# Оценка покрытия матрицы MITRE ATT&CK

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Статья онлайн-справки «Покрытие матрицы MITRE ATT&CK»:
> https://support.kaspersky.ru/kuma/4.0/272743

Если вы хотите оценить покрытие матрицы MITRE ATT&CK (https://attack.mitre.org/) корреляционными правилами, используемыми в KUMA («коробочными» и/или пользовательскими), выполните следующие шаги:

- Загрузите справочник техник MITRE из официального репозитория MITRE ATT&CK и импортируйте справочник техник MITRE в KUMA.
- Привяжите техники MITRE к правилам корреляции.
- Экспортируйте правила корреляции в MITRE ATT&CK Navigator.
- В результате вы сможете визуально оценить покрытие матрицы MITRE ATT&CK.

Загрузить справочник техник MITRE можно из официального репозитория MITRE ATT&CK:
https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json

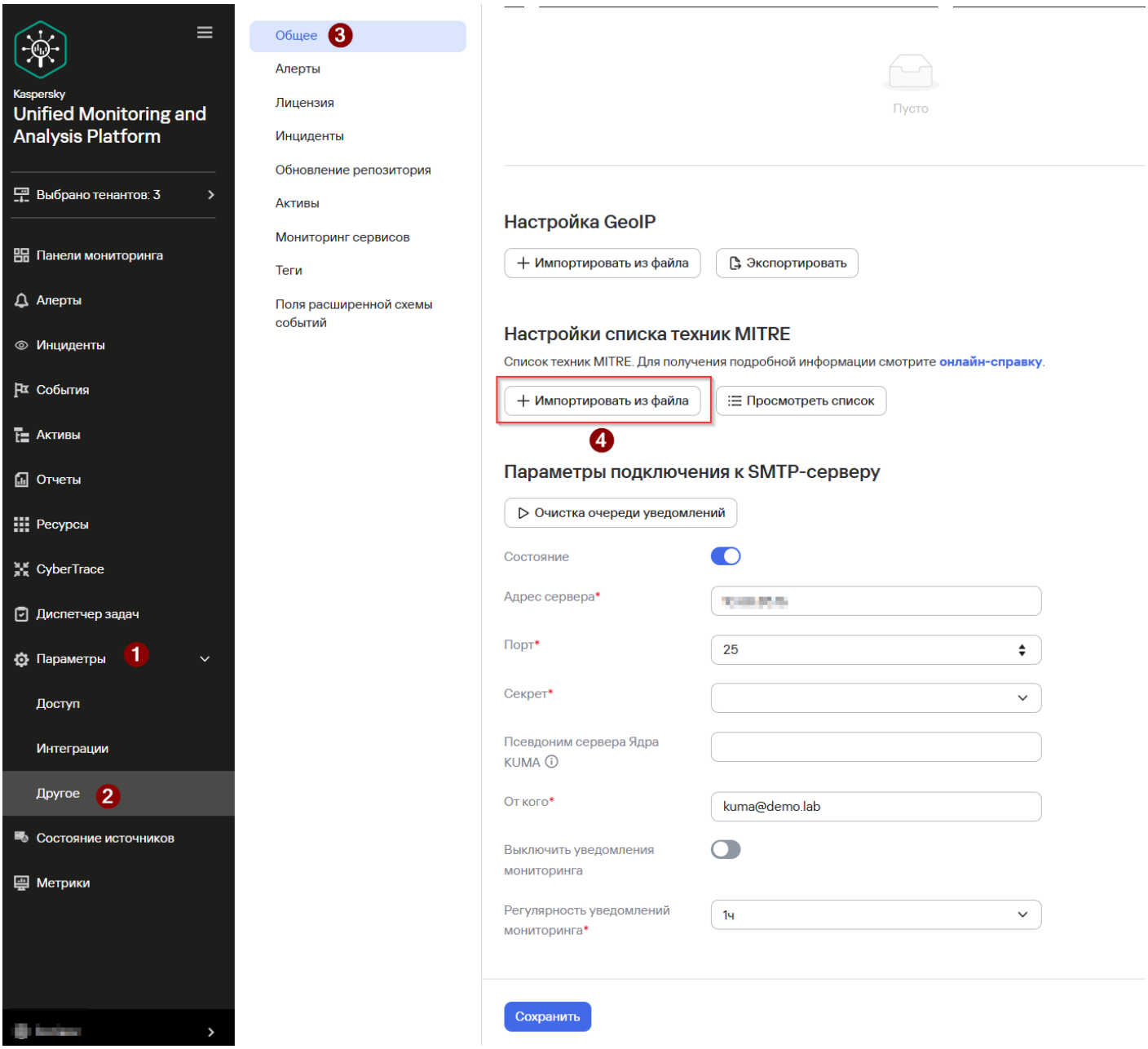
> KUMA поддерживает работу только со справочником техник MITRE ATT&CK версии 14.1.

