|  |  |  |
| --- | --- | --- |
|  |  | |
| [ТМ] НПО ПОИСК | Июль 2025 |

# Основные результаты мониторинга

В результате мониторинга событий информационной безопасности  
и управления уязвимостями (далее – SOC-центр) подключены следующие источники событий информационной безопасности инфраструктуры предприятия (далее – источники):

* Журналы событий безопасности операционной системы **Windows**  
  на конечных узлах (автоматизированных рабочих местах и серверах);
* центр управления антивирусной защиты **Kaspersky Security Center**;
* журналы событий межсетевого экрана **UserGate;**
* журналы событий активного сетевого оборудования.

В период 01.07.2025 - 31.07.2025 на подключенных источниках зафиксировано:

* 530572078 событий информационной безопасности;
* 111 алертов;
* **{типы}** типов алертов.

Рисунок 1 – Категорирование инцидентов по типам\*

\* Сводное описание типов, согласно классификации MITRE ATT&CK:

|  |
| --- |
| Разведка (Reconnaissance, TA0043) - попытки сбора информации |
| которая может быть использована для атак; |
| Подготовка ресурсов (Resource Development, TA0042) - попытки получения |
| злоумышленником ресурсов, с которых может быть проведена атака; |
| Первоначальный доступ (Initial Access, TA0001) - попытки проникновения в сеть; |
| Выполнение (Execution, TA0002) - попытки запуска вредоносного кода; |
| Закрепление (Persistence, TA0003) - попытки злоумышленника сохранить присутствие |
| в системе; |
| Повышение привилегий (Privilege Escalation, TA0004) - попытки злоумышленника |
| получить права более высокого уровня |
| Предотвращение обнаружения (Defence Evasion, TA0005) - методы, позволяющие |
| злоумышленнику избежать обнаружения в скомпрометированной системе; |
| Получение учетных данных (Credential Access, TA0006) - методы получения легитимных |
| учетных данных, либо их кражи с целью получения доступа к системам; |
| Обнаружение (Discovery, TA0007) - методы для получения сведений о системе или сети; |
| Перемещение (Lateral Movement, TA0008) - методы, используемые для входа и управления |
| удаленными системами, расположенными в сети предприятия; |
| Сбор данных (Collection, TA0009) - методы сбора информации, интересующей |
| злоумышленника; |
| Организация управления (Command and Control, TA0011) - методы установления контроля |
| и управление атакуемыми системами; |
| Эксфильтрация (Exfiltration, TA0010) - методы кражи данных; |
| Деструктивноое воздействие (Impact, TA0040) - методы, используемые для нарушения |
| доступности или целостности данных |

В рамках 111 алертов затронуто 49 источников.

Таблица 1. Имена затронутых источников

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя** | **№** | **Имя** | **№** | **Имя** | **№** | **Имя** |
| 1 | KSC | 2 | PSK-10-26 | 3 | PSK-23-02 | 4 | PSK-30-14 |
| 5 | PSK-30-18 | 6 | PSK-58-03 | 7 | SHARE | 8 | 00-W10 |
| 9 | BDC | 10 | MAIL | 11 | PDC | 12 | PSK-04-06 |
| 13 | PSK-05-18 | 14 | PSK-06-11 | 15 | PSK-09-00 | 16 | PSK-09-03 |
| 17 | PSK-09-TH | 18 | PSK-10-33 | 19 | PSK-12-10 | 20 | PSK-21-02 |
| 21 | PSK-30-03 | 22 | PSK-30-04 | 23 | PSK-30-37 | 24 | PSK-32-65 |
| 25 | PSK-32-74 | 26 | PSK-33-07 | 27 | PSK-33-08 | 28 | PSK-37-13 |
| 29 | PSK-41-13 | 30 | PSK-41-14 | 31 | PSK-41-15 | 32 | PSK-41-16 |
| 33 | PSK-42-01 | 34 | PSK-46-19 | 35 | PSK-51-12 | 36 | PSK-58-01 |
| 37 | PSK-58-07 | 38 | SECRETAR-GD | 39 | SQL | 40 | SQL-DEV |
| 41 | SQL2 | 42 | SRV-EVENT | 43 | SRV-NANOCAD-LIC | 44 | SRV-TERM-GTW |
| 45 | SRV-TERM-MSC | 46 | TS1 | 47 | TS2 | 48 | TS3 |
| 49 | bkp |  |  |  |  |  |  |

