# Бастион-3 – СС ТМК. Руководство администратора

## Версия 2023.1

()

Самара, 2023

# Оглавление

1 Общие сведения....2
1.1 Назначение и область применения....2
2 Условия применения....2
2.1 Требования к совместимости....2
2.2 Лицензирование системы....2
3 Установка системы....2
4 Настройка системы....3
4.1 Настройка сервиса....3
4.2 Настройка передачи инцидентов....5
5 Работа в штатном режиме....7
5.1 Общие сведения....7
5.2 Передаваемые события....7
6 Нештатные ситуации....8
Приложения....8
Приложение 1. История изменений....8

# 1 Общие сведения

## 1.1 Назначение и область применения

Модуль «Бастион-3 – СС ТМК» предназначен для подключения ПК «Бастион-3» к системе сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры (СС ТМК).

Основной функцией модуля является формирование и передача событий от ПК «Бастион-3» к СС ТМК. В СС ТМК передаются события от следующих подсистем ПК «Бастион-3»:

- Система видеонаблюдения;
- Система контроля и управления доступом;
- Охранно-пожарная сигнализация;
- Система пожарной сигнализации.

Передача событий осуществляется по подписке, параметры которой определяются в СС ТМК.

Дополнительно, модуль предоставляет возможность вручную определить, какие события ПК «Бастион-3» будут передаваться в СС ТМК в качестве инцидентов.

Модуль ПК «Бастион-3 – СС ТМК» не передает в СС ТМК видеопотоки.

# 2 Условия применения

## 2.1 Требования к совместимости

На модуль «Бастион-3 – СС ТМК» распространяются те же требования к аппаратной и программной платформе, что и для ПК «Бастион-3».

Для работы модуля с настройками по умолчанию на сервере должен быть открыт сетевой порт 8099. Порт можно изменить в настройках.

Модуль совместим с ПК «Бастион-3» версии 2023.1 и выше.

## 2.2 Лицензирование системы

Для работы модуля требуется дополнительная лицензия.

# 3 Установка системы

Модуль входит в комплект поставки ПК «Бастион-3». Для его установки в ОС Windows необходимо отметить соответствующую галочку в инсталляторе ПК «Бастион-3».

Для ОС Linux модуль поставляется в виде отдельного пакета формата DEB или RPM, с именем bastion3-tmk_*.

# 4 Настройка системы

## 4.1 Настройка сервиса

Настройка сервиса осуществляется при помощи панели управления ПК «Бастион-3». Для открытия страницы настройки модуля «Бастион-3 – СС ТМК» необходимо кликнуть по кнопке в панели управления (Рис. 1).

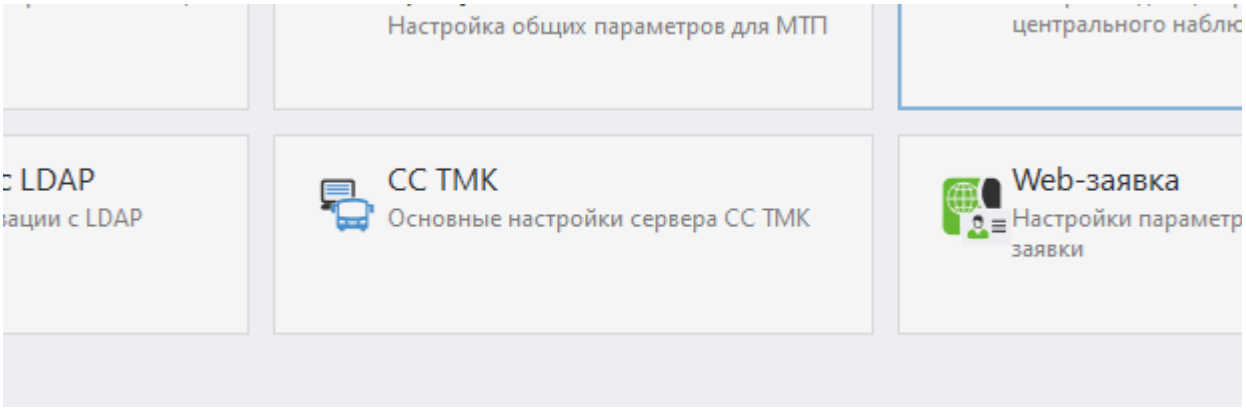


**Рис. 1 Кнопка открытия страницы настроек модуля «Бастион-3 – СС ТМК»**

Окно конфигуратора представлено на Рис. 2 и состоит из дерева конфигурации, панели инструментов и вкладки с информацией. Дерево конфигурации представлено одним основным элементом – «Настройки». Панель инструментов содержит кнопки «Сохранить» и «Отменить изменения».