---

# Импорт справочника техника MITRE

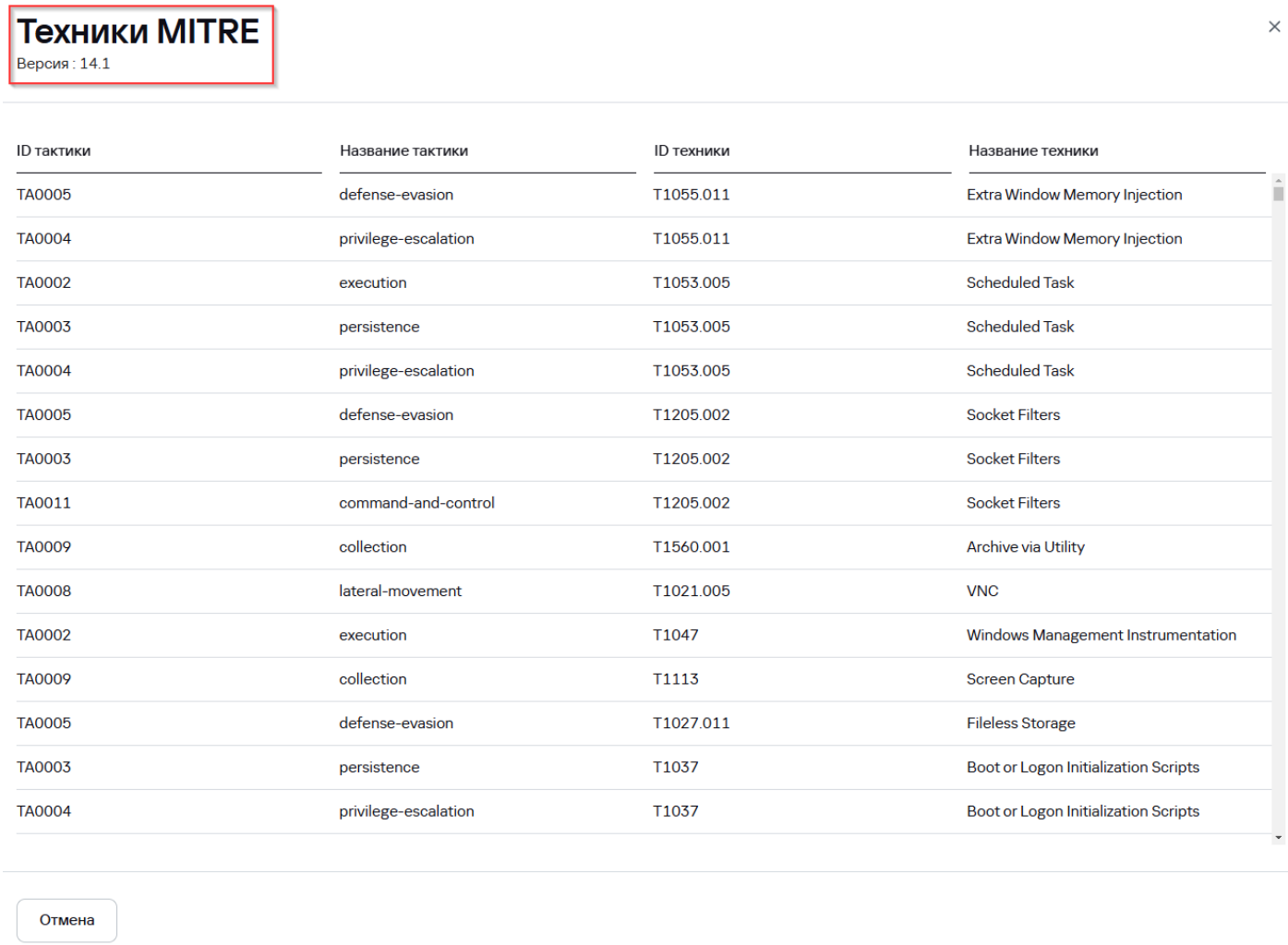
Чтобы импортировать список техник MITRE ATT&CK:

- В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие**.
- В разделе **Настройки списка техник MITRE** нажмите на кнопку Импортировать из файла.



