечек происходит через внешние IT-службы;
- телекоммуникации, образование и транспорт показывают меньшие значения, однако данные этих отраслей всё чаще фигурируют как вторичные утечки (через подрядчиков и интеграторов).

Дополнительным риском становится маскированный сетевой трафик, проходящий через VPN-приложения и сервисы, запрещённые корпоративными политиками.

Злоумышленники активно используют такие каналы для обхода систем мониторинга и DLP-решений, шифруя фишинговые и командные соединения в легитимный сетевой поток. Это требует:

- пересмотра политик сетевой безопасности;
- внедрения анализа поведенческих аномалий;
- ограничения или сегментации VPN-доступа.

ТРИ НАИБОЛЕЕ ЗНАЧИМЫХ КЕЙСА ГОДА

Mamont

Одной из ключевых тенденций в актуальном киберландшафте является рост активности троянов, распространяемых через мессенджеры. Характерным примером выступает троян Mamont, ставший популярным среди киберпреступников в экосистеме Telegram.

Распространение осуществляется за счёт социальной инженерии: пользователям пересылаются вредоносные файлы в формате .apk, замаскированные под фото- или видеоматериалы, которые сопровождаются сообщениями провокационного характера Например: «Это ты на фото?».

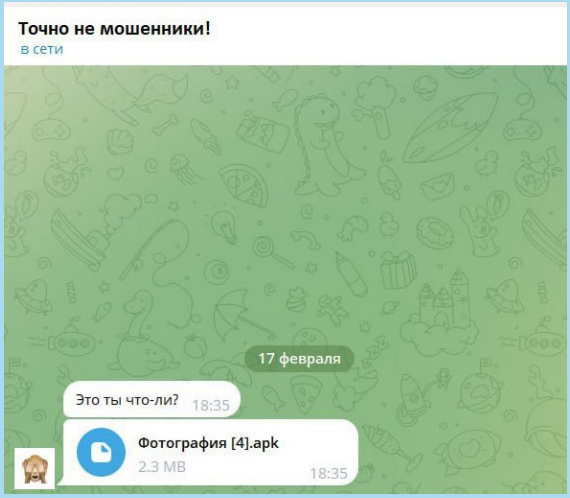


Рисунок 14 - Пример сообщения

```
00B|000  72 65 73 2F 6D 69 70 6D 61 70 2D 78 78 78 68 64  res/mipmap-xxxhd
00B|010  70 69 2F 69 63 5F 6C 61 75 6E 63 68 65 72 5F 72  pi/ic_launcher_r
00B|020  6F 75 6E 64 2E 77 65 62 70 00 18 18 72 65 73 2F  ound.webp...res/
00B|030  78 6D 6C 2F 62 61 63 6B 75 70 5F 72 75 6C 65 73  xml/backup_rules
00B|040  2E 78 6D 6C 00 21 21 72 65 73 2F 78 6D 6C 2F 64  .xml.!!res/xml/d
00B|050  61 74 61 5F 65 78 74 72 61 63 74 69 6F 6E 5F 72  ata_extraction_r
00B|060  75 6C 65 73 2E 78 6D 6C 00 0A 0A 73 61 6E 73 2D  ules.xml...sans-
00B|070  73 65 72 69 66 00 10 10 73 61 6E 73 2D 73 65 72  serif...sans-ser
00B|080  69 66 2D 6C 69 67 68 74 00 11 11 73 61 6E 73 2D  if-light...sans-
00B|090  73 65 72 69 66 2D 6D 65 64 69 75 6D 00 1E 1E 77  serif-medium...w
00B|0A0  73 3A 2F 2F 31 2E 6D 61 6D 6F 6E 74 76 69 72 75  s://1.mamontviru
00B|0B0  73 2E 6E 65 74 3A 38 38 38 38 2F 77 73 00 11 1F  s.net:8888/ws...
00B|0C0  D0 94 D0 B0 D0 B9 D1 82 D0 B5 D0 A4 D0 B8 D0 BA  Ð”Ð°Ð¹Ñ‚Ðµ Ð¤Ð¸Ð
00B|0D0  D1 81 D1 83 37 30 24 D0 94 D0 B5 D0 BD D1 8C 00  Ñ.Ñƒ70$Ð”ÐµÐ½ÑŒ.
00B|0E0  66 80 BB D0 94 D0 BB D1 8F 20 D0 BA D0 BE D1 80  f€»Ð”Ð»Ñ. Ð°Ð¾Ñ€
00B|0F0  D1 80 D0 B5 D0 BA D1 82 D0 BD D0 BE D0 B9 20 D1  Ñ€ÐµÐ°Ñ‚Ð½Ð¾Ð¹ Ñ
00B|100  80 D0 B0 D0 B1 D0 BE D1 82 D1 8B 20 D0 BF D1 80  €Ð°Ð±Ð¾Ñ‚Ñ‹ Ð¿Ñ€
00B|110  D0 B8 D0 BB D0 BE D0 B6 D0 B5 D0 BD D0 B8 D1 8F  Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ.
00B|120  20 D0 BD D0 B5 D0 BE D0 B1 D1 85 D0 BE D0 B4 D0   Ð½Ð¾Ð±Ñ…Ð¾Ð´Ð
00B|130  B8 D0 BC D0 BE 20 D1 83 D1 81 D1 82 D0 B0 D0 BD  ¸Ð¼Ð¾ ÑƒÑ.Ñ‚Ð°Ð½
00B|140  D0 BE D0 B2 D0 B8 D1 82 D1 8C 20 D0 B5 D0 B3 D0  Ð¾Ð²Ð¸Ñ‚ÑŒ ÐµÐ³Ð
00B|150  BE 20 D0 B2 20 D0 BA D0 B0 D1 87 D0 B5 D1 81 D1  ¾ Ð² Ð°Ð°Ñ‡ÐµÑ.Ñ
00B|160  82 D0 B2 D0 B5 20 D0 BF D1 80 D0 B8 D0 BB D0 BE  ‚Ð²Ðµ Ð¿Ñ€Ð¸Ð»Ð¾
```

Рисунок 15 - Фрагмент hex-дампа

Подобный подход стимулирует пользователя к открытию файла и запуску установки без должной проверки источника.

После установки троян запрашивает у пользователя расширенные разрешения, критичные с точки зрения информационной безопасности и конфиденциальности: доступ к сети, чтение, перехват и отправку SMS-сообщений и иных уведомлений, а также доступ к контактам и истории телефонных вызовов.

Получив эти права, вредоносное ПО выстраивает сетевое взаимодействие с инфраструктурой злоумышленников: для загрузки дополнительных модулей используются протоколы HTTP и HTTPS, а для связи с C&C-сервером применяется канал на базе WebSocket. Такая архитектура позволяет гибко наращивать функциональность трояна и оперативно управлять заражёнными устройствами.

Основная целевая функция Mamont и аналогичных семейств — компрометация финансовых данных.

За счёт перехвата SMS, уведомлений и взаимодействия с платежными сервисами злоумышленники получают доступ к данным банковских карт и учётным записям в платёжных системах.