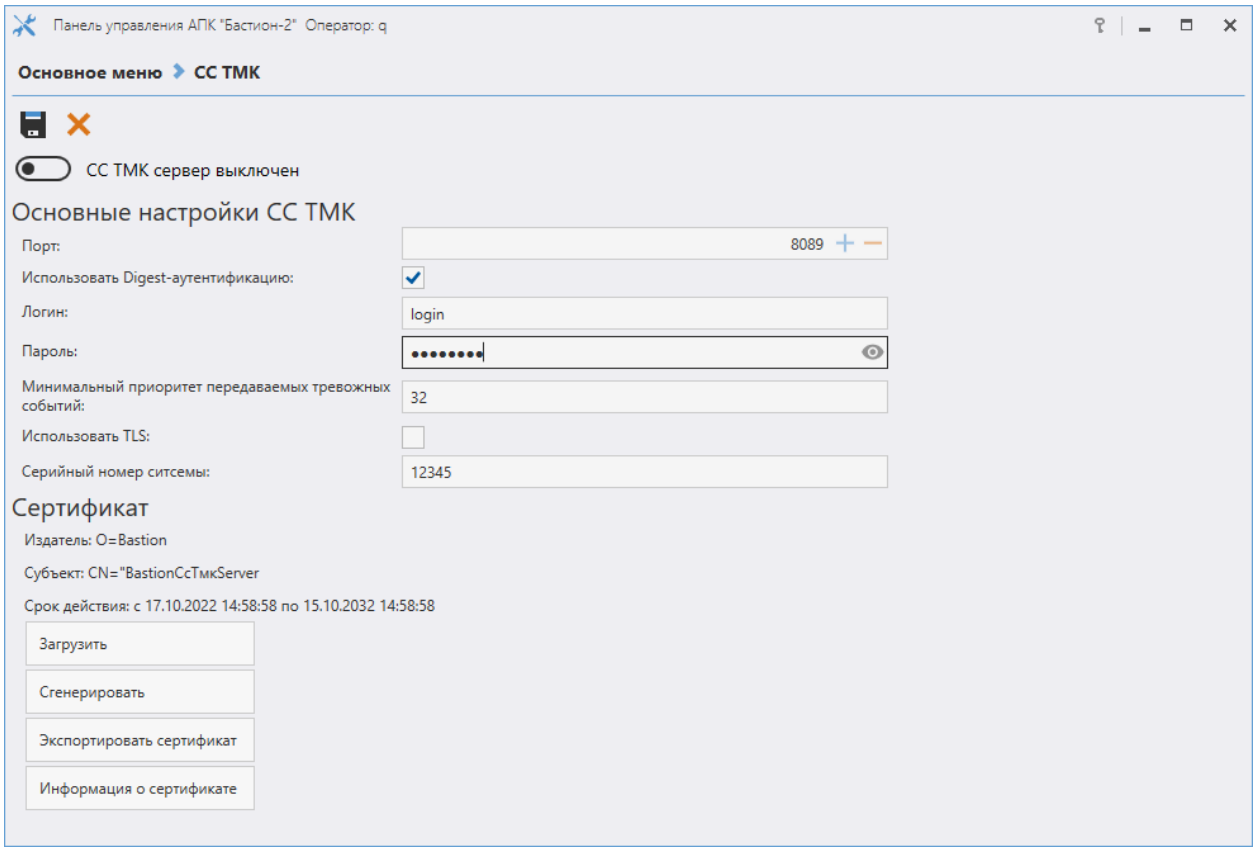


**Рис. 2 Страница настройки модуля «Бастион-3 – СС ТМК»**

Настройки модуля представлены параметрами, которые описаны ниже.

*Включить службы СС ТМК* – если флаг отключен, модуль СС ТМК не функционирует.

