



Бастион-3 – Аудит системы. Руководство  
администратора

Версия 2024.3

(17.10.2024)



Самара, 2024



## Оглавление

1. Общие сведения.....	2
2. Условия применения.....	2
3. Установка.....	2
4. Настройка.....	3
4.1. Настройка параметров подсистемы аудита.....	3
4.2. Настройка прав доступа к подсистеме аудита.....	4
5. Выполнение основных операций.....	5
5.1. Просмотр журнала аудита.....	5
5.2. Экспорт журнала аудита.....	7
Приложения.....	7
Приложение 1. История изменений.....	7

## 1. Общие сведения

Модуль «Бастиян-3 — Аудит системы» предназначен для протоколирования действий всех операторов системы, технологических процессов внутри системы, событий безопасности, операций доступа операторов к информационным ресурсам, а также для доступа и поиска по журналам аудита.

Информация в журнале аудита представляется в структурированном виде в терминах прикладной области, то есть фиксируются события с бизнес-сущностями, а не с объектами баз данных.

Доступ к журналу аудита предоставляется только уполномоченным пользователям через прикладной интерфейс приложения «Бастиян-3 — Аудит системы».

В журнале аудита для каждого события указываются следующие реквизиты: дата и время; идентификатор пользователя, действия которого привели к возникновению события; наименование; идентификатор/наименование данных, на которые происходило воздействие; параметры; результат (успешный/неуспешный).

Наличие в журнале аудита чувствительных данных (пароли пользователей, биометрические данные, аутентификации информация, токены доступа и т.п.) исключено.

В системе реализована возможность формирования отчетов, отражающих события, зафиксированные в журнале аудита. Сформированные отчеты могут выводиться на экран компьютера, а также распечатываться и сохраняться в файлы.

В настоящее время модуль «Аудит системы» фиксирует все действия, который выполняются с данными, на сервере системы. Выгрузка/сохранение фотографии персоны в «Бюро пропусков» выполняется уже на стороне клиента.

## 2. Условия применения

Требования к программной и аппаратной среде модуля «Бастиян-3 — Аудит системы» соответствуют общим требованиям для ПК «Бастиян-3».

Дополнительно, следует учитывать, что журнал аудита может иметь очень большой размер, особенно при включении протоколирования доступа к данным. Это может создавать дополнительную существенную нагрузку на сервер БД.

Модуль «Бастиян-3 — Аудит системы» может применяться с ПК «Бастиян-3» начиная с версии 2024.2.

Для запуска клиентского приложения «Бастиян-3 — Аудит системы» необходимо наличие лицензии.

Следует учитывать, что сам механизм протоколирования изменений может быть включен, даже если в системе нет ни одной лицензии на «Бастиян-3 — Аудит системы». Весь протокол изменений данных будет сохранен с момента включения протоколирования изменений.

## 3. Установка

Установка приложения «Бастиян-3 — Аудит системы» производится в рамках установки ПК «Бастиян-3».



Для установки клиентского приложения «Бастсион-3 — Аудит системы» в установщике для ОС Windows следует выбрать пункт «Аудит» в списке устанавливаемых компонентов. Для установки компонентов, ответственных за запись журнала аудита и настройку подсистемы аудита, следует выбрать пункт «Аудит» в списке компонентов расширения.

Для ОС Linux система «Бастсион-3 — Аудит системы» поставляется в виде двух пакетов:

bastion3-audit\* - серверный пакет + модуль настройки подсистемы аудита.

bastion3-audit-client\* - клиентское приложения подсистемы аудита.

Там, где используется клиентское приложение аудита, необходима установка обоих пакетов.

## 4. Настройка

### 4.1. Настройка параметров подсистемы аудита

Настройка системы «Бастсион-3 — Аудит системы» производится в панели управления ПК «Бастсион-3» на странице «Аудит системы» (Рис. 1).

По умолчанию, аудит полностью отключен. Пользователь имеет возможность включить аудит и настроить уровни протоколирования для различных групп сущностей системы. На Рис. 1 приведены доступные группы сущностей и их содержание.

Для каждой группы доступны следующие уровни протоколирования:

*Выкл.* — аудит группы сущностей полностью отключен.

*Основное* — будет протоколироваться только факты доступа к сущности, факты действия с сущностью, а также факты изменения сущности, без указания деталей, какие именно поля были затронуты.

*Детально* — будут протоколироваться все действия с сущностью с указанием старых и новых значений для всех изменённых полей сущности.

Дополнительно, есть возможность для всех групп сущностей включить / отключить:

- Протоколирование изменений объектов системы;
- Протоколирование доступа к объектам системы.

Настройки протоколирования объединяются по правилу «И». Таким образом, например, если отключено протоколирование доступа к объектам системы, и включено детальное протоколирование для группы сущностей «Отчёты», то события доступа к отчётам не будут протоколироваться системой.