Дополнительным фактором риска является встроенная функция автоматической пересылки заражённых файлов всем контактам жертвы в Telegram, что обеспечивает быстрое и лавинообразное распространение вредоносной программы среди большого числа пользователей без участия оператора на каждом шаге.

По статистическим данным, в России с использованием вредоносных программ с аналогичным функционалом было скомпрометировано более 100 тысяч Android-устройств. Это указывает на масштаб проблемы и подтверждает, что мобильные трояны, распространяемые через мессенджеры и ориентированные на кражу данных банковских карт, являются значимым элементом современного киберландшафта и требуют приоритетного внимания при выработке мер защиты.

DeliveryRAT

Всё более заметной становится тенденция использования корпоративной тематики и узнаваемых брендов для распространения вредоносного ПО. Характерным примером является Android-троян DeliveryRAT, распространяемый под видом служебных приложений для сотрудников. Сценарий атаки строится на социальной инженерии: пользователю предлагается установить «обязательное» или «производственное» приложение, якобы связанное с рабочими процессами, логистикой или обслуживанием клиентов. Такой подход повышает уровень доверия и снижает вероятность критической оценки источника установки.

Ключевой целью злоумышленников является сбор конфиденциальных данных и последующая кража денежных средств. Для реализации этих задач троян запрашивает расширенный набор разрешений, позволяющих сформировать практически полный профиль активности пользователя. В частности, осуществляется сбор номера мобильного телефона, информации об операторе сотовой связи, а также предоставляется доступ к чтению и отправке SMS-сообщений. Дополнительно вредоносное ПО может перехватывать и скрывать push-уведомления, что затрудняет обнаружение подозрительных операций и уведомлений от банков и платёжных сервисов.

Сбор содержимого буфера обмена, данных об установленных приложениях и другой информации об операционной системе позволяет злоумышленникам точнее адаптировать атаки под конкретное устройство и

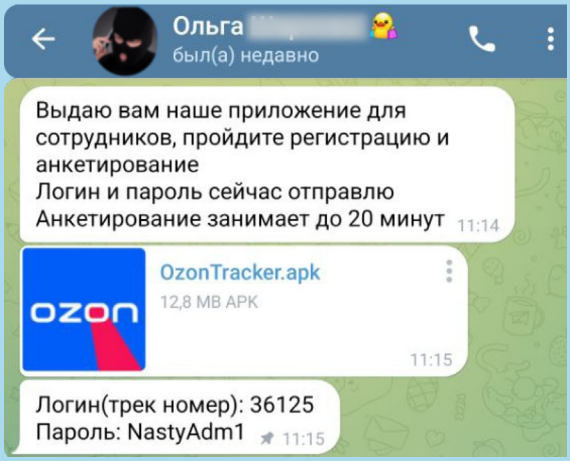


Рисунок 16 - Переписка со злоумышленником

используемую пользователем инфраструктуру.

Для повышения эффективности распространения DeliveryRAT маскируется под приложения известных брендов и сервисов, в том числе служб доставки, маркетплейсов и банковских приложений. В публичных аналитических материалах, в частности в отчёте компании F6 [9], указывается использование различных наименований одного и того же вредоносного ПО, такого как CdekTracker, AvitoTracker, WildberriesTracker и др. Это затрудняет его идентификацию конечными пользователями и может вводить в заблуждение даже при беглом визуальном контроле иконки и названия приложения.

Таким образом, DeliveryRAT и связанные с ним модификации представляют собой характерный пример эволюции мобильных угроз, ориентированных на финансовую мотивацию и эксплуатирующих доверие к известным брендам и корпоративной коммуникации. Наличие у трояна широкого набора прав, позволяющих контролировать коммуникации и получать доступ к конфиденциальным данным, делает подобные кампании значимым фактором риска для пользователей Android-устройств.

9

GemoDL

Специалистами АО «ПМ» зафиксирована атака с применением ранее неизвестного ВПО GemoDL, при которой злоумышленники реализуют первоначальный доступ в инфраструктуру организации посредством фишинговой рассылки.

Целевым адресатам направляется электронное письмо, содержащее архивный файл 60ZWZ2uhB1LpC2g16uKp3nBZmHomS0keQkan00iJ.zip , внутри которого располагается вредоносный исполняемый файл «Список ко дню России.exe». Подобный подход направлен на эксплуатацию доверия сотрудников и инициирование ручного запуска вредоносного кода.

После активации вредоносного файла происходит операция XOR-дешифрования строк, обеспечивающая расшифровку конфигурационных данных и последующее выполнение кода в системе. На этом этапе реализуется сетевое обращение к внешнему ресурсу https://new[.]systeme-electric[.]tech/news.html, с которого загружается ключ шифрования, необходимый для дальнейших этапов атаки.

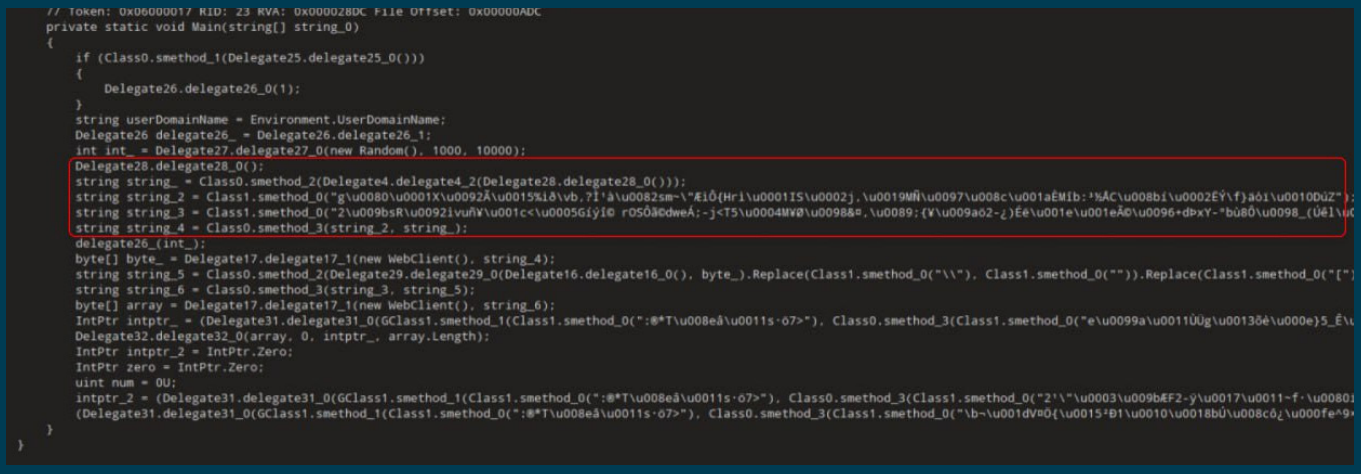


Рисунок 17 - Часть исходного кода, отвечающая за дешифрование строк с помощью пользовательских методов Class0.smethod_2, Class1.smethod_0 и Delegate28, Delegate29

Данный фрагмент иллюстрирует выполнение операции XOR-дешифрования строк перед обращением к внешнему ресурсу для получения ключа шифрования.