*Порт* – сетевой порт, на котором будет выполняться основная сетевая служба, а также побочные службы, обслуживающие подписки на события. Значение должно быть числом в диапазоне 1 – 65535. Выбранный порт должен быть открыт в сетевых экранах, в противном случае возможны проблемы с доступом к сервисам.

*Использовать Digest-аутентификацию* – если флаг установлен, то при обработке запросов модуль будет проверять заголовок Digest-аутентификации в каждом запросе на соответствие параметрам, указанным ниже – логину и паролю. По умолчанию Digest-аутентификация выключена.

*Логин/пароль* – логин и пароль для Digest-аутентификации. Пара логин/пароль проверяется для каждого входящего запроса в случаях, когда активирована опция «Использовать Digest-аутентификацию».

*Минимальный приоритет передаваемых тревожных событий* – значение этой настройки определяет, какие тревожные события будут передаваться в СС ТМК в качестве инцидента (события типа AccessControl/Accident). Тревоги с приоритетом ниже заданного передаваться не будут.

*Использовать TLS* – активация этой настройки меняет используемый протокол коммуникации с HTTP на HTTPS. При этом необходимо, чтобы был привязан корректный сертификат X.509 (настройка *TSL-сертификат*).

*Серийный номер системы* – это поле нужно заполнить серийным номером ПК «Бастион-3», который указан в Паспорте на систему.

*Сертификат* – TLS-сертификат для использования защищенного протокола HTTPS. Сертификат необходим, если включена опция *использовать TLS*. Его можно сгенерировать на сервере системы, нажав кнопку "Сгенерировать".

Имеется возможность использовать свой сертификат, для этого нужно воспользоваться кнопкой «Загрузить», где в появившимся окне необходимо выбрать файл сертификата. Для этого сертификат должен быть экспортирован вместе с приватным ключом в файл формата *pfx* или *p12*. По стандарту PKSC#12 сертификат и закрытый ключ хранятся в одном зашифрованном файле, поэтому при загрузке сертификата понадобится ввести пароль от этого файла. Если сертификат загружен корректно и с правильным паролем, то в окне настроек появится издатель, субъект и срок действия сертификата. Если данные поля остались не заполненными, убедитесь в корректности сертификата и его пароля при вводе.

Для получения сертификата в виде файла в формате *der* необходимо воспользоваться кнопкой «Экспортировать сертификат», после чего выбрать место сохранения и имя, нажать на кнопку «Сохранить». Сертификат в виде файла в формате der можно использовать для размещения в хранилище сертификатов.

Для получения более полной информации о сертификате требуется нажать кнопку «Информация о сертификате», что приведёт к открытию диалогового окна с расширенной информацией.

Рекомендуется использовать сертификаты с алгоритмом шифрования *RSA* или *ECDsa* и алгоритмом подписи *SHA256*, *SHA384* или *SHA512*.

## 4.2 Настройка передачи инцидентов

С настройками по умолчанию ПК «Бастион-3» с установленным модулем «Бастион-3 – СС ТМК» передаёт инциденты (события типа AccessControl/Accident) только при возникновении тревожных событий с приоритетом не ниже, чем указано в настройке «Минимальный приоритет передаваемых тревожных событий».

Помимо этого, есть возможность дополнительно настроить, при каких событиях в СС ТМК будет передаваться информация об инциденте. Для этого необходимо задействовать механизм сценариев ПК «Бастион-3», процесс настройки которых описан в руководстве администратора ПК «Бастион-3».

Для того чтобы настроить формирование инцидента при возникновении события, следует создать сценарий, выполняющий действие «Оповестить об инциденте» (Рис. 3).

