|  |  |  |
| --- | --- | --- |
|  |  | |
| [ТМ] Позис | Август 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 - 01.08.2025 на подключенных источниках зафиксировано:

* 90667077 событий информационной безопасности;
* 136 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 136 алертов затронуто 5 источников.

Таблица 1. Имена затронутых источников

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя** | **№** | **Имя** | **№** | **Имя** | **№** | **Имя** |
| 1 | BPK-2 | 2 | CEO-NACH | 3 | KP-TORG-2 | 4 | REJM-2 |
| 5 | UPMIPK-5 |  |  |  |  |  |  |

# Тактики и техники MITRE ATT&CK

Таблица 2. Тактики и техники

| **Тактика** | **Техника** |
| --- | --- |
| Организация управления | R084\_Использование ПО для удаленного администрирования |
| Перемещение | R071\_Получен доступ к ADMIN$ |
| Закрепление | R051\_Учетная запись была добавлена в группу подозрительным пользователем |
| Закрепление | R055\_Изменение группы в ОС Windows подозрительным пользователем |
| Выполнение | R080\_Всплеск заражений ВПО |
| Выполнение | R079\_Несколько хостов заражены одним типом вируса |
| Неизвестная тактика | R077\_07\_KSC. Вредоносный объект обнаружен и был вылечен |
| Выполнение | R290\_Запуск скриптов из общедоступной директории |
| Выполнение | R061\_Действия над учетной записью |
| Обнаружение | R224\_Сбор информации о системе |
| Выполнение | R003\_Удаленный вход под учетной записью локального администратора |
| Получение учетных данных | R035\_Возможный подбор пароля методом перебора учетных записей |
| Выполнение | R296\_Подозрительные аргументы при запуске системной утилиты |
| Неизвестная тактика | Отключение правила на 1 час |
| Повышение привилегий | R087\_Подозрение на внедрение в процесс |
| Сбор данных | R407\_Обнаружение следов возможного перехвата вводимых данных |
| Закрепление | R060\_Большое количество манипуляций с группами за короткий промежуток времени |
| Выполнение | R078\_Обнаружено большое количество вредоносных объектов на одном хосте |
| Закрепление | R053\_Создание группы на Windows системе подозрительным пользователем |
| Закрепление | R410\_Подписка на события WMI |

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

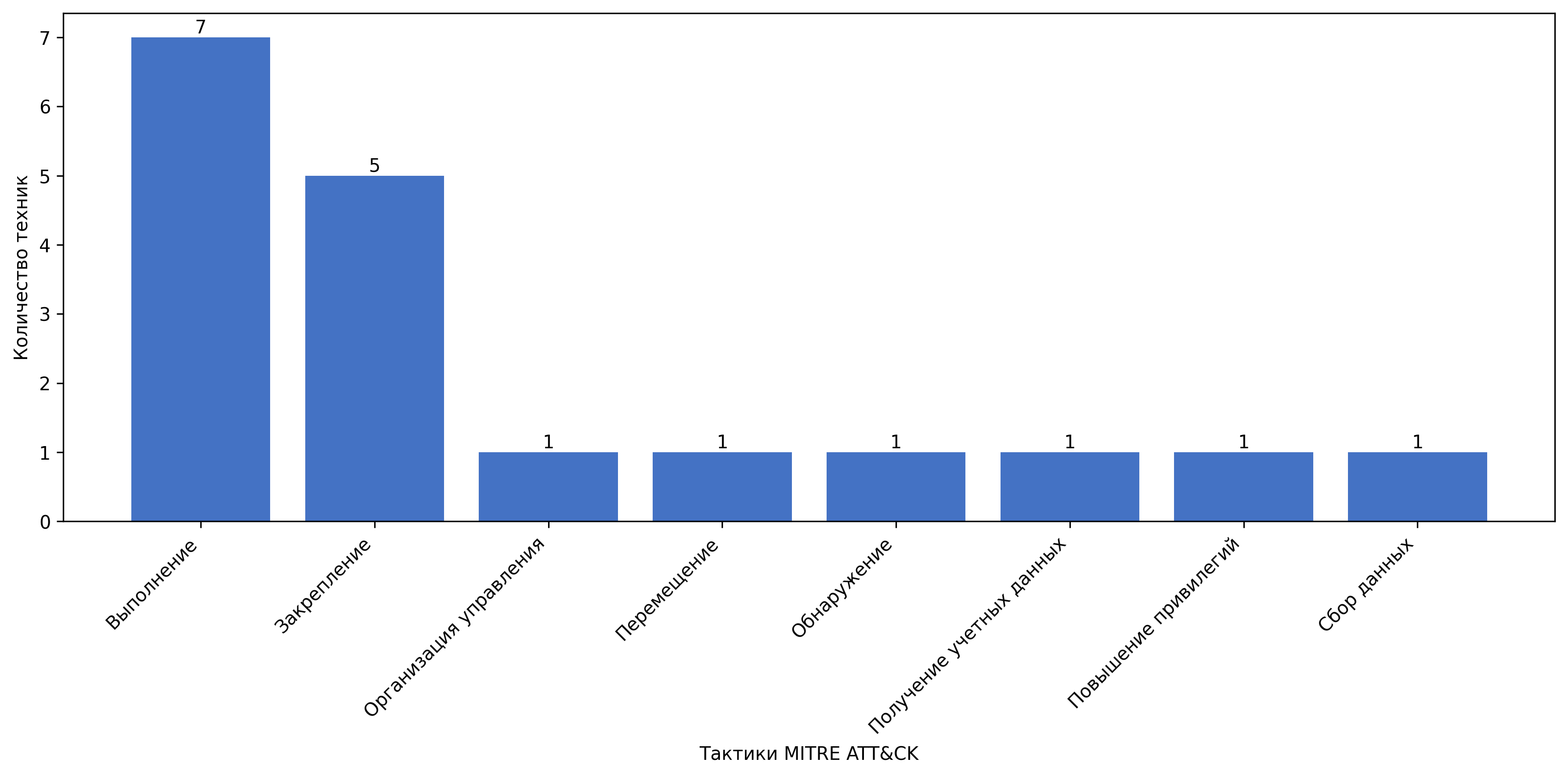


Рисунок 1. Распределение техник по тактикам MITRE ATT&CK