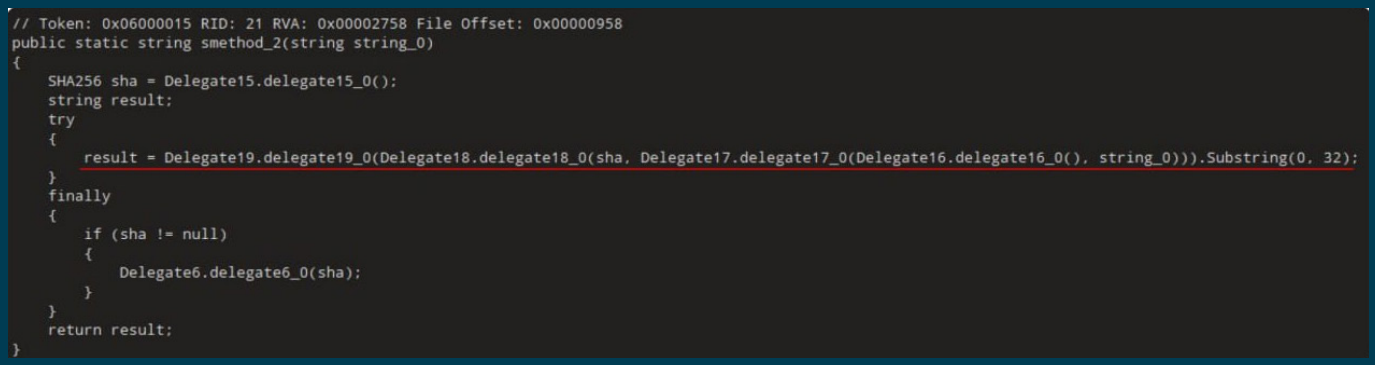


Рисунок 18 - Фрагмент кода, реализующий генерацию ключа шифрования с использованием алгоритма SHA256 и делегатов. Данный элемент задействуется при расшифровке строк и формировании параметров для обращения к внешнему ресурсу злоумышленников

Используя полученные данные и случайно сгенерированное целочисленное значение, вредонос формирует динамический URL-адрес http://lk[.]systeme-electric[.]tech:8080/kukuruza.7z, к которому инициируется подключение для загрузки второй стадии — шеллкода Donut. Присутствие строк WebClient и DownloadData в коде подтверждает активность, связанную с загрузкой дополнительных модулей.

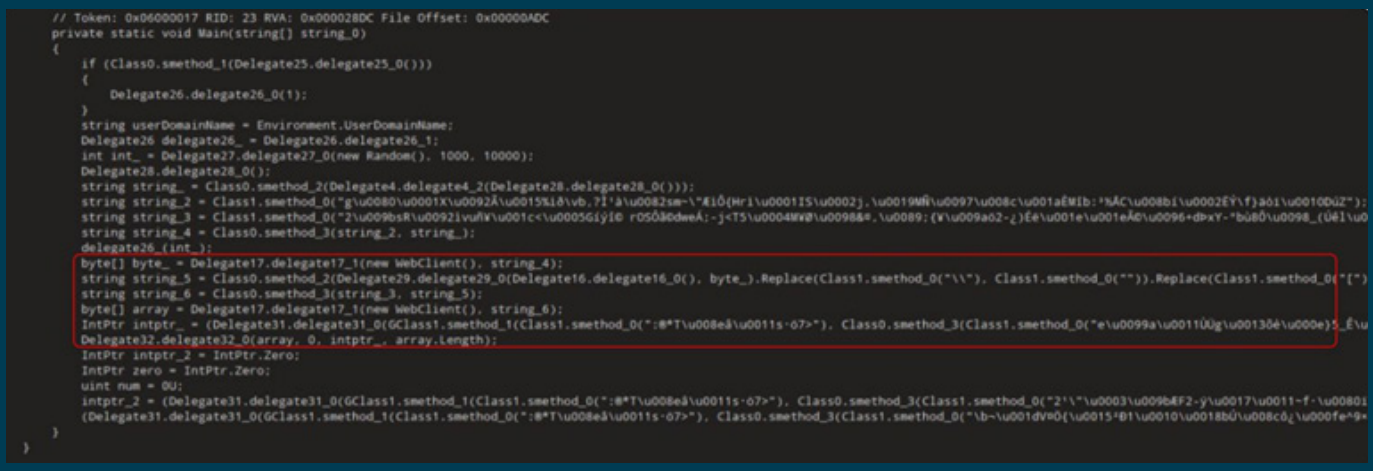


Рисунок 19 - Фрагмент кода, демонстрирующий сетевую активность вредоносного ПО при загрузке второго этапа (шеллкода Donut) с использованием класса WebClient и методов DownloadData

После успешной доставки шеллкод внедряется в легитимные процессы операционной системы с использованием механизма динамического вызова WinAPI через указатели с соглашением вызова stdcall. На следующем этапе из загруженного шеллкода извлекается имплант фреймворка C2 Sliver, который обеспечивает устойчивое присутствие и дальнейшее управление заражённым хостом.

Финальным этапом кампании является установление соединения с C2-сервером злоумышленников для передачи данных и получения управляющих команд. По совокупности признаков активность носит кибершпионский характер. Основными целями атакующей стороны, вероятно, являются эксфильтрация конфиденциальных данных и удалённое администрирование скомпрометированных узлов в интересах дальнейшего разведывательного или саботажного использования.

```
public class GClass0
{
    // Token: 0x02000003 RID: 3
    // (Invoke) Token: 0x06000003 RID: 3
    [UnmanagedFunctionPointer(CallingConvention.StdCall)]
    public delegate IntPtr GDelegate0(uint uint_0, uint uint_1, uint uint_2, uint uint_3);

    // Token: 0x02000004 RID: 4
    // (Invoke) Token: 0x06000007 RID: 7
    [UnmanagedFunctionPointer(CallingConvention.StdCall)]
    public delegate IntPtr GDelegate1(uint uint_0, uint uint_1, IntPtr intptr_0, IntPtr intptr_1, uint uint_2, ref uint uint_3);

    // Token: 0x02000005 RID: 5
    // (Invoke) Token: 0x0600000B RID: 11
    [UnmanagedFunctionPointer(CallingConvention.StdCall)]
    public delegate uint GDelegate2(IntPtr intptr_0, uint uint_0);
}
```

Рисунок 20 - Фрагмент кода, реализующий генерацию ключа шифрования с использованием алгоритма SHA256 и делегатов. Данный элемент задействуется при расшифровке строк и формировании параметров для обращения к внешнему ресурсу злоумышленников

УЯЗВИМОСТИ

Согласно открытым источникам, за неполный 2025 год было зарегистрировано 44 676 уязвимостей.

