Table of Contents

Table of Contents 1
Инциденты 2
- Общие сведения 3
- Настройки инцидентов 4
- Дашборд по инцидентам 6
- Журнал инцидентов 7
- Создание инцидентов безопасности 9
- Подробности инцидента 10
- Передача отчётов об инцидентах информационной безопасности в ГосСОПКА 12

Инциденты

Общие сведения

Documentation: ☑
Technology: IRP
Version: 7.1.x
Product: SIEM

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 читайте разделе Настройки инцидентов).

IRP система плотно интегрирована с системой SIEM, функциональность которой представлена разделом Аналитика.
Раздел **Аналитика** позволяет задать создание инцидента в качестве действия реагирования, тем самым автоматизируя процесс создания инцидентов информационной безопасности (подробнее о настройке действий реагирования читайте в разделе Действия реагирования).

Также, помимо автоматического создания, инциденты могут быть созданы вручную инженером информационной безопасности (подробнее читайте в разделе Создание инцидентов безопасности).

Настройки инцидентов

Technology: IRP
Version: 7.1.x
Product: SIEM
Documentation: ☑

Процесс расследования инцидента проходит в несколько этапов, на каждом из которых инциденту присваивается определенный статус или **Состояние**, например, **Открыт → Сбор данных → В работе → Закрыт**. Переход между состояниями возможен по определенным правилам, определяемыми администратором, например, нельзя перейти из состояния **Открыт** сразу в состояние **Закрыт**. Возможные переходы между состояниями инцидентов описываются в **Схеме инцидентов**.

По окончании расследования каждому инциденту присваивается **Решение**, например, ложная атака, подтвержденная атака, выполнено и т.п.

Тип инцидента выбирается на этапе создания инцидента и определяет назначение инцидента. Например, типом инцидента может быть Инцидент безопасности, Задача и т.п.

Схема инцидента связывает воедино состояния, возможные переходы между состояниями, решения и типы инцидентов, формируя процесс расследования инцидента информационной безопасности.

UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании. После первоначальной установки решения создается схема расследования по умолчанию с названием **Incident**. Администратор системы может изменить существующую схему или создать свою собственную схему. Можно создать несколько схем расследования инцидентов, но использоваться может только одна схема, которая является активной.

Чтобы создать свою собственную схему расследования инцидентов необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создайте необходимые решения инцидентов	В разделе **Настройки инцидентов → Решения инцидентов** нажмите добавить, укажите название и описание создаваемого решения и нажмите кнопку **Сохранить**.
Шаг 2. Создайте типы инцидентов	В разделе **Настройки инцидентов → Типы инцидентов** нажмите добавить, укажите название и описание создаваемого типа и нажмите кнопку **Сохранить**.
Шаг 3. Создайте состояния инцидентов	В разделе **Настройки инцидентов → Состояния инцидентов** нажмите добавить, укажите название, описание и группу создаваемого состояния. Группа состояние определяет положение данного состояние в схеме состояний. Возможно 3 варианта: • **Открыто** — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • **В работе** — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • **Закрыто** — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. После определения всех полей нажмите кнопку **Сохранить**.

Наименование	Описание
Шаг 4. Создайте схему инцидентов	В разделе **Настройки инцидентов → Схемы инцидентов** нажмите добавить и укажите следующие параметры: • Сделать активной — делает данную схему активной. Только одна схема может быть активной, если была активна другая схема, то данное действие сделает ее не активной, и все новые и существующие инциденты перейдут на работу по новой схеме. • Схема — название схемы. • Префикс — префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид Префикс — порядковый номер, например INC-99. • Описание — необязательное описание данной схемы. • Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле. Добавьте сюда все состояния инцидентов, созданные на предыдущем шаге. • Начальное состояние — указывает начальное состояние, которое принимает инцидент при его создании. • Переходы — необходимо указать все возможные переходы между состояниями и дать им названия. Например, создать переход под названием **Взять в работу** для перехода из состояния **Открыто** в состояние **В работе**. Перевод инцидента между состояниями возможен только для тех состояний, между которыми определены переходы. • Решения инцидентов — указывает список возможных решений инцидентов. Решение является обязательным при завершении работы по расследованию тикета, то есть при переводе его в состояние, относящееся к группе **закрыто**. Выберите все необходимые решения, которые были созданы ранее. • Типы инцидентов — укажите типы инцидентов, которые могут быть использованы в этой схеме.
Шаг 5. Активируйте схему инцидентов	После создания схемы инцидентов ее необходимо активировать. Для этого активируйте чекбокс **Сделать активной** в настройках схемы инцидентов.