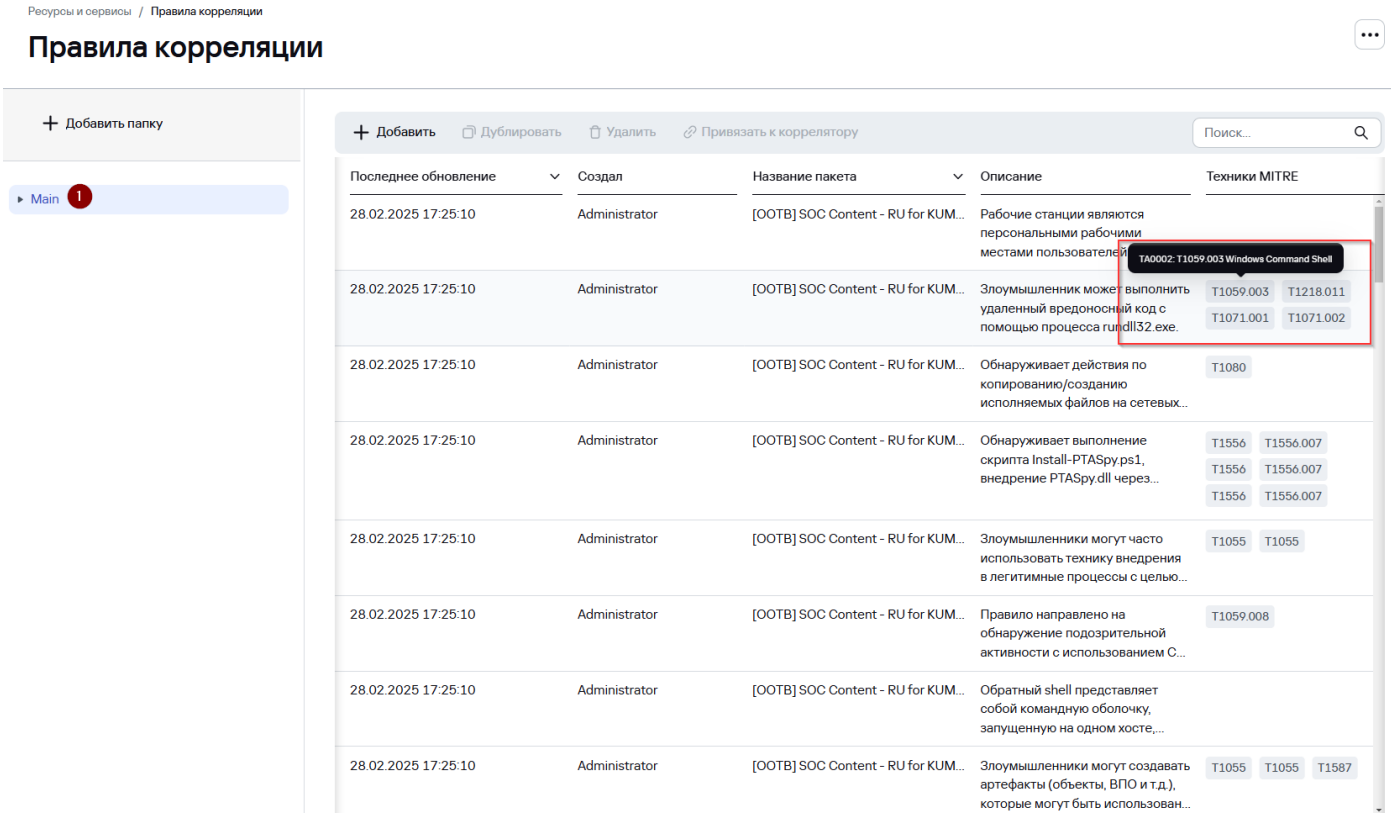

- В окне выбора файлов выберите скачанный справочник техник MITRE ATT&CK и нажмите на кнопку **Открыть**.

Список техник MITRE ATT&CK будет импортирован в KUMA. Вы можете увидеть список импортированных техник и версию справочника техник MITRE ATT&CK, нажав на кнопку **Просмотреть список**.




Чтобы проверить отображение списка техник MITRE ATT&CK для «коробочных» правил корреляции [OOTB] SOC Content - RU for KUMA 3.2:

- Перейдите в **Ресурсы → Правила корреляции** и выберите слева папку **Main**.
- Убедитесь, что в столбце **Техники MITRE** отображается **ID Техники**.