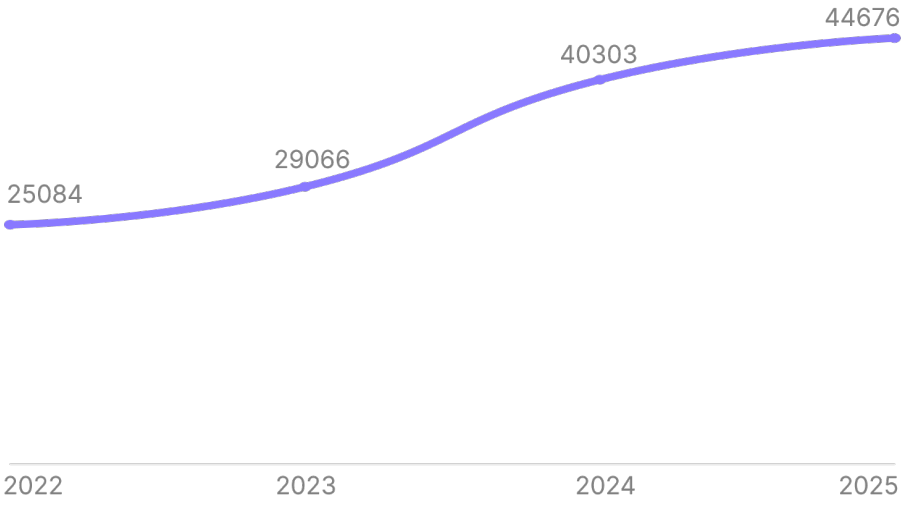


График 1 - Зарегистрированные уязвимости с 2022 по 2025 гг.

Топ-10 вендоров 2025 (по числу CVE) выглядит так:

1. Linux — 4962;
2. Microsoft — 1236;
3. Adobe — 709;
4. Apple — 665;
5. Google — 651;
6. Phpgurukul — 609;
7. IBM — 589;
8. Tenda — 421;
9. Totolink — 330;
10. Fabian — 314.

Сложность киберландшафта растёт: больше компонентов открытого кода, больше связей между ними. При этом рост числа зарегистрированных уязвимостей — это необязательно признак «небезопасного мира», а отражение следующих тенденций:

1. Больше кода и его компонентов теперь мониторится.
2. Больше исследовательской активности и инструментов для поиска уязвимостей.
3. Процессы раскрытия и учёта стали масштабнее.

Также рост может быть обусловлен не только увеличением реального числа уязвимостей, но и расширением круга участников программы CVE Mitre, которые занимаются обнаружением и регистрацией уязвимостей.

Инструменты автоматизации и использование методов на основе ИИ позволяют исследователям и злоумышленникам находить уязвимости быстрее, что также повышает темп публикаций. Стоит отметить и расширение поверхности атаки: больше устройств IoT увеличивает атакуемую область.

Для организаций это означает, что геометрический рост числа уязвимостей требует подхода, ориентированного не просто на реагирование, а на приоритизацию, оценку риска и управление поверхностью атаки.

На отчётный период 2025 года наиболее эксплуатируемыми уязвимостями по данным исследователей АО «ПМ» являются:

1. CVE-2025-55182 (React2Shell) — уязвимость позволяет неаутентифицированному пользователю выполнять произвольный код на уязвимом сервере через отправку предварительно сформированного HTTP-запроса на сервис с React Server Components.
2. CVE-2023-38831 (WinRAR), активно использующаяся для распространения вредоносного ПО.
3. CVE-2025-11001 (7-Zip) связана с неверным определением символических ссылок перед доступом к файлу.
4. CVE-2025-62215 (Windows Kernel Elevation of Privilege Vulnerability) — уязвимость в ядре Windows, которая позволяет повысить права пользователя.
5. CVE-2024-4577 (PHP-CGI RCE на Windows) PHP, режим CGI под Windows. Специально оформленный HTTP-запрос приводит к выполнению произвольных команд на веб-сервере.
6. CVE-2021-34473 (ProxyShell, Exchange) Microsoft Exchange. Удалённое выполнение кода через уязвимый HTTP-эндпоинт. Уязвимость эксплуатируется без пароля, если сервер доступен снаружи.
7. CVE-2021-26084 (Confluence OGNL RCE) Atlassian Confluence. Некорректная обработка OGNL-выражений позволяет неаутентифицированному атакующему выполнить команды на сервере.

ОТРАСЛЕВОЙ ПРОФИЛЬ АТАК В РОССИИ

Киберландшафт России 2024–2025 годов демонстрирует смещение интересов злоумышленников в сторону отраслей с высокой концентрацией персональных данных, финансовых потоков, критичных функций управления и технологических процессов, завязанных на непрерывность. Одновременно второй год растёт число атак через цепочки поставок и подрядчиков, что делает даже защищённые организации уязвимыми через «слабые звенья».

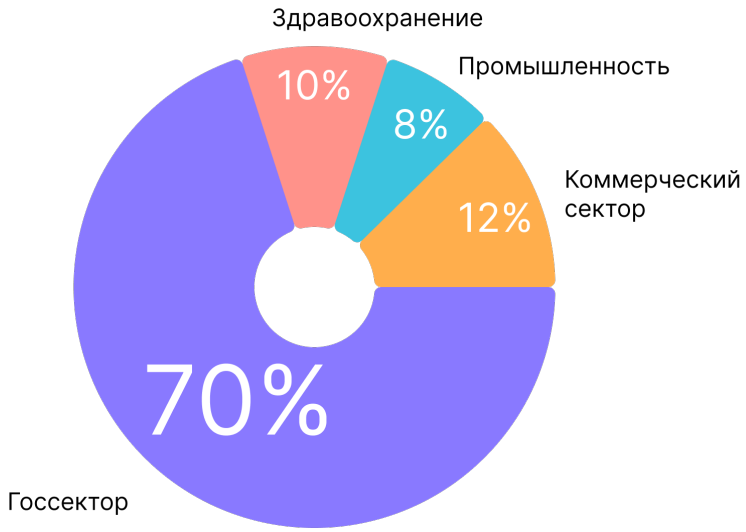


Диаграмма 7 - Статистика по инцидентам за 2024–2025 гг.

Государственные учреждения

Приоритет угроз: очень высокий.

1 Госсектор остаётся центром агрегирования данных о населении, собственности, обращениях граждан, финансовых и юридических действиях.

2 Инциденты в государственных системах приводят к максимальному общественному резонансу, что делает их привлекательными для хактивистов и APT-групп.

3 Система обмена информацией и взаимодействия между различными государственными органами создаёт эффект домино: доступ в одно звено позволяет проникнуть в смежные сервисы.

Какие атаки наиболее вероятны:

- разведка и компрометация цепочек коммуникаций;
- фишинг сотрудников ведомств и операторов реестров;
- эксплуатация уязвимостей;
- атаки на сервисы электронного правительства, региональные платформы.

Ключевая аналитика:

- 2024 и 2025 годы характеризуются ростом атак на подрядчиков госсектора, что превращается в новый основной вектор компрометации;
- переход к импортозамещению повышает нагрузку на ИТ-службы, увеличивая вероятность ошибок при миграциях.

Промышленность

Приоритет угроз: высокий.

Что привлекает злоумышленников:

1 Возможность нанести материальный и операционный ущерб: остановка производства, нарушение логистики, повреждение оборудования.

2 Доступ к внутренним производственным данным, технологиям — важная цель как для криминала, так и для индустриального шпионажа.

3 Широкое использование старых систем OT/АСУ ТП без возможности обновлений.