Дашборд по инцидентам

Technology: IRP
Version: 7.1.x
Product: SIEM
Documentation: ☑

В данной вкладке можно просмотреть текущее состояние инцидентов информационной безопасности, созданных на UserGate SIEM. Отчеты представлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице Дашборд.

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображено в Дашборд.
Диаграмма	Тип представления данных: • Число. • Вертикальная гистограмма. • Таблица.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета.
Описание	Описание виджета.
Количество записей	Максимальное количество записей для отображения.

Журнал инцидентов

Version: 7.1.x
Technology: IRP
Product: SIEM
Documentation: ☑

Во вкладке **Журнал инцидентов** представлен список созданных инцидентов информационной безопасности. В таблице отражена следующая информация об инцидентах.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Создан	date	Дата и время создания инцидента.
Изменён	updateDate	Дата и время последнего изменения.
Индекс	incidentPrefix	Префикс инцидента (INC-N, где N — порядковый номер инцидента; нумерация начинается с 0).
Имя	incidentName	Название инцидента.
Правило	rule	Название правила аналитики, в результате срабатывания которого автоматически был создан инцидент, т.е. при настройке правила аналитики было задано действие реагирования **Создать инцидент**.
Статус	status	Статус инцидента. Существует 3 группы состояний, которые определяют положение данного состояние в схеме состояний: • **Открыто** — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • **В работе** — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • **Закрыто** — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. По умолчанию в UserGate создана схема Incident, которая содержит переходы между всеми состояниями. Схемы инцидентов можно добавить в разделе **Настройки → Настройка инцидентов → Схема инцидентов**. Дополнительные состояния инцидентов можно задать во вкладке **Настройки → Настройка инцидентов → Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Решение	resolution	Решение инцидента. По умолчанию созданы: • **False positive**: ложная атака. • **True positive**: подтверждённая атака. • **Duplicate**: проблема повторяет другую проблему. • **Won't do**: задача не выполнима. • **Done**: проблема решена. Дополнительные решения инцидентов можно создать во вкладке **Настройки → Настройка инцидентов → Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Тип	type	Тип инцидента. По умолчанию доступны 2 типа: инцидент безопасности и задача. Дополнительно типы инцидентов можно создать в разделе **Настройки → Настройка инцидентов → Типы инцидентов** . Подробнее читайте в разделе Настройки инцидентов.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Приоритет	priority	Приоритет инцидента: • Низкий. • Нормальный. • Важный. • Критический.
Инициатор	reporter	Имя администратора, который создал инцидент.
Последнее изменение	lastChangeBy	Имя администратора, который внёс последнее изменение.
Назначен	assignee	Имя администратора, назначенного на инцидент.
Активность		Количество комментариев, срабатываний правил аналитики и журналов событий, добавленных в инцидент.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Возможно производить фильтрацию инцидентов по параметрам, представленным в таблице. Фильтрация доступна в двух режимах: простой и расширенный (подробнее о синтаксисе расширенного поиска читайте в разделе Поиск и фильтрация данных).

Настроенные фильтры можно сохранять, нажав кнопку **Сохранить как**. Сохранённые фильтры можно просмотреть с использованием кнопки **Популярные фильтры**.

Нажатием кнопки **Экспортировать в CSV** администратор может скачать отфильтрованный список инцидентов в csv-файл для дальнейшего анализа.

Создание инцидентов безопасности

Technology: IRP
Version: 7.1.x
Product: SIEM
Documentation: ☑

Во вкладке **Журнал инцидентов** также можно создавать инциденты информационной безопасности. Для создания и работы с инцидентами информационной безопасности пользователь должен обладать определёнными ролевыми разрешениями (подробнее читайте в разделе Роли и ролевые разрешения пользователей).

Инциденты создаются нажатием кнопки **Создать инцидент**. Далее необходимо указать следующие параметры.

Наименование	Описание
Имя	Указать название инцидента информационной безопасности.
Тип	Указать тип инцидента. По умолчанию созданы 2 типа инцидентов: инцидент безопасности и задача. Дополнительно типы инцидентов могут быть созданы в разделе **Настройки → Настройка инцидентов → Типы инцидентов** . Подробнее читайте в разделе Настройки инцидентов.
Приоритет	Назначить приоритет • Низкий. • Нормальный. • Важный. • Критический.
Назначен	Назначить ответственного на инцидент.
Наблюдатели	Указать список сотрудников для наблюдения за инцидентом. При любых изменениях инцидента они будут получать уведомление.
Вложения	Прикрепить файлы, относящиеся к инциденту.
Описание	Ввести описание инцидента.