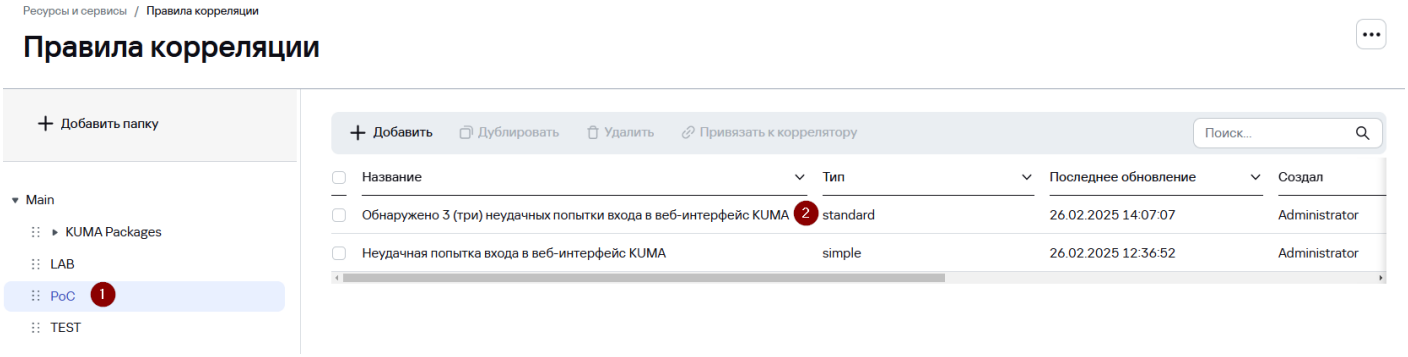

- Если столбец **Техники MITRE** остается пустым, выполните повторный импорт пакета **[OOTB] SOC Content - RU for KUMA 3.2** из репозитория (см. Раздел Импорт ресурсов из репозитория).

---

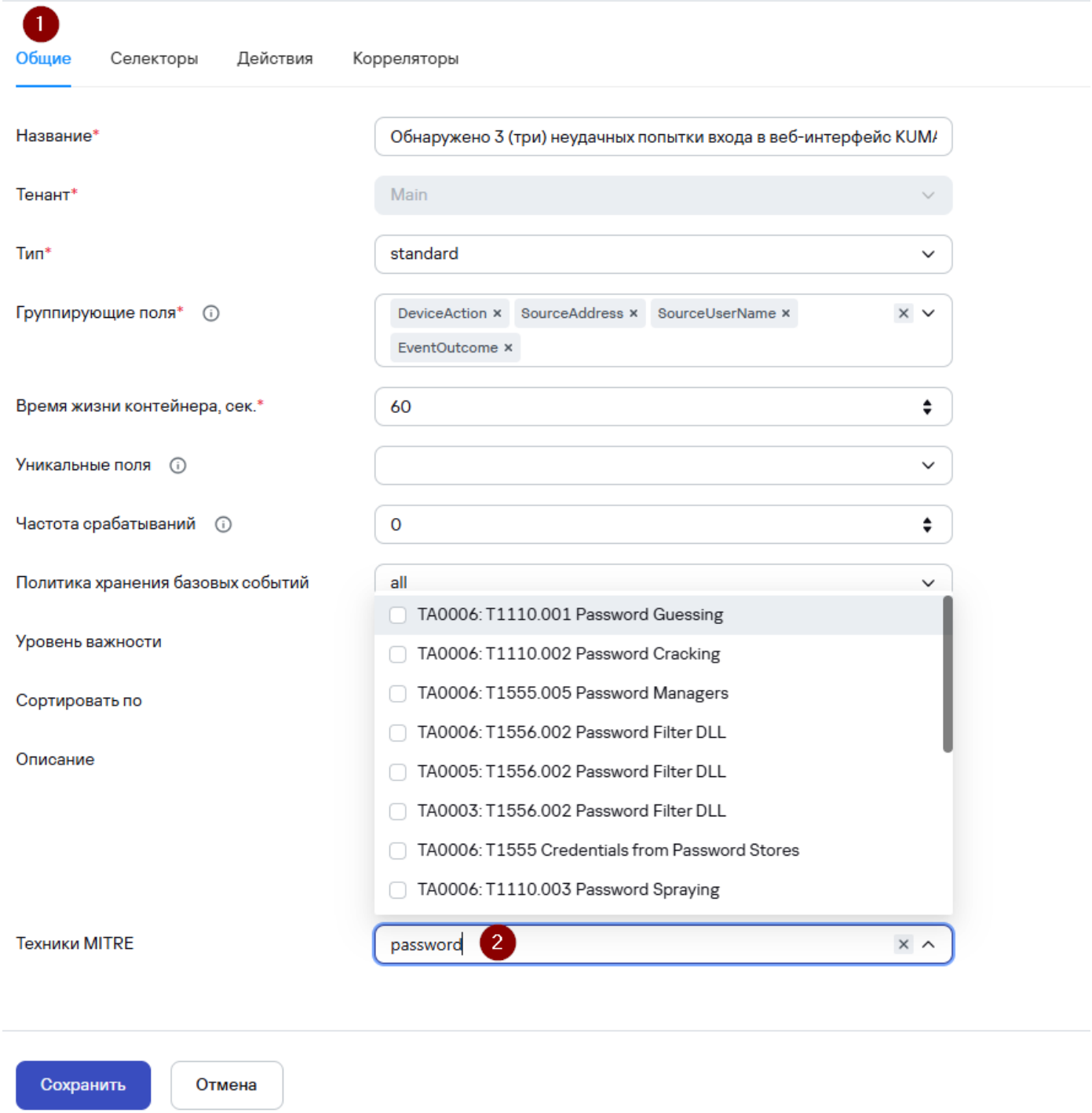
# Привязка техник MITRE к правилам корреляции