В 2024–2025 годах фиксируется рост атак с целью «разведки» (T1000–T1600) инфраструктуры — злоумышленники не стремятся сразу ломать, а готовят плацдарм.

Основная проблема — слабая сегментация между офисной IT-сетью и операционной OT-средой.

Всё чаще используются сценарии, где вредонос проникает в IT-сегмент, и через слабые точки — в технологическую сеть.

Финансовый сектор

Приоритет угроз: высокий.

1 Здесь концентрируются прямые деньги, финансовые операции и доступ к платёжным инструментам.

2 Уровень защиты высок, что стимулирует злоумышленников применять социальную инженерию и сложные схемы обмана.

3 Рост фрод-активности в экосистемах маркетплейсов и финтеха повышает общую атакуемость сектора.

Типичные атаки:

- BEC-сценарии, включая deepfake-голоса;
- фишинг под службы банка, мобильный фрод;
- стилеры и захват сессий;
- атаки на API платёжных сервисов.

Количество персонализированных фишинговых атак в 2024–2025 гг. выросло многократно из-за использования ИИ.

Злоумышленники активно тестируют обходы антифрод-систем через дробление транзакций, «цепочки переводов» и атаки через функционал экосистем (кэшбэк, баллы, подписки).

Финорганизации находятся в «золотой середине»: атаки сложные, но уровень зрелости позволяет быстрее реагировать.

Здравоохранение

Приоритет угроз: средний-высокий.

По данным аналитиков АО «ПМ», злоумышленники похитили более 302 миллионов записей за 2025 год.

Рост объёмов цифровых медицинских данных коррелирует с увеличением интенсивности атак на организации здравоохранения. Основной причиной успешных инцидентов остаётся низкая защищённость инфраструктуры. Текущий уровень реализации ИБ-мер в ряде организаций не обеспечивает реальную защиту данных, ограничиваясь выполнением минимально необходимых требований законодательства.

Основными причинами инцидентов остаются распространение вредоносного ПО (ВПО), нарушение политик ИБ и эксплуатация уязвимостей. Данная статистика свидетельствует о критическом влиянии человеческого фактора (пренебрежение правилами цифровой гигиены, подверженность фишингу) в сочетании с техническими рисками, обусловленными использованием устаревшего программного обеспечения и оборудования.

Причины интереса злоумышленников к медицинским данным:

1 Медицинские данные содержат чувствительную и долговечную информацию, которая крайне ценна на теневых рынках.

2 Системы построены на множестве интеграций между частными и государственными клиниками, лабораториями и регистратурами, что расширяет поверхности атаки.

3 В отрасли часто используются устаревшие медицинские информационные системы (далее — МИС) и ПО.

Основные атаки:

1. Компрометация ЕМИАС и региональных медицинских систем;
2. Фишинг сотрудников и врачей (частая точка входа);
3. Утечки реестров пациентов.

Аналитические наблюдения:

1. Медсектор становится одной из лидирующих областей по объёму утечек ПДн.
2. Атаки часто направлены не на деструкцию, а на тихий доступ и кражу баз.
3. Нарушения работы МИС могут иметь прямые последствия для жизни и здоровья пациентов, что увеличивает критичность угроз.

СПЕЦИАЛЬНЫЕ ФОКУСЫ РОССИЙСКОГО КИБЕРЛАНДШАФТА

ДЕТСКАЯ БЕЗОПАСНОСТЬ

Детская безопасность в Интернете — это совокупность мер, политик, технологий и практик, направленных на защиту детей и подростков от вредоносного, незаконного, манипулятивного или психологически опасного контента, а также от киберугроз (включая кибербуллинг, онлайн-эксплуатацию, мошенничество и утечку персональных данных) в цифровой среде.

В рамках российского киберландшафта детская безопасность подразумевает:

- обеспечение безопасного доступа несовершеннолетних к цифровым ресурсам;
- развитие цифровой грамотности и культуры ответственного поведения в сети;
- защиту персональных данных и цифровой идентичности детей;
- соблюдение законодательства РФ в сфере защиты информации и прав несовершеннолетних (в частности, Федерального закона № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и Федерального закона № 152-ФЗ «О персональных данных»);
- участие государства, образовательных учреждений, IT-компаний и родителей в создании безопасной цифровой экосистемы.

Согласно данным УБК МВД России, количество несовершеннолетних, пострадавших от киберпреступлений за девять месяцев 2025 года, возросло на 120% [10].

Основные векторы:

1 Кибербуллинг и травля в сети.

Согласно опросам, проводимых ВЦИОМ, каждый пятый россиянин считает кибербуллинг одной из ключевых угроз для детей в Интернете. Она встает в один ряд с мошенничеством, вовлечением в противозаконную деятельность и распространением непредназначенного для детей контента [11].

2 Онлайн-мошенничество и фишинг — целевые атаки на подростков (социальные сети, игровые платформы) ради денег или персональных данных.

Игровые и «скин»-ловушки (Roblox, Fortnite, Minecraft и пр.) — пользователя заводят на фальшивую «лендинг-страницу», просят ввести логин/пароль, данные платёжной карты или скачать «конвертер/кряк», который содержит ВПО или клавиатурный трекер.

Или же предлагают перейти в бот в Telegram, чтобы в дальнейшем украсть аккаунт.

Киберпреступники активно используют YouTube для распространения мошеннических материалов. Они публикуют видеоролики, рекламирующие бесплатные читы, «взломанные» читы или услуги, которые обещают мгновенное обогащение. В описании видео или в комментариях к нему они оставляют ссылки, по которым зрители могут скачать эти ресурсы.

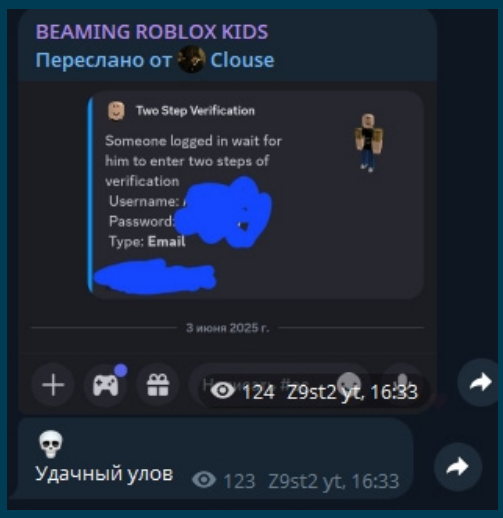


Рисунок 21 - Скриншот
из Телеграм-канала мошенников

10 11

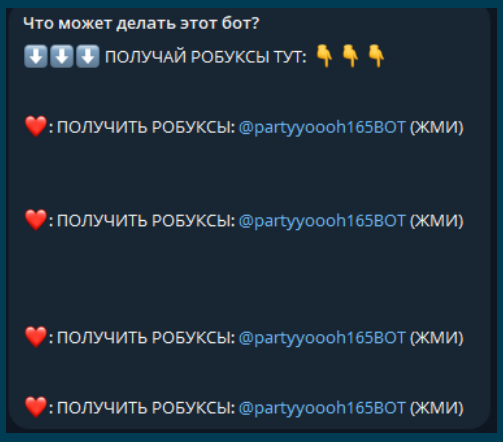


Рисунок 22 - Скриншот
из Телеграм-канала мошенников

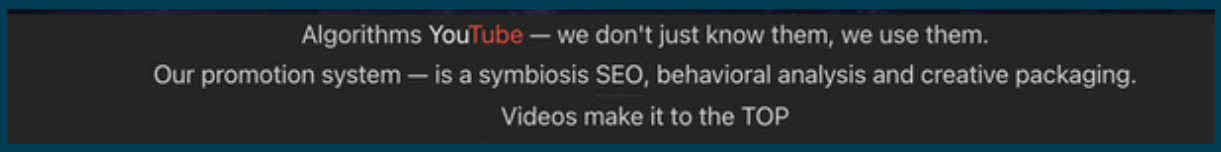


Рисунок 23 - Скриншот с сервиса злоумышленников с заявлением об использовании YouTube

