

Table of Contents

Table of Contents	1
Настройка инцидентов	2
Настройка инцидентов (описание)	3

Настройка инцидентов (описание)

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Инциденты** предоставляет функциональность встроенной в UserGate SIEM системы IRP — платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

Подробнее о функциональности системы IRP читайте в разделе [Инциденты](#) в Руководстве администратора UserGate SIEM.

Настройки инцидентов в интерфейсе CLI производятся на уровне **incident**.

Для создания собственной схемы расследования инцидентов необходимо:

1. Создать необходимые решения инцидентов.
2. Создать типы инцидентов.
3. Создать состояния инцидентов.
4. Создать схему инцидентов.
5. Активировать схему инцидентов.

Для создания решения инцидентов используется команда:

```
Admin@nodename# create incident resolutions name <incident-name> description <incident-description>
```

Для создания типов инцидентов используется команда:

```
Admin@nodename# create incident types name <incident-type-name> description <incident-type-description>
```

Для создания состояния инцидентов используется команда:

```
Admin@nodename# create incident states name <incident-state-name> description <incident-state-description> group <open|closed|progress>
```

Для создания схемы инцидентов используется команда:

```
Admin@nodename# create incident schema <parameters>
```

Для редактирования доступны следующие параметры схемы инцидентов:

Параметр	Описание
name	Название схемы.
description	Описание схемы
prefix	Префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид: префикс — порядковый номер, например INC-99.
initial-state	Начальное состояние, которое принимает инцидент при его создании.
workflow-states	Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле.
incidents-resolutions	Решения инцидентов — указывает список возможных решений инцидентов.
incidents-types	Типы инцидентов, которые могут быть использованы в этой схеме.
transition	Все возможные переходы между состояниями.

Для всех этапов создания схемы инцидентов также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