Чтобы привязать техники MITRE ATT&CK к правилам корреляции (на примере созданного правила корреляции из Раздела Создание правила корреляции типа Standard):

- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Правила корреляции**.
- В панели слева выберите ранее созданную папку для пользовательских правил корреляции и откройте окно редактирования правила корреляции, нажав на имя правила корреляции.

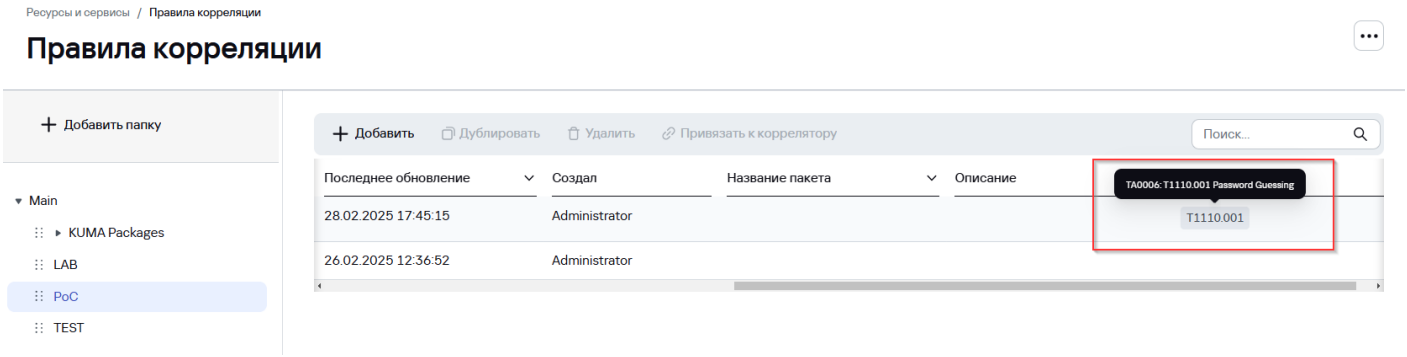



- В окне редактирования правила корреляции во вкладке **Общие** нажмите на поле **Техники MITRE** откроется список доступных техник.
- Для удобства поиска доступен фильтр: в поле можно ввести название техники, ID техники или тактики. Для привязки к правилу корреляции доступна одна или несколько техник MITRE ATT&CK. Так как созданное правило относится к технике Brute Force и производится многократная попытка подобрать пароль введите в поле саб-технику **Password Guessing** (https://attack.mitre.org/techniques/T1110/001/).




- Нажмите на кнопку **Сохранить**.