3 Grooming (сексуальная эксплуатация/сближение в сети) — процесс, при котором взрослые эксплуатируют детей, чаще всего в сексуальном плане. Наиболее уязвимые площадки — открытые игровые экосистемы (Roblox, Discord, VRChat), где возможно прямое общение в чате и через голос.

4 Нарушение конфиденциальности персональных данных и риски цифровой идентичности. Проблема защиты данных несовершеннолетних усугубляется отсутствием у них навыков безопасного размещения личной информации (геолокации, биометрии, паролей). К типовым рискам относятся регистрация в сервисах без родительского контроля, а также сбор данных образовательными и игровыми платформами при недостаточном уровне технической защищённости.

К основным рискам и угрозам целесообразно отнести:

1 Разрыв между нормативной базой и практической реализацией. Законодательные механизмы защиты детей в цифровой среде сформированы, однако на региональном уровне часто отсутствуют ресурсы, инструменты мониторинга и контроль исполнения.

2 Низкая вовлечённость взрослых в актуальную повестку кибербезопасности. Наблюдается системный разрыв между техническими возможностями современных сервисов и навыками их безопасного использования со стороны законных представителей и педагогов. Это касается как распознавания попыток фишинга, так и противодействия манипулятивным механикам социальных сетей и игровых платформ. 12

3 Недостаток аналитики и единой статистики. Исследования по регионам остаются фрагментированными, а различия в методиках подсчёта осложняют объективную оценку масштабов угроз и эффективность мер профилактики. 13

12

13

Показатель	Значение	Комментарий
Доля подростков, сталкивающихся с агрессией/кибербуллингом	До 50–60% (разные опросы: 52–59% и выше) 14 15	Высокая распространенность среди подростков от 10-17 лет
Доля подростков, регулярно встречающихся с вредным/опасным контентом	Значительная часть пользователей (по данным отраслевых исследований) 16 17	Отмечается постоянное взаимодействие с контентом, потенциально вредящим психическому и моральному развитию
Объём утечек персональных данных (все группы)	Рост в 2024–2025 гг., включая случаи компрометации детских аккаунтов	Повышается риск утраты цифровой идентичности несовершеннолетних
Наличие правовой базы	Федеральный закон №436-ФЗ (ред. 2023) 18 и сопутствующие акты; программы по цифровой грамотности в реализации	Норма о защите детей от вредной информации действует; в 2024–2025 — активизация программ и методик в школах 19

Таблица 3 - Общие данные по детской безопасности

Детская безопасность в Интернете в российском киберландшафте 2024–2025 годов остаётся приоритетным направлением и требует комплексных мер. Отраслевые исследования и социологические опросы показывают, что значительная часть подростков регулярно сталкивается с агрессией и травлей в сети, а также с контентом, способным нанести вред их развитию. Одновременно фиксируется рост числа утечек персональных данных, что повышает риск компрометации цифровой идентичности несовершеннолетних.

14 15 16 17 18 19

МЕЖДУНАРОДНЫЕ ОТЧЁТЫ О КИБЕРУГРОЗАХ: СОПОСТАВЛЕНИЕ С РОССИЙСКИМ ЛАНДШАФТОМ

Международные профильные организации и ведущие вендоры ежегодно формируют отчёты, отражающие глобальную динамику киберугроз. Наиболее репрезентативными источниками для анализа ландшафта 2024–2025 годов являются ENISA [20], Mandiant [21], Crowdstrike [22], Verizon DBIR [23]

20 21 22 23

Приведённые ниже значения основаны на усреднении и сопоставлении показателей из различных международных отчётов (ENISA Threat Landscape 2025, Verizon DBIR 2024–2025, Mandiant M-Trends, CrowdStrike GTR). Поскольку методики отчётов различаются, данные следует рассматривать как ориентировочные доли зафиксированных инцидентов по основным категориям угроз.

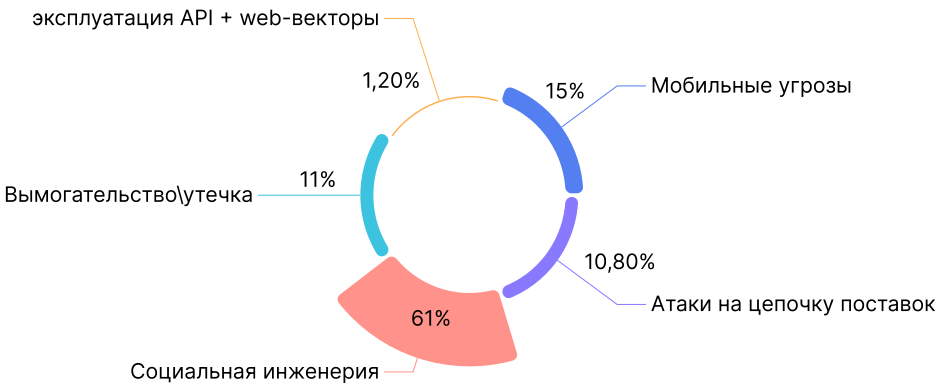


Диаграмма 8 - Основные зафиксированные типы атак в 2024–2025 гг.

1 По совокупным данным ENISA, Mandiant и CrowdStrike, атаки на цепочки поставок становятся одним из основных драйверов роста киберугроз. Данный вектор позволяет противнику масштабировать воздействие, компрометируя сразу десятки и сотни организаций через единый уязвимый компонент.

Наиболее характерные аспекты данного тренда включают:

- смещение атакующих в сторону CI/CD-пайплайнов, репозиториев и инструментов DevOps;
- компрометацию сервисных и аутсорсинговых компаний, оказывающих услуги широкому набору клиентов;
- атаки через сторонние библиотеки и зависимости открытого кода;
- эксплуатацию уязвимостей в корпоративных облаках поставщиков.

В результате атаки на цепочки поставок становятся одним из наиболее разрушительных типов инцидентов с точки зрения масштаба и глубины поражения.

2 Также стоит упомянуть устойчивый рост мобильных атак, особенно на android-устройства. Сегмент мобильных устройств становится отдельной и высокорискованной частью киберландшафта.

3 Международные наблюдения фиксируют изменение парадигмы вымогательских атак. Если ранее доминировало шифрование данных, то сегодня основной фокус смещается на их кражу и последующий шантаж.

