|  |  |  |
| --- | --- | --- |
|  |  | |
| [ТД] Гидравлика | 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 01.08.2025 - 31.08.2025 на подключенных источниках зафиксировано:

* 1340145538 событий информационной безопасности;
* 226 алертов;
* **{типы}** типов алертов.

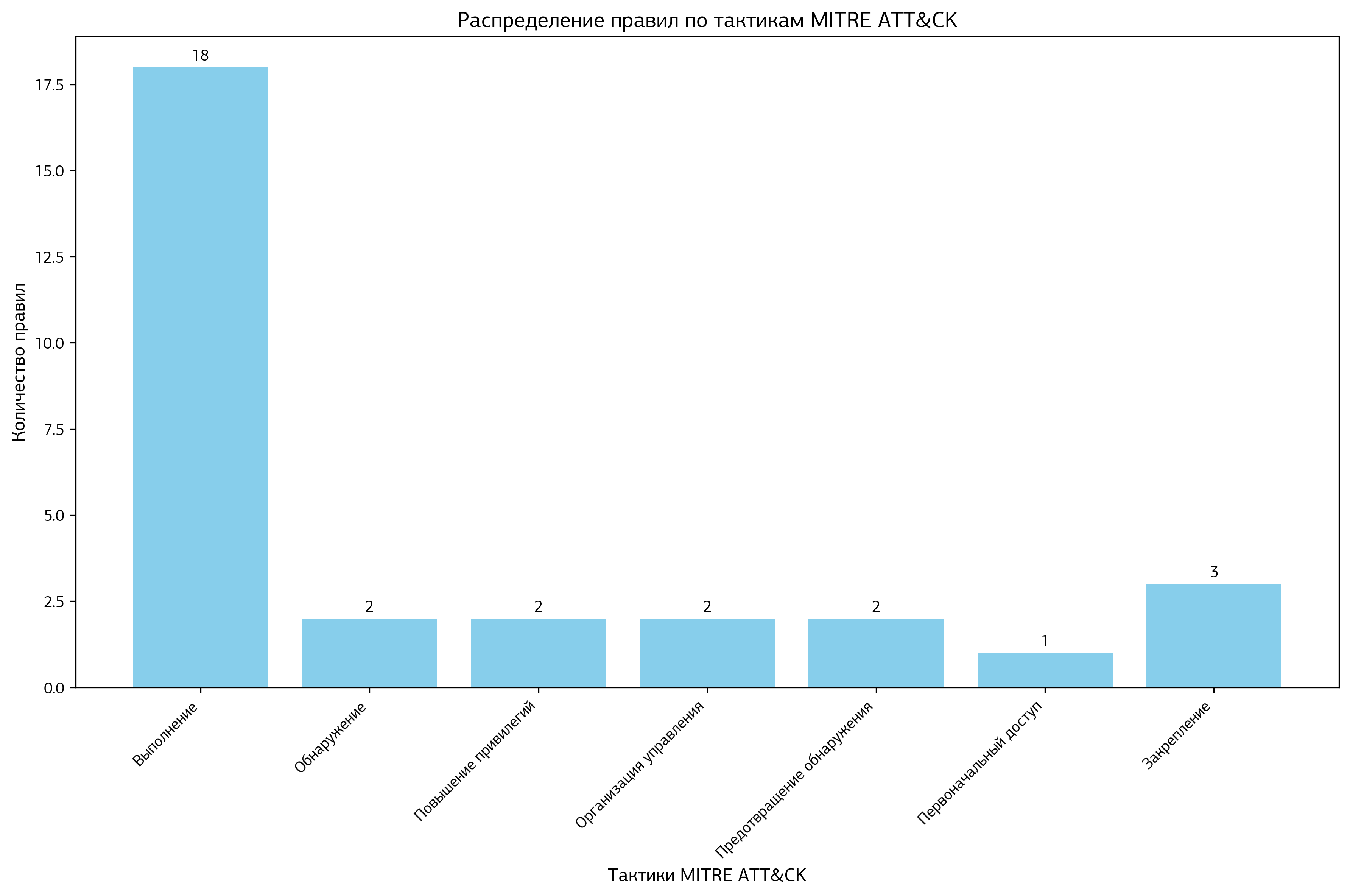


Рисунок 1 Распределение алертов по тактикам MITRE

\* 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 226 алертов затронуто 33 источников.

