|  |  |  |
| --- | --- | --- |
|  |  | |
| [ТД] КУЛЗ | 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:

* 36926316 событий информационной безопасности;
* 94 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 94 алертов затронуто 1 источников.

Таблица 1. Имена затронутых источников

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя** | **№** | **Имя** | **№** | **Имя** | **№** | **Имя** |
| 1 | OTD89-1520220 |  |  |  |  |  |  |

# Тактики и техники MITRE ATT&CK

Таблица 2. Тактики и техники

| **Тактика** | **Техника** |
| --- | --- |
| Обнаружение | R220\_Сбор информации об учетных записях |
| Обнаружение | R221\_Сбор информации о группах |
| Закрепление | R062\_Действия над группой из командной строки |
| Повышение привилегий | R003\_Удаленный вход под учетной записью локального администратора |
| Выполнение | R089\_Обнаружены возможные следы действий программ-вымогателей |
| Выполнение | R109\_Использование известных зловредных фреймворков для эксплуатации уязвимостей |
| Выполнение | R110\_Использование подозрительных опций в командах PowerShell |
| Обнаружение | R229\_Сбор информации о службах |
| Неизвестная тактика | R093\_37\_Манипуляции с корневым сертификатом через реестр Windows |
| Предотвращение обнаружения | R093\_Изменение критичных веток реестра |
| Выполнение | R105\_Подозрение на обфускацию кода с использованием спецсимволов+S.ScriptBlockText |
| Первоначальный доступ | R431\_Подозрительная активность подключаемых устройств |
| Получение учетных данных | R035\_Возможный подбор пароля методом перебора учетных записей |
| Закрепление | R059\_Большое количество манипуляций с учетными записями за короткий промежуток времени |
| Обнаружение | R224\_Сбор информации о системе |
| Выполнение | R350\_Подозрительная активность приложения MS Office |
| Выполнение | R107\_Использование сжатия данных |
| Неизвестная тактика | Отключение правила на 1 час |
| Выполнение | R296\_Подозрительные аргументы при запуске системной утилиты |
| Предотвращение обнаружения | R294\_Обфускация команд PowerShell |
| Предотвращение обнаружения | R106\_Подозрительные PowerShell команды. Подозрение на кодирование команд |

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

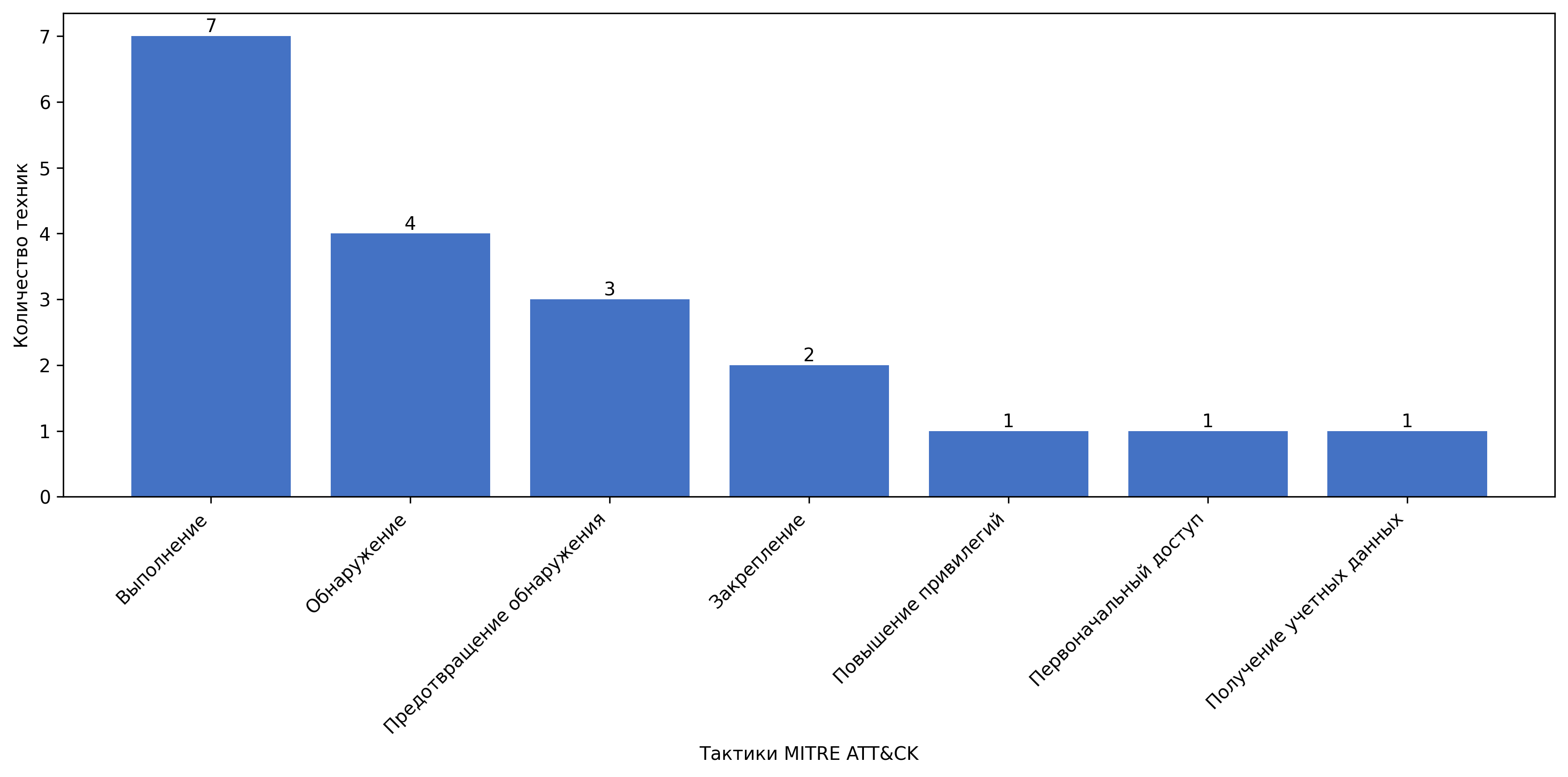


Рисунок 1. Распределение техник по тактикам MITRE ATT&CK