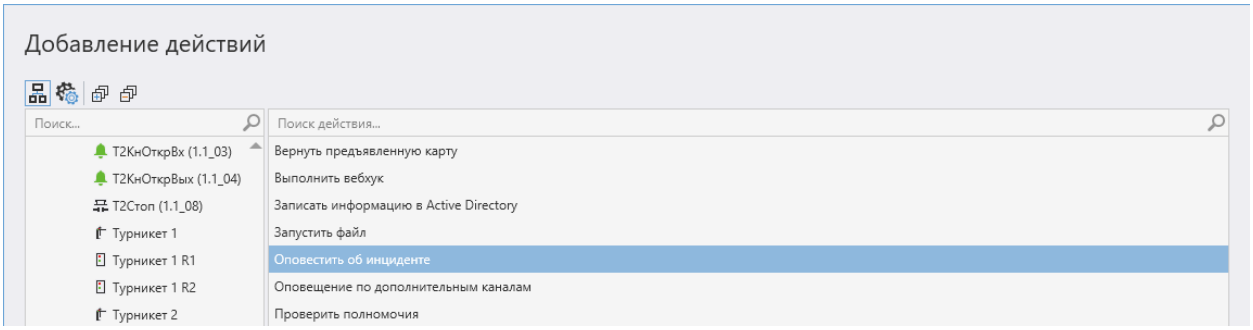


**Рис. 3 Действие «Оповестить об инциденте»**

Наименование инцидента (значение элемента «Name» события типа AccessControl/Accident) задаётся в качестве параметра выполняемого действия (Рис. 4).

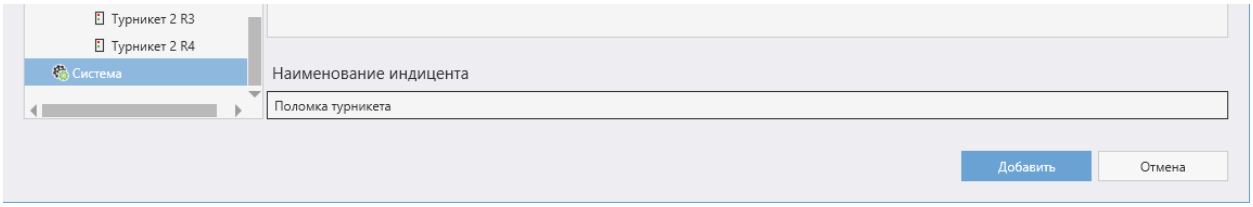


**Рис. 4 Наименование инцидента**

Пример настроенного формирования инцидента при возникновении события в ПК «Бастион-3» изображен на Рис. 5.

Для формирования одинаковых сообщений об инциденте при разных исходных событиях ПК «Бастион-3», можно добавить в сценарий несколько триггеров. Это могут триггеры любых типов. Пример такой настройки изображен на Рис. 6.