Ключевые элементы новой модели:

- повышенная доля «бесшифровых» атак, ориентированных исключительно на кражу данных;
- применение двойного и тройного вымогательства;
- использование публичных площадок (включая Telegram и дарквеб-форумы) для давления на пострадавшие организации;
- снижение временного интервала между первичной компрометацией и этапом выдвижения требований.

Этот тренд снижает эффективность традиционных инструментов защиты от ВПО и увеличивает значимость контроля данных и мониторинга аномалий.

Большинство зафиксированных инцидентов в мире связано с финансовыми мотивами: вымогательством, кражей данных, мошенничеством и продажей доступов. APT составляют 1/4 от серьёзных инцидентов. Хотя финансовые мотивы доминируют, APT и хактивизм активно пересекаются с криминальным миром — инструменты, инфраструктура и техники часто взаимозаменяемы.

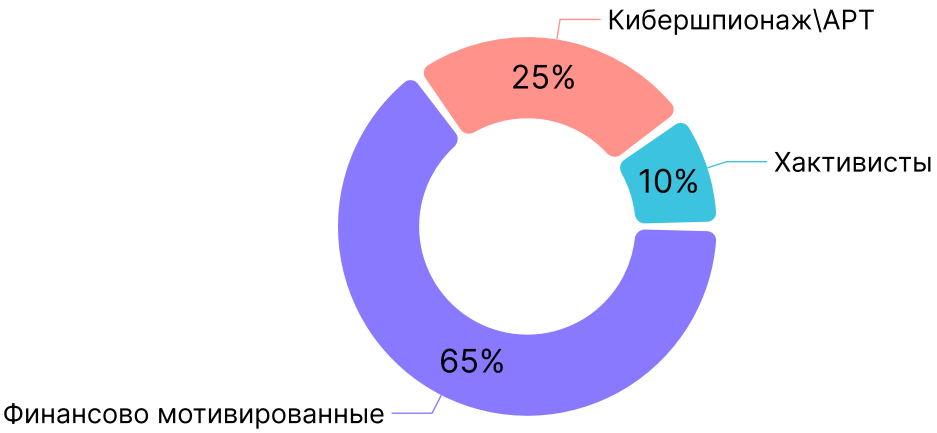


Диаграмма 9 - Акторы атак

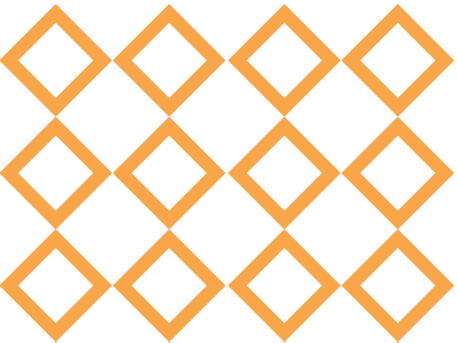
4 APT-группировки остаются одним из ключевых источников высокотехнологичных угроз, при этом их инструментарий и тактика продолжают усложняться. Согласно оценкам Mandiant и CrowdStrike, в 2024–2025 гг. наблюдается:

- рост числа атак с использованием zero-day-уязвимостей, в том числе в продуктах для удалённого доступа;
- активизация атак на облачные платформы, где злоумышленники стремятся закрепиться в сервисных учётных записях и механизмах авторизации;
- распространение техник долговременного скрытого присутствия в облачной среде (cloud persistence);
- расширение прогосударственных кампаний, нацеленных на госорганы, инфраструктуру и крупный бизнес;
- фокус APT-операций смещается от получения единичных данных к глубокому, системному доступу и контролю над инфраструктурой жертвы.

5 Глобальная миграция бизнеса в «облако» привела к значительному росту атак, связанных с нарушениями конфигурации и ошибками управления идентификацией. В отчётах ENISA и DBIR выделяются следующие ключевые проблемы:

- некорректные настройки IAM (Identity and Access Management) и избыточные привилегии сервисных аккаунтов;
- наличие открытых или некорректно настроенных ролевых моделей API-интерфейсов;
- уязвимости, возникающие вследствие автоматизации DevOps (включая ошибки в pipeline-скриптах);
- слабый контроль за межсервисными взаимодействиями.

В результате облачная среда становится привлекательной целью для атакующих, а масштабы последствий инцидентов увеличиваются из-за плотной интеграции сервисов.



6 По данным Verizon DBIR, социальная инженерия остаётся наиболее распространённым механизмом начальной компрометации. В 2024–2025 гг. этот вектор приобрёл новые характеристики:

- персонализированные фишинговые атаки, подготовленные с использованием моделей ИИ;
- переход к использованию нескольких векторов атаки (e-mail — мессенджеры — телефонные звонки);
- значительный рост вишинг-атак с применением дипфейк-голосов;
- использование автоматизированных инструментов для ведения переписки.

Эта комбинация делает социальную инженерию одним из наиболее опасных типов угроз с высокой сложностью обнаружения.

7 VPN-шлюзы, почтовые серверы, VoIP-системы, рокси-устройства и решения для удалённого доступа остаются одними из наиболее уязвимых сегментов. Согласно международным отчётам, статистика демонстрирует:

- постоянную эксплуатацию старых CVE;
- высокий процент компрометации через устройства с неустановленными обновлениями;
- использование доступа к периферийным устройствам как отправной точке для дальнейшего скрытого продвижения внутри корпоративной сети.

Вектор угроз смещается от классического вредоносного ПО к более гибким, малозаметным и модульным инструментам. Тем не менее, есть несколько классов ВПО, которые доминируют в реальных атаках:

1. стилеры (Racoon, Lumma, MetaStealer);
2. RAT (PlugX, AsyncRat, Quasar);
3. загрузчики и дропперы (Latrodectus, GootLoader, SmoleLoader);
4. бэкдоры (Cobalt Strike Beacon, Brute Ratel C4);
5. вымогательское ПО / шифовальщики (Ransomware) и инструменты эксфильтрации (LockBit, BlackCat/ALPHV).

Общий вывод:

Российский киберландшафт движется в одном направлении с мировыми трендами, но испытывает их в более концентрированной и острой форме, что делает его более динамичным.

Это связано со следующими тенденциями:

1. Высокая геополитическая нагрузка.
2. После ухода иностранных вендоров из России часть компаний продолжает использовать зарубежные решения.
3. Повышенная чувствительность к атакам на КИИ.

Россия полностью разделяет следующие глобальные тренды: атаки через цепочки поставок, кража данных с последующим вымогательством, действия продвинутых хакерских групп, угрозы в облаках и схемы социальной инженерии.

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ И ПРАВОВЫЕ НОРМЫ

В 2025 году в России произошло несколько значимых законодательных нововведений в сфере информационной безопасности и противодействия киберпреступности, которые усиливают контроль и ответственность, но при этом создают и новые условия, к которым злоумышленникам приходится адаптироваться.