Подробности инцидента

Technology: IRP
Version: 7.1.x
Product: SIEM
Documentation: ☑

Выбор инцидента и нажатие кнопки **Показать** произведет перевод на новую вкладку (название вкладки формируется из индекса и заданного имени инцидента), где будет отображена подробная информация о выбранном инциденте. На данной вкладке также можно редактировать (кнопка **Редактировать**) и комментировать (кнопка **Комментировать**) инцидент, изменять ответственного за инцидент (кнопка **Назначить**), и статус рабочего процесса (кнопка **Рабочий процесс**). Помимо информации об инциденте, отображённой во вкладке **Журнал инцидентов** (подробнее читайте в разделе Журнал инцидентов), можно увидеть следующую информацию.

В разделе **Срабатывания** отражена информация о срабатываниях правил аналитики, добавленных в инцидент. Подробнее читайте в разделе Срабатывания. Добавить срабатывания в инцидент можно нажатием кнопки **Добавить срабатывания**. Далее необходимо выбрать срабатывания, которые необходимо добавить в инцидент. Чтобы просмотреть подробности срабатывания выделите нужное срабатывание правила аналитики и нажмите кнопку **Показать подробно**. Также можно просмотреть краткую информацию о срабатывании нажав на кнопку **Показать**. Нажатием на кнопку **Удалить из инцидента** можно удалить запись о срабатывании правила аналитики из инцидента. Список срабатываний правил аналитики, добавленный в инциденты, можно скачать в csv-файл для дальнейшего анализа нажатием кнопки **Экспортировать в CSV**.

В разделе **Журналы** отображена подробная информация о событиях всех журналов (подробнее о записях журналов читайте в разделе Поиск). Чтобы добавить события в инцидент нажмите **Добавить в инцидент** и выберите события для добавления. Нажатие кнопки **Удалить из инцидента** позволяет удалить ненужные события.

В разделе **Улики** отображены записи о наблюдениях за объектами, указанными при настройке. Улики необходимы для упрощения анализа инцидента информационной безопасности, принятия верного решения и уменьшения затраченного на инцидент времени. Для получения информации используются ресурсы для обогащения (подробнее читайте в разделе Внешние сервисы обогащений). Подробную информацию, предоставленную сервисом, можно увидеть в настройках обогащения, нажав на обогащение.

Улики можно создать нажатием кнопки **Добавить**. Далее необходимо указать параметры, которые будут отражены в таблице раздела.

Наименование	Описание
Тип улики	Возможен выбор одного из следующих типов улик: • **Автономная система**: система IP-сетей и маршрутизаторов, находящихся под единым управлением. • **Домен**: имя сайта в Интернете. • **Файл**: файл, о котором необходимо собрать информацию. • **Имя файла**: название файла, о котором необходимо собрать информацию. • **FQDN**: полное доменное имя. • **Хэш**: хэш какого-либо файла, например, добавленного в инцидент. • **Имя хоста**: метка устройства, подключённого к компьютерной сети и использующаяся для идентификации устройства. • **IP**: уникальный адрес, идентифицирующий устройство в компьютерной сети. • **Почта**: адрес электронной почты. • **Тема письма**: часть письма, указанная в поле subject. • **Реестр**: ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. • **Путь URI**: последовательность символов, идентифицирующая абстрактный или физический ресурс. • **URL**: индивидуальный адрес ресурса в сети Интернет. • **Агент пользователя**: буквенно-цифровая строка, идентифицирующая программу, которая отправляет запрос на сервер и одновременно запрашивает доступ к web-сайту. • **Другое**.
Значение	Необходимо указать объект, с которым будет производиться работа: IP-адрес, домен, и т.п.

Наименование	Описание
Тип атаки	Для указания доступны следующие типы атаки: • **Ботнет** — сеть заражённых компьютеров, удалённо управляемых преступниками. • **Фишинг** — вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. • **Вредоносное ПО** — любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство. • **DDoS** — способ заблокировать работу сайта путем подачи большого количества запросов, превышающих пропускную способность сети. • **Угон трафика** — злоумышленное перенаправление трафика. • **Сетевое сканирование** — сканирование узлов сети для определения уязвимостей. • **Брутфорс** — метод взлома учётных записей путём подбора паролей к ним. • **Компроментация** — факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа. • **Спам** — массовая рассылка с использованием специальных программ, коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать. • **Другое**.
TLP	Отображена маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • **RED**: информация является крайне конфиденциальной. • **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. • **GREEN**: информация может быть широко распространена в пределах определённого сообщества. • **WHITE**: информация в свободном распространении, но не нарушает авторские права.
Индикатор компроментации?	Чекбокс необходимо отметить, если объект является потенциальным индикатором компроментации.
Сервисы	Отображён список сервисов, которые используются для получения дополнительной информации об объектах наблюдения. Список сервисов отображается автоматически после выбора типа улики. Список сервисов доступен в разделе **Настройки → Библиотеки → Внешние сервисы обогащений** . Подробнее читайте в разделе Внешние сервисы обогащений.
Обновлено	Показаны дата и время последнего обновления сервиса.