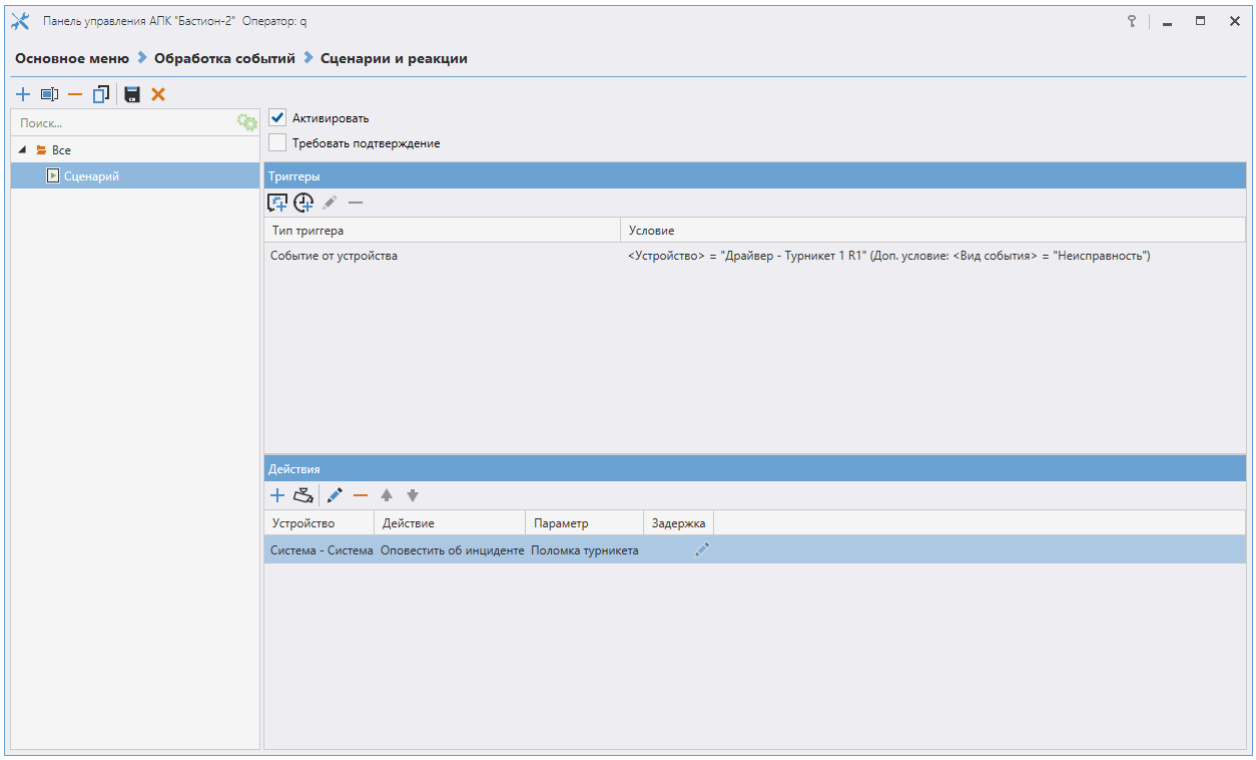


**Рис. 5 Сценарий формирования инцидента при возникновении события**

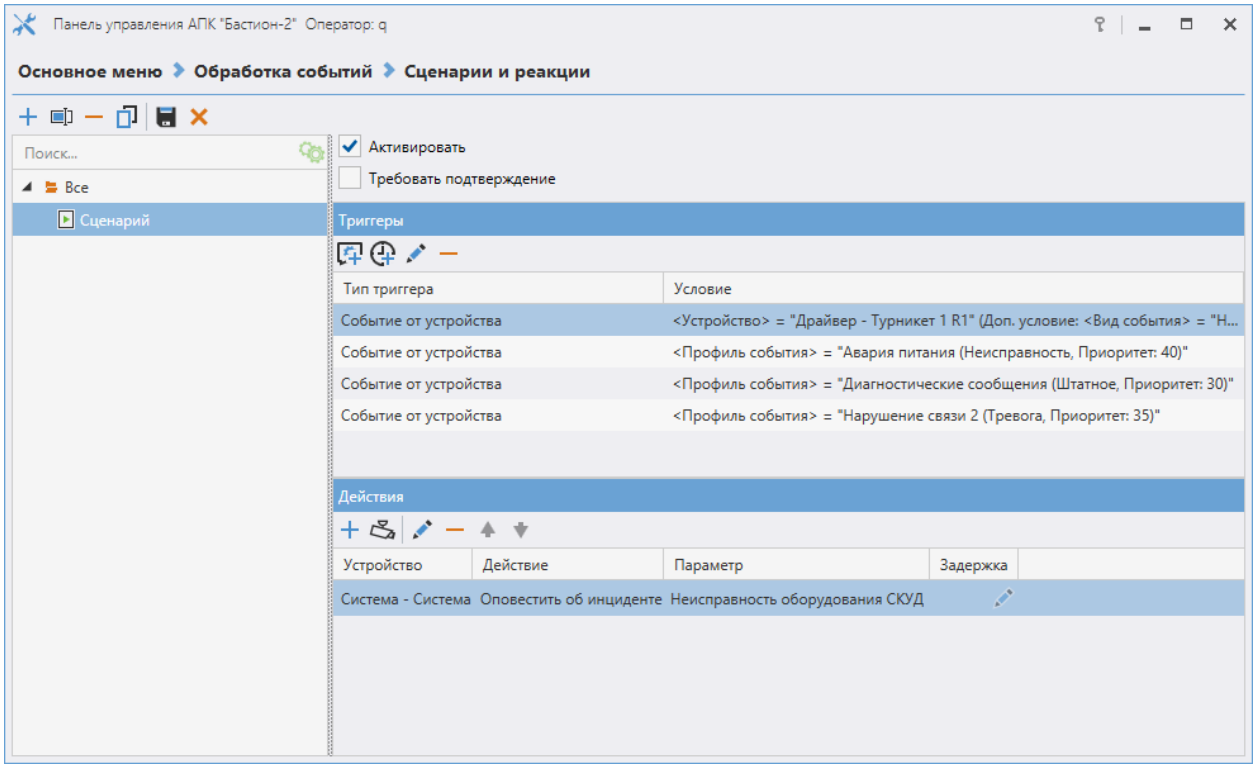


**Рис. 6 Сценарий формирования инцидента при срабатывании любого триггера из группы**

# 5 Работа в штатном режиме

## 5.1 Общие сведения

В штатном режиме модуль «Бастион-3 – СС ТМК» позволяет СС ТМК подписываться на события и получать их.