Наименование	Краткое содержание	Комментарий
Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» 24	Создание государственной системы для регистрации, анализа и противодействия ИКТ-преступлениям	Централизация данных об инцидентах, повышение скорости обмена информацией, улучшение координации расследований и мониторинга
Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» 25	Ввод минимальных требований к аппаратным средствам, ПО, их происхождению, обновляемости	Повышение уровня защищённости инфраструктуры, рост нагрузки на компании по обеспечению сертификации, ограничение использования «серого» оборудования

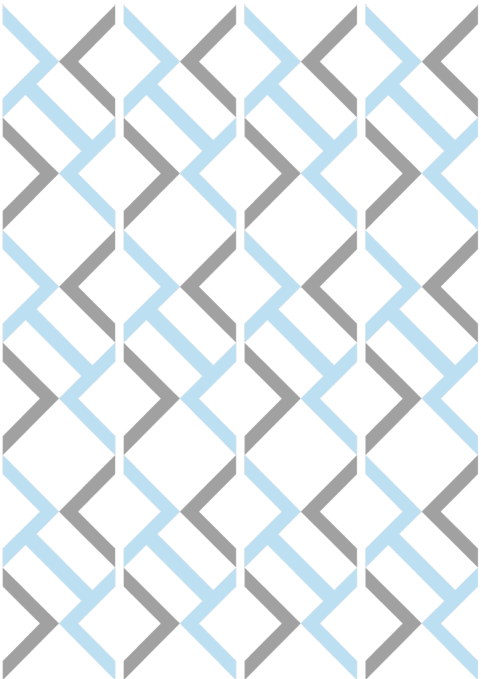
Таблица 4 - Законодательство в области обеспечения информационной безопасности

24

25

Наименование	Краткое содержание	Комментарий
Федеральный закон от 31.07.2025 № 325-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» 26	Вводит понятие «значимый разработчик» российского ПО для поддержки импортозамещения и реализации особо значимых проектов.	Повышение зрелости разработки, снижение числа уязвимостей на стадии поставки, усиление поставки цепочки ПО
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Уточнены требования к трансграничной передаче данных, введены новые обязанности операторов – уведомление о рисках, усиление мер защиты, расширение полномочий мер защиты, расширение полномочий Роскомнадзора, новые требования к категорированию и локализации, обязательное уведомление об инцидентах ИБ	Усиление контроля за обработкой ПДн, рост требований к защищенности систем, повышенные санкции\штрафы за утечки информации, компании вынуждены улучшать ИБ-процессы.
Федеральный закон от 31 июля 2025 г. № 281-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях и Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» 27	Новые правила для SIM-карт: ограничено 20 номеров на физическое лицо, запрещена передача SIM-карт третьим лицам под штраф до 50 000 руб. (с исключениями для родственников), а операторы обязаны проверять данные и блокировать «лишние» номера, чтобы бороться с мошенничеством	

Таблица 4 - Законодательство в области обеспечения информационной безопасности



26

27

ПРОГНОЗ НА 2026 ГОД

2026 году киберландшафт продолжит стремительно усложняться в связи с ростом генеративного ИИ, усилением атак на цепочки поставок и расширением угроз для КИИ. Компании столкнутся с переходом отрасли к новым стандартам безопасности:

1. Архитектура Zero Trust станет фактически обязательной.
2. Киберстрахование будет ключевым механизмом управления рисками.
3. Преступные группировки будут активно использовать ИИ для автоматизации атак и повышения точности социальной инженерии.
4. Усиление регуляторных требований, персонализация атак на сотрудников, а также рост теневой «киберэкономики» создадут дополнительное давление на бизнес.
5. Социально уязвимые слои населения в 2026 году останутся одной из главных целей кибермошенников из-за сочетания ограниченной цифровой грамотности и зависимости от онлайн-сервисов. Такие группы чаще становятся жертвами финансовых схем, мошенничества в сфере социальных выплат и поддельных сервисов поддержки.

В совокупности это делает 2026 год временем, когда устойчивость организаций будет определяться уровнем их цифровой зрелости, скоростью адаптации и реакции на инциденты, а также способностью внедрять защитные технологии нового поколения.

ИСТОЧНИКИ

1. https://rt-solar.ru/analytics/reports/6170/
2. https://www.anti-malware.ru/products/stormwall
3. https://softline.ru/about/blog/importozameshchenie-v-2025-godu#:~:text=%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%83%20%D0%B2%20%D0%BE%D0%B1%D0%BB%D0%B0%D0%BA%D0%B5.-,%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C,%D0%B7%D1%80%D0%B5%D0%BB%D1%8B%D1%85%20%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B9%20%D0%B4%D0%BB%D1%8F%20%D0%B2%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D0%BD%D0%B0%D0%B3%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%BD%D1%8B%D1%85%20%D1%81%D1%80%D0%B5%D0%B4.&text=Infosecurity:%20%D0%BB%D0%B8%D0%B4%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D0%B9%20%D0%B8%D0%B3%D1%80%D0%BE%D0%BA%20%D0%B2%20%D1%81%D1%84%D0%B5%D1%80%D0%B5,DLP%2D%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%B8%20%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5%20%D1%81%D0%BE%D1%82%D1%80%D1%83%D0%B4%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2.
4. https://amonitoring.ru/service_aml_web_protection/
5. https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html
6. https://cisoclub.ru/sotrudnichestvo-apt-premier-pass-as-a-service-i-posrednik-dostupa/
7. https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-2025-cyber-risk-report
8. https://www.gazeta.ru/tech/news/2025/10/16/26964326.shtml
9. https://www.f6.ru/blog/android-deliveryrat-research/
10. https://t.me/cyberpolice_rus/4249
11. ttps://wciom.ru/analytical-reviews/analiticheskii-obzor/travlja-v-cifrovuju-ehpokhu
12. https://wciom.ru/analytical-reviews/analiticheskii-obzor/travlja-v-cifrovuju-ehpokhu
13. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B4%D0%B5%D1%82%D0%B5%D0%B9_%D0%B2_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5
14. https://www.comnews.ru/content/242148/2025-11-01/2025-w44/1010/pochti-tret-molodykh-rossiyan-proyavlyayut-agressiyu-seti
15. https://rg.ru/2025/11/05/pravila-obshcheniia.html
16. https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_analiticheskiy_otchet_2024
17. https://www.vyatsu.ru/internet-gazeta/uchenyie-sozdali-reyting-ugroz-s-kotoryimi-stalkiv.html
18. https://www.consultant.ru/document/cons_doc_LAW_108808/
19. https://www.scli.ru/upload/docs/obuchenie/4/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D0%9A%D0%9F%D0%9A_%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BD%D0%B5%D1%81%D0%BE%D0%B2%D0%B5%D1%80%D1%88%D0%B5%D0%BD%D0%BD%D0%BE%D0%BB%D0%B5%D1%82%D0%BD%D0%B8%D1%85_2025.pdf
20. https://www.iisf.ie/files/UserFiles/Documents/2025/ENISA-Threat-Landscape-2025_0.pdf
21. https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
22. https://www.crowdstrike.com/en-us/global-threat-report/
23. https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
24. https://www.consultant.ru/document/cons_doc_LAW_502182/
25. https://www.consultant.ru/document/cons_doc_LAW_502581/
26. https://www.consultant.ru/document/cons_doc_LAW_511130/
27. https://www.garant.ru/news/1850123/