С использованием соответствующих кнопок **Редактировать** и **Удалить** улики можно редактировать или удалять.

В разделе **Активность** можно просмотреть комментарии по инциденту и историю внесения изменений (добавление наблюдателей, изменение статуса рабочего процесса и т.д.).

С использованием кнопки **Создать отчёт** можно создать отчёт об инциденте:

- **Incident report**: пользовательский отчёт, который может быть создан на английском или русском языках в формате PDF или HTML. При создании отчёта возможно использование шаблонов, список которых доступен в разделе **Журналы и отчёты → Отчёты инцидентов → Правила отчётов инцидентов**.
- **GOSSOPKA report**: для создание отчёта используется шаблон **Форма для ГОССОПКА**, который соответствует требованиям к отчётам ГОССОПКА. Отчёт можно просто скачать (кнопка **Создать файл**) или сразу сформировать в требуемом формате и отправить в систему личных кабинетов ГОССОПКА (кнопка **Послать через сеть**). Для автоматической отправки отчёта пользователю необходимо предоставить учётную запись для входа в личный кабинет на сайте ГОССОПКА и защищённый канал передачи. Подробнее читайте в разделе Передача отчётов об инцидентах информационной безопасности в ГосСОПКА .

Передача отчётов об инцидентах информационной безопасности в ГосСОПКА

Technology: IRP
Version: 7.1.x
Product: SIEM
Documentation: ☑

ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Целью создания ГосСОПКА является защита критической информационной инфраструктуры (КИИ), владельцы объектов которой должны подключиться к ГосСОПКА. Также к ГосСОПКА можно подключиться и на добровольной основе для обеспечения более высокого уровня информационной безопасности и улучшения методов выявления и реагирования на инциденты.

В UserGate SIEM реализована возможность передачи отчётов о компьютерных атаках, инцидентах и уязвимостях в стандартизированном формате через личный кабинет ГосСОПКА.

Для отправки отчётов необходимо:

1. Самостоятельно подключиться к системе личных кабинетов ГосСОПКА.

Подключение необходимо для взаимодействия и автоматизации обмена информацией о зафиксированных инцидентах информационной безопасности и методах их предотвращения с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

2. Добавить криптографический шлюз для организации межсетевого взаимодействия с сетью НКЦКИ (Национальный координационный центр по компьютерным инцидентам; главный центр ГосСОПКА).

Для самостоятельного подключения к ГосСОПКА используются аппаратно-программные комплексы компаний Инфотекс (ViPNet), Код безопасности (Континент), С-Терра (С-Терра Шлюз).

ПримечаниеНе указывайте криптографический шлюз в качестве шлюза по умолчанию.

3. Добавить DNS-серверы для определения адреса системы личных кабинетов ГосСОПКА.

Для определения адреса системы личных кабинетов ГосСОПКА необходимо добавить серверы с адресами 10.0.100.49 и 10.0.100.50.

ПримечаниеВ список системных DNS-серверов можно добавить не более трёх серверов. Серверы ГосСОПКА не могут быть использованы для преобразования доменных имён в сети Интернет.

4. Настроить статический маршрут в сеть ГосСОПКА для обеспечения доступности DNS-серверов, указанных в пункте 3.

Для обеспечения доступности серверов ГосСОПКА необходимо добавить статический маршрут с адресом назначения: 10.0.100.0/24. Подробнее о настройке маршрутов читайте в разделе Маршруты.

5. Настроить подключение к личному кабинету ГосСОПКА с UserGate SIEM для возможности отправки отчёта.

В UserGate SIEM по умолчанию создан коннектор **Gossopka**, предназначенный для взаимодействия с ГосСОПКА.