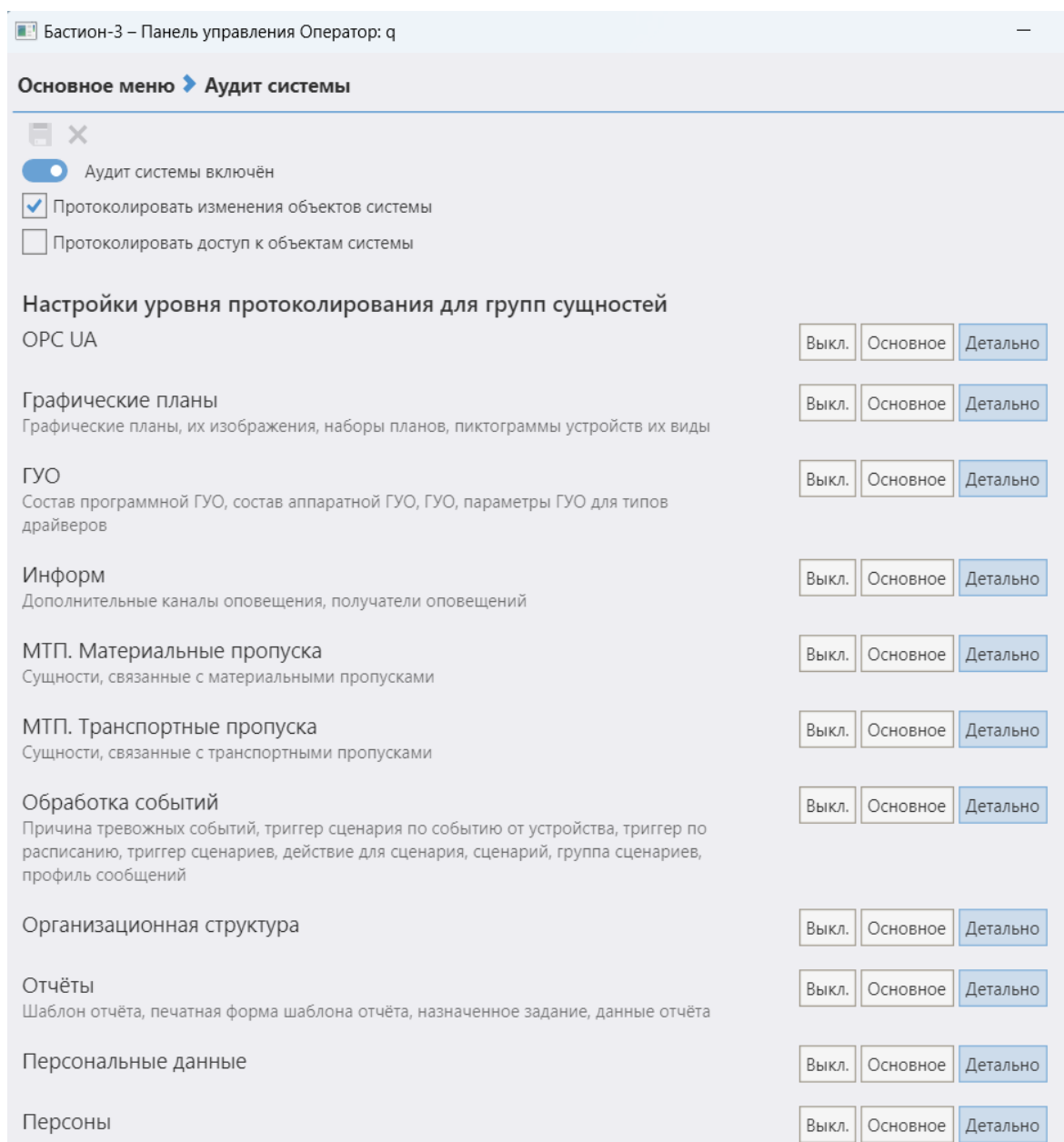


Рис. 1. Настройка модуля «Бастион-3 — Аудит системы»

## 4.2. Настройка прав доступа к подсистеме аудита

В системе предусмотрен следующий набор полномочий, которыми должен обладать оператор, чтобы иметь доступ к подсистеме аудита:

*Право запуска приложения «Аудит системы».* Только оператор с ролью, для которой установлено это полномочие, сможет запустить и авторизоваться в клиентском приложении «Бастион-3 — Аудит системы».

*Доступ к данным Аудита системы.* Только оператор с ролью, для которой установлено это полномочие, сможет получить доступ к данным аудита через любые интерфейсы системы, включая Web API.