Техника MITRE ATT&CK будет привязана к правилу корреляции. Убедитесь, что в столбце **Техники MITRE** отображается **ID Техники.**

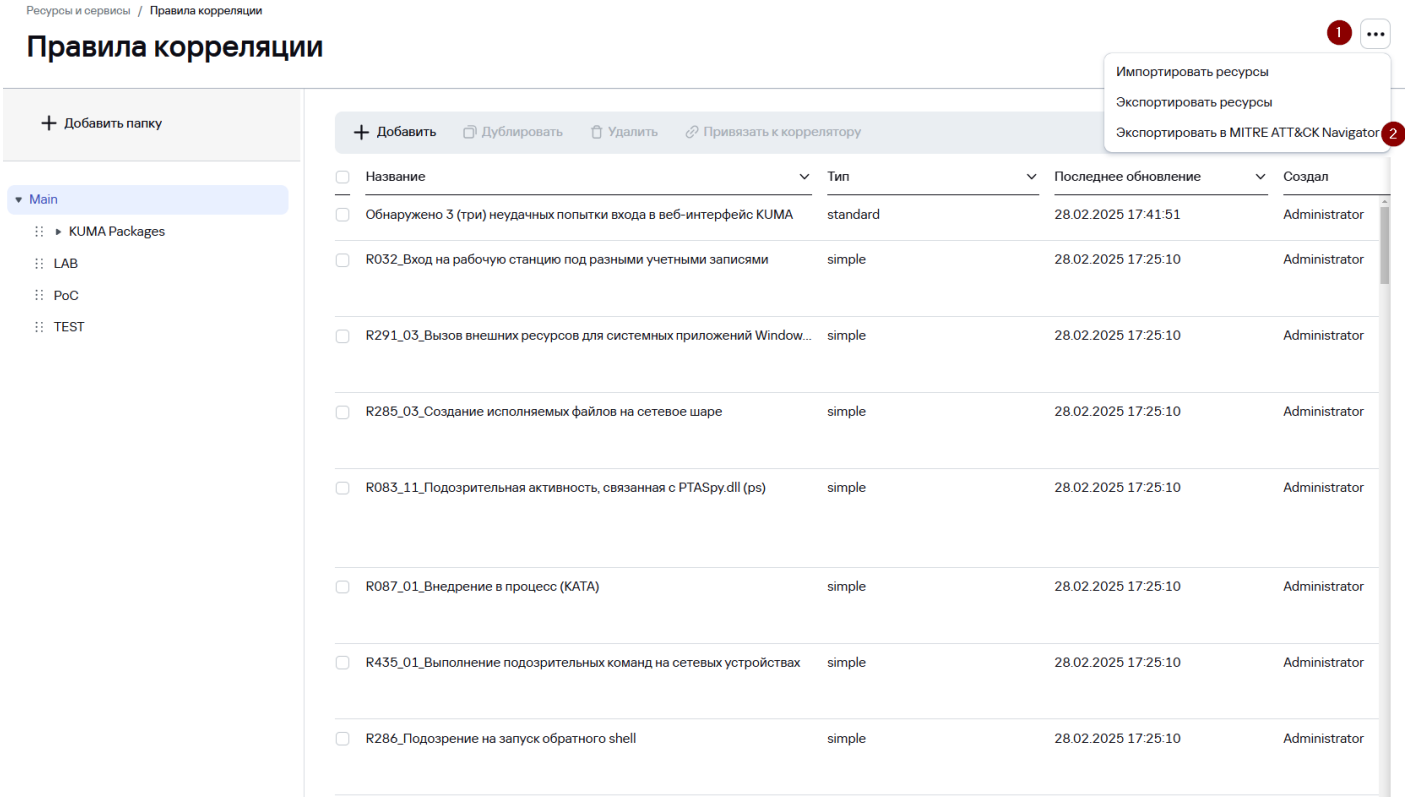



# Экспорт правил корреляции в MITRE ATT&CK Navigator

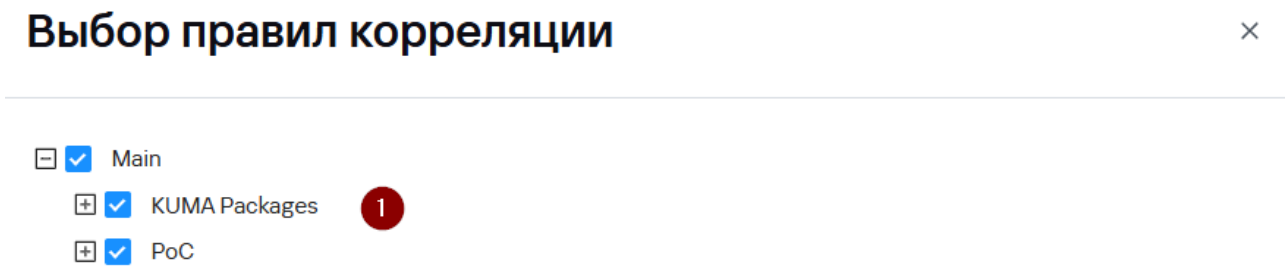
Чтобы оценить покрытие матрицы MITRE ATT&CK корреляционными правилами, используемыми в KUMA («коробочными» и/или пользовательскими), выполните следующие шаги:

> Предварительно выполните привязку техник MITRE к правилам корреляции, созданным самостоятельно.