Таблица 1. Имена затронутых источников

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя** | **№** | **Имя** | **№** | **Имя** | **№** | **Имя** |
| 1 | SERV-BUH | 2 | CEX4-I21156 | 3 | CEX4K-I24549 | 4 | ERO-I23496 |
| 5 | SERV-1CDB2 | 6 | SERV-TFLEX | 7 | BKI-M5 | 8 | CEX10A-I24482 |
| 9 | CEX2-I1131756 | 10 | CEX4D-I22148 | 11 | CEX4D-I23299 | 12 | CEX4K-I22182 |
| 13 | CMS-I22739 | 14 | DC1 | 15 | DC2 | 16 | DC3 |
| 17 | MAIL | 18 | OEA-ITD68 | 19 | OGS-I23326 | 20 | OIIN-I23893 |
| 21 | OIT-I22847 | 22 | OIT-I24410 | 23 | OIT-I24510~~300318 | 24 | OIT-M11862 |
| 25 | OKB-I23649 | 26 | OKB-I24670 | 27 | OKB-TD26 | 28 | OOTIZ-I23619 |
| 29 | OTK-I23963 | 30 | PDO-I23325 | 31 | PROFCOM-I23739 | 32 | RSO-I24211 |
| 33 | SERV-SPRUT |  |  |  |  |  |  |

# Тактики и техники MITRE ATT&CK

Таблица 2. Тактики и техники

| **Тактика** | **Техника** |
| --- | --- |
| Выполнение | R226\_Сбор информации о сетевых подключениях |
| Выполнение | R089\_Обнаружены возможные следы действий программ-вымогателей |
| Выполнение | R110\_Использование подозрительных опций в командах PowerShell |
| Обнаружение | R224\_Сбор информации о системе |
| Повышение привилегий | R087\_Подозрение на внедрение в процесс |
| Выполнение | R109\_Использование известных зловредных фреймворков для эксплуатации уязвимостей |
| Выполнение | R111\_Размонтирование сетевых ресурсов |
| Организация управления | R084\_Использование ПО для удаленного администрирования |
| Предотвращение обнаружения | R302\_07\_Модификация атрибутов времени файла с помощью PowerShell+FilePath |
| Повышение привилегий | R302\_Манипуляции с атрибутами файла+FilePath |
| Первоначальный доступ | R003\_Удаленный вход под учетной записью локального администратора |
| Выполнение | R288\_Манипуляции с файлами, имеющими нестандартные расширения |
| Закрепление | R410\_Подписка на события WMI |
| Организация управления | R205\_Обнаружен новый DNS сервер |
| Обнаружение | R223\_Сбор информации о процессах |
| Выполнение | R296\_Подозрительные аргументы при запуске системной утилиты |
| Выполнение | R280\_Изменение параметров сервиса Windows |
| Выполнение | R295\_Манипуляции с системой непривилегированным процессом |
| Выполнение | R282\_Остановка сервиса через CLI |
| Выполнение | R152\_Запущенный процесс имеет подозрительный родительский процесс |
| Выполнение | R290\_Запуск скриптов из общедоступной директории |
| Выполнение | R099\_Манипуляции с задачами по расписанию |
| Закрепление | R059\_Большое количество манипуляций с учетными записями за короткий промежуток времени |
| Выполнение | R080\_Всплеск заражений ВПО |
| Выполнение | R077\_08\_KSC. Вредоносный объект обнаружен и не был вылечен |
| Выполнение | R077\_07\_KSC. Вредоносный объект обнаружен и был вылечен |
| Выполнение | R291\_Вызов внешних ресурсов для системных приложений Windows |
| Закрепление | R058\_Локальная учетная запись была создана подозрительным пользователем |
| Выполнение | R063\_Добавление учетной записи в группу доменных или локальных администраторов |
| Предотвращение обнаружения | R150\_Манипуляции с именами системных утилит |

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