Максимальное количество одновременно обслуживаемых подписок не ограничено. Подписки могут быть ограниченными по времени, либо неограниченными (keep-alive).

## 5.2 Передаваемые события

Модуль отправляет в СС ТМК события в перечисленных ниже случаях:

- При возникновении события «Подключился к серверу видеонаблюдения» драйвера «Бастион-3 – Видео» формируется сообщение VideoSurveillanceSystem ServerPowerOn (система видеонаблюдения – включение сервера);
- При возникновении события «Отключился от сервера видеонаблюдения» драйвера «Бастион-3 – Видео» формируется сообщение VideoSurveillanceSystem ServerPowerOff (система видеонаблюдения – выключение сервера);
- При возникновении события «Штатный въезд», «Штатный выезд», «Обнаружено лицо», «Зафиксирован звук», «Зафиксировано пересечение линии», «Зафиксирован вход в зону», «Зафиксирован выход из зоны», «Зафиксировано появление в зоне», «Зафиксировано исчезновение из зоны», «Сработал детектор оставленных объектов», «Сработал детектор толпы», «Сработал детектор саботажа», «Сработал тревожный вход 1», «Сработал тревожный вход 2», «Сработал тревожный вход 3», «Сработал тревожный вход 4», «Зафиксировано движение», «Проезд т/с с разрешенным № в запрещенном направлении», «Въезд т/с с запрещенным №», «Выезд т/с с запрещенным номером», «Проезд т/с с запрещенным № в запрещенном направлении», «Въезд т/с с неизвестным №», «Выезд т/с с неизвестным №», «Проезд т/с с неизвестным № в запрещенном направлении», «Въезд т/с с противоречивым статусом №», «Выезд т/с с противоречивым статусом №», «Проезд т/с с противоречивым статусом № в запрещенном направлении», «Проезд т/с № в неопределённом направлении», «Проезд т/с с запрещённым номером № в неопределённом направлении», «Проезд т/с с неизвестным № в неопределённом направлении» или «Проезд т/с с противоречивым статусом № в неопределённом направлении» драйвера «Бастион-3 – Видео» формируется сообщение VideoSurveillanceSystem MotionDetectorTrigger (система видеонаблюдения – срабатывание детекторов движения);

- При возникновении события «Пожарная тревога», «Дым ниже порога» или «Тушение» драйвера «Бастион-3 – Рубеж» формируется сообщение FireAlarm Alarm (система пожарной сигнализации - тревога);
- При возникновении события «Опасность пожара» или «Пожарная тревога» драйвера «Бастион-3 – С2000» формируется сообщение FireAlarm Alarm (система пожарной сигнализации - тревога);
- При возникновении любого события типа «Неисправность» (кроме драйверов «Бастион-3 –Видео») формируется сообщение AccessControl Fault (система контроля и управления доступом и охранная сигнализация - неисправность);
- При возникновении любого тревожного события (кроме драйверов «Бастион-3 –Видео») с приоритетом не ниже указанного в настройке «Минимальный приоритет передаваемых тревожных событий» (пп. 4.2.5) формируется сообщение AccessControl Accident (система контроля и управления доступом и охранная сигнализация - инцидент);
- При срабатывании сценарного действия «Оповестить об инциденте» во всех случаях формируется сообщение AccessControl Accident (система контроля и управления доступом и охранная сигнализация - инцидент).

# 6 Нештатные ситуации

В случае, когда модуль «Бастион-3 – СС ТМК» не смог запустить главную службу, в отладочную консоль ПК «Бастион-3» выведется сообщение об ошибке. Это может быть ошибка, свидетельствующая о том, что модуль не может воспользоваться указанным в параметрах портом для запуска сетевых служб по причине того, что порт занят другим приложением. Для устранения этой неисправности следует сменить порт, используемый службами модуля «Бастион-3 – СС ТМК».

# Приложения

# Приложение 1. История изменений

## 1.0.6 (03.04.2023)

[+] Первая версия модуля для ПК «Бастион-3».