# Тактики и техники MITRE ATT&CK

Таблица 2. Тактики и техники

| **Тактика** | **Техника** |
| --- | --- |
| Неизвестная тактика | R077\_08\_KSC. Вредоносный объект обнаружен и не был вылечен |
| Повышение привилегий | R003\_Удаленный вход под учетной записью локального администратора |
| Выполнение | R089\_Обнаружены возможные следы действий программ-вымогателей |
| Повышение привилегий | R152\_Запущенный процесс имеет подозрительный родительский процесс |
| Выполнение | R080\_Всплеск заражений ВПО |
| Закрепление | R051\_Учетная запись была добавлена в группу подозрительным пользователем |
| Предотвращение обнаружения | R302\_Манипуляции с атрибутами файла+FilePath |
| Закрепление | R058\_Локальная учетная запись была создана подозрительным пользователем |
| Выполнение | R079\_Несколько хостов заражены одним типом вируса |
| Неизвестная тактика | R302\_04\_Изменение разрешений папки/файла |
| Закрепление | R055\_Изменение группы в ОС Windows подозрительным пользователем |
| Закрепление | R052\_Учетная запись была удалена из группы подозрительным пользователем |
| Организация управления | R083\_Обнаружены следы использования нежелательных утилит |
| Закрепление | R053\_Создание группы на Windows системе подозрительным пользователем |
| Закрепление | R059\_Большое количество манипуляций с учетными записями за короткий промежуток времени |
| Первоначальный доступ | R351\_Подозрение на фишинг при создании подозрительного файла |
| Закрепление | R060\_Большое количество манипуляций с группами за короткий промежуток времени |
| Организация управления | R205\_Обнаружен новый DNS сервер |
| Выполнение | R296\_Подозрительные аргументы при запуске системной утилиты |
| Получение учетных данных | R035\_Возможный подбор пароля методом перебора учетных записей |
| Предотвращение обнаружения | R050\_Очистка журнала событий Windows |
| Неизвестная тактика | Отключение правила на 1 час |
| Выполнение | R078\_Обнаружено большое количество вредоносных объектов на одном хосте |
| Сбор данных | R407\_Обнаружение следов возможного перехвата вводимых данных |

Подробная информация по событиями и инцидентам, собранная  
за отчетную и предыдущие даты, представлена в соответствующем разделе  
вашего Личного кабинета «Отчеты\Сформированные отчеты».

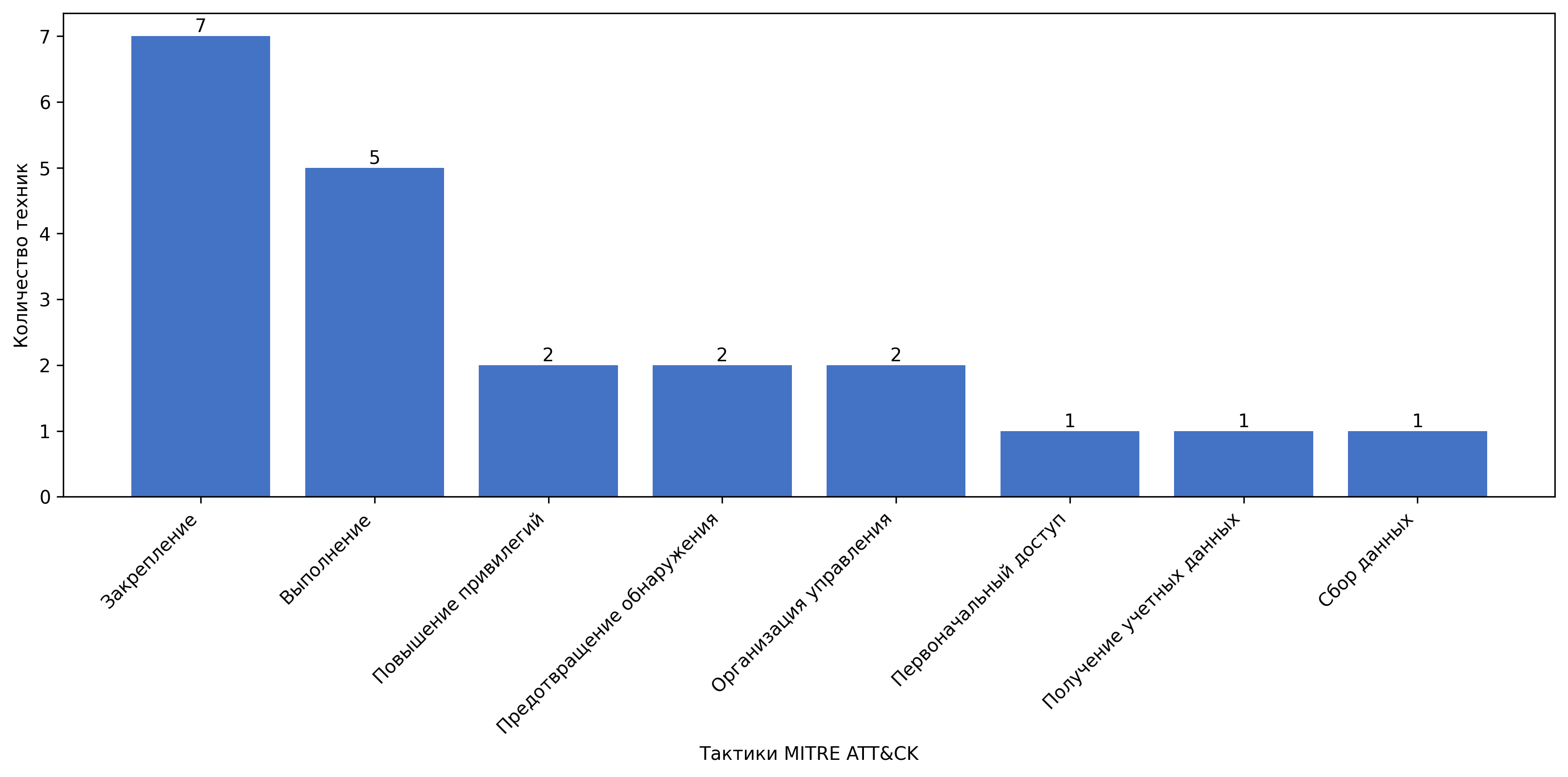


Рисунок 1. Распределение техник по тактикам MITRE ATT&CK