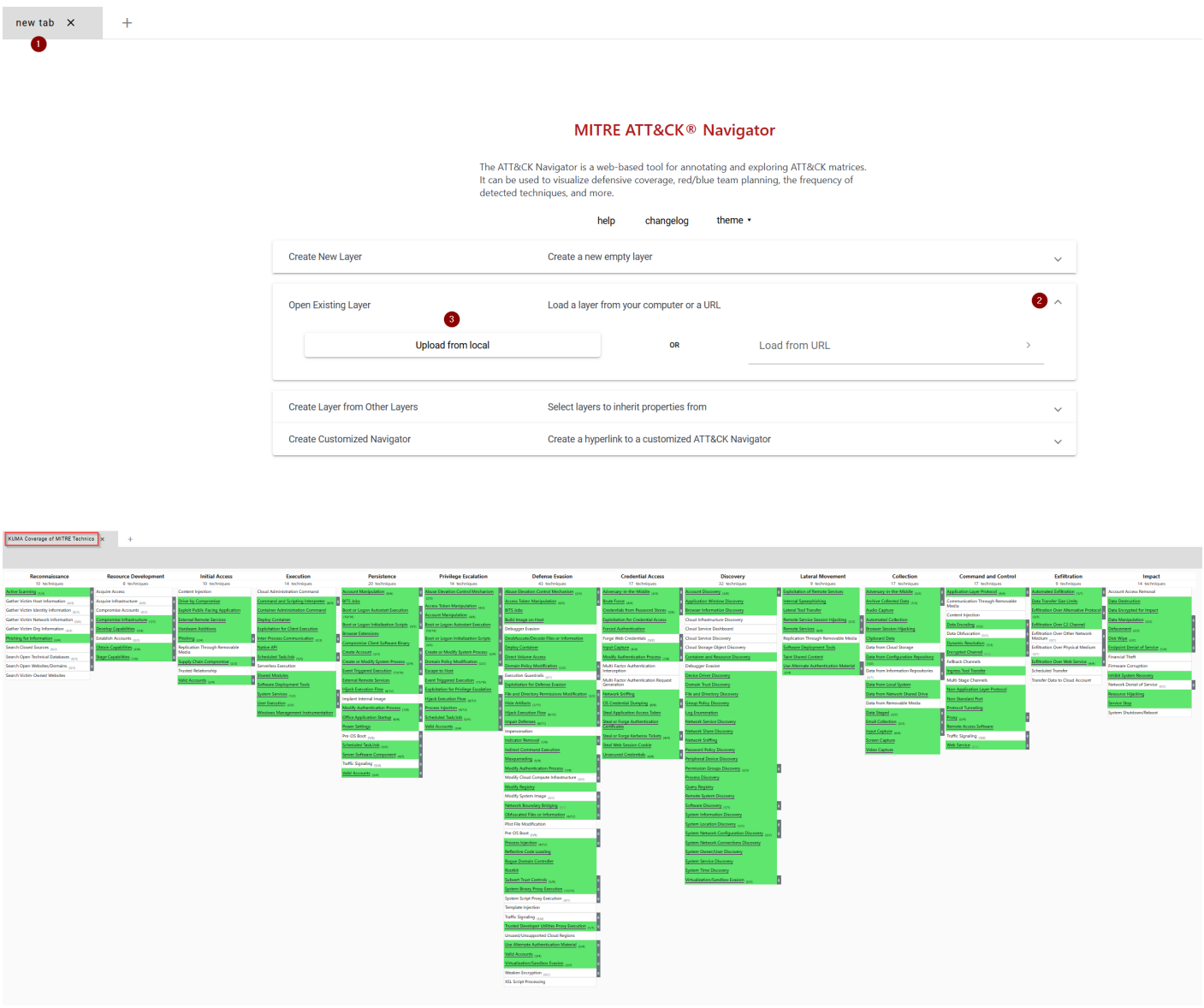
- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Правила корреляции.**
- В правом верхнем углу нажмите на кнопку ••• .
- В раскрывающемся списке нажмите на кнопку **Экспортировать в MITRE ATT&CK Navigator**.