Для настройки коннектора перейдите во вкладку **Настройки** в раздел **Сенсоры → Коннектор**. Используйте коннектор **Gossopka**, созданный в UserGate SIEM по умолчанию; необходимо указать: FQDN личного кабинета, вместо указанного по умолчанию (значение по умолчанию отображает формат, в котором должно быть указано значение поля), логин/пароль и ключ API, который добавляется в поле HTTP заголовки.

6. Настроить шаблон отчёта.

По молчанию создан шаблон **Форма для ГОССОПКА**, соответствующий требованиям ГосСОПКА к отчётам. Заполните поля формы; данная форма будет использоваться при формировании отчёта.

Наименование	Описание
Организация	Название организации.
Категория	Категория уведомления: • Уведомление о компьютерном инциденте. • Уведомление о компьютерной атаке. • Уведомление о наличии уязвимости.

Наименование	Описание
Тип события ИБ	Тип события информационной безопасности: • Вовлечение контролируемого ресурса в инфраструктуру ВПО. • Замедление работы ресурса в результате DDoS-атаки. • Заражение ВПО. • Захват сетевого трафика. • Использование контролируемого ресурса для фишинга. • Компрометация учётной записи. • Несанкционированное изменение информации. • Несанкционированное разглашение информации. • Публикация на ресурсе запрещённой законодательством РФ информации. • Рассылка спам-сообщений с контролируемого ресурса. • Успешная эксплуатация уязвимости.
Статус реагирования на инцидент	Статус реагирования на инцидент: • Меры приняты. • Проводятся мероприятия по реагированию. • Возобновлены мероприятия по реагированию.
Необходимость привлечения сил ГосСОПКА	Отметьте чекбокс в случае необходимости привлечения сил ГосСОПКА.
Краткое описание события ИБ	Описание события информационной безопасности.
Сведения о средстве или способе выявления инцидента	Информация о способе и устройстве/ПО, посредством которого был выявлен инцидент.
Дата и время выявления инцидента	Дата и время выявления инцидента заполняются автоматически.
Дата и время завершения инцидента	Дата и время завершения инцидента заполняются автоматически.
Ограничительный маркер TLP	Маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • **RED**: информация является крайне конфиденциальной. • **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. • **GREEN**: информация может быть широко распространена в пределах определённого сообщества. • **WHITE**: информация в свободном распространении, но не нарушает авторские права.
Влияние на доступность	Потенциальное влияние на доступность информационных ресурсов: • Отсутствует. • Низкое. • Высокое.
Влияние на целостность	Потенциальное влияние на целостность ресурсов информационной системы: • Отсутствует. • Низкое. • Высокое.

Наименование	Описание
Влияние на конфиденциальность	Потенциальное влияние на конфиденциальность (ограничение доступа к информационным ресурсам, разрешения доступа к системе только авторизованным пользователям, предотвращение раскрытия информации неуполномоченным лицам): • Отсутствует. • Низкое. • Высокое.
Краткое описание иной формы последствий компьютерного инцидента	Описание последствий инцидента, кроме тех, что были указаны ранее.
Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент	Наименование контролируемого информационного ресурса объекта КИИ, на котором выявлен компьютерный инцидент, компьютерная атака или уязвимость.
Информация о категорировании ОКИИ	Присвоенная объекту КИИ категория значимости: • Информационный ресурс не является объектом КИИ. • Объект КИИ без категории значимости (объект признан незначимым). • Объект КИИ третьей категории значимости (самая низкая). • Объект КИИ второй категории значимости. • Объект КИИ первой категории значимости (самая высокая).
Сфера функционирования субъекта	Сфера функционирования объекта КИИ (например, банковская сфера, здравоохранение и т.п.).
Наличие подключения к сети Интернет	Наличие подключения к сети Интернет: • **Да**. • **Нет**.
Страна/регион	Код в соответствии с ISO-3166-2.
Населенный пункт или геокоординаты	Название населённого пункта или его географические координаты. Географические координаты указываются в формате: *широта* — С.Ш, *долгота* — В.Д.

7. Сформировать и отправить отчёт об инциденте информационной безопасности.

Формирование отчёта доступно во вкладке с подробностями об инциденте нажатием кнопки **Создать отчёт → GOSSOPKA report**. Для отправки отчёта необходимо указать коннектор, настроенный ранее и нажать **Послать через сеть**.

Далее нужно заполнить необходимые поля формы (большинство поле заполнено в соответствии с шаблоном **Форма для ГОССОПКА**) и нажать **ОК**. В случае успешного соединения сервер UserGate SIEM отправит отчёт на коннектор (в систему личных кабинетов ГосСОПКА).

Запись об отправке отчёта будет отображена в журнале событий SIEM.