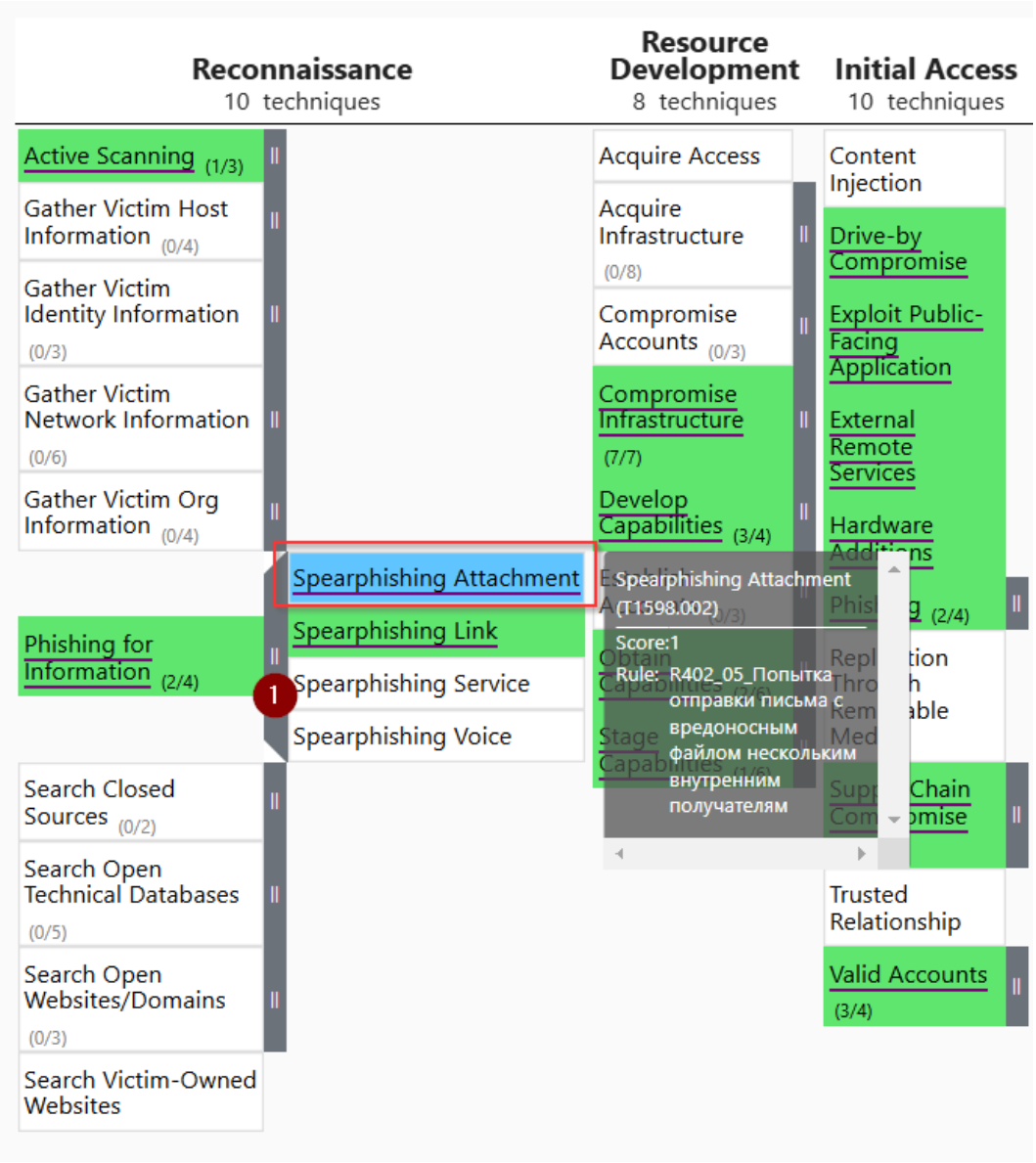

- В открывшемся окне выберите правила корреляции, которые вы хотите экспортировать (выберите все для оценки покрытия всеми правила корреляции).




  Нажмите на кнопку **OK**.
- Файл с экспортированными правилами будет загружен на ваш компьютер в формате json.
- Загрузите файл с вашего компьютера в MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) для оценки покрытия матрицы MITRE ATT&CK.




В результате будет отображено покрытие MITRE ATT&CK. При наведении курсора на конкретную технику или саб-технику будет отображено, покрывающее ее правило.




Revision #2
Created 2026-08-07 16:55:38 UTC by Dmitry Borisov
Updated 2026-08-07 17:21:00 UTC by Dmitry Borisov