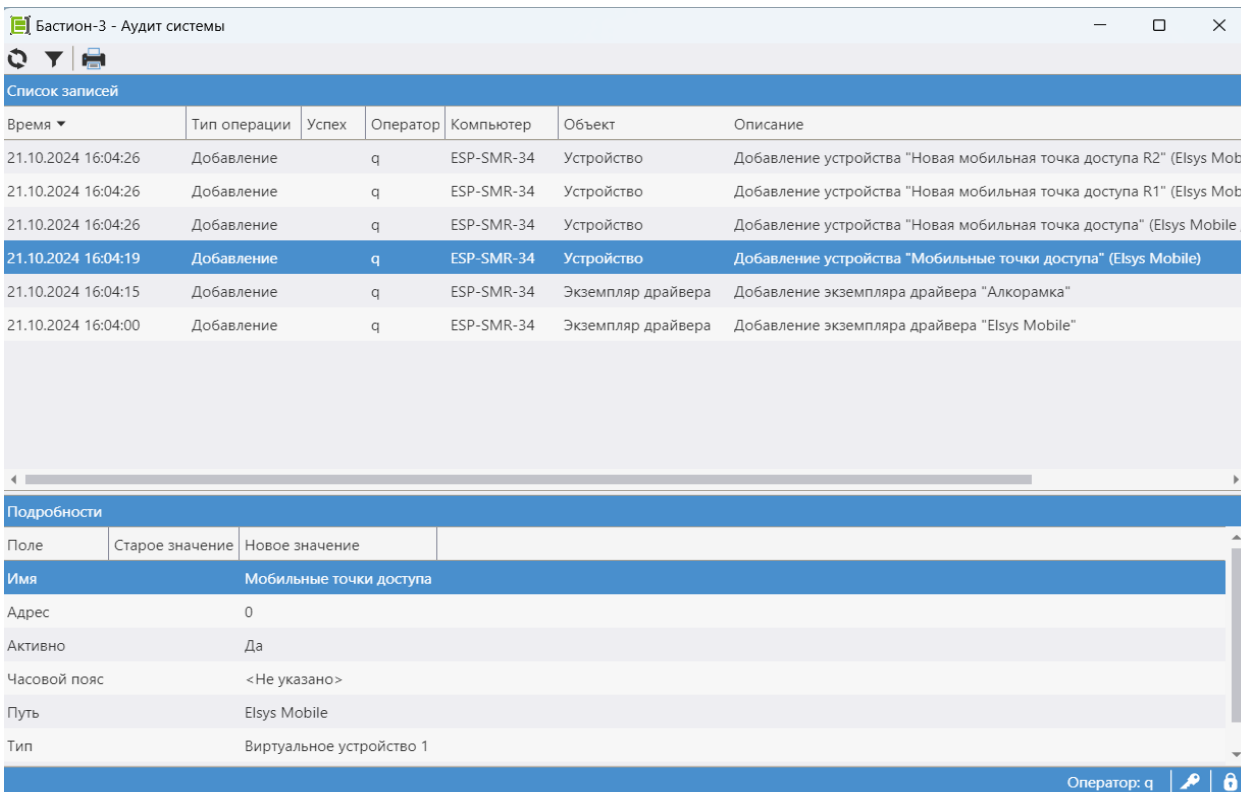
Редактирование параметров Аудита системы. Только оператор с ролью, для которой установлено это полномочие, сможет изменять настройки подсистемы аудита.

## 5. Выполнение основных операций

### 5.1. Просмотр журнала аудита

В основном окне приложения «Бастион-3 — Аудит системы» можно просматривать журнал аудита (Рис. 2).

При запуске приложения отобразится пустая таблица. Для отображения данных следует нажать кнопку «Обновить».



The screenshot shows the 'Бастион-3 - Аудит системы' application window. It features a table titled 'Список записей' (List of records) with columns: 'Время' (Time), 'Тип операции' (Operation type), 'Успех' (Success), 'Оператор' (Operator), 'Компьютер' (Computer), 'Объект' (Object), and 'Описание' (Description). The table contains several entries, with the most recent one highlighted in blue. Below the table is a 'Подробности' (Details) pane showing fields like 'Имя' (Name), 'Адрес' (Address), 'Активно' (Active), 'Часовой пояс' (Time zone), 'Путь' (Path), and 'Тип' (Type).

Время	Тип операции	Успех	Оператор	Компьютер	Объект	Описание
21.10.2024 16:04:26	Добавление	q	ESP-SMR-34	Устройство	Добавление устройства "Новая мобильная точка доступа R2" (Elsys Mobile)	
21.10.2024 16:04:26	Добавление	q	ESP-SMR-34	Устройство	Добавление устройства "Новая мобильная точка доступа R1" (Elsys Mobile)	
21.10.2024 16:04:26	Добавление	q	ESP-SMR-34	Устройство	Добавление устройства "Новая мобильная точка доступа" (Elsys Mobile /	
21.10.2024 16:04:19	Добавление	q	ESP-SMR-34	Устройство	Добавление устройства "Мобильные точки доступа" (Elsys Mobile)	
21.10.2024 16:04:15	Добавление	q	ESP-SMR-34	Экземпляр драйвера	Добавление экземпляра драйвера "Алкорамка"	
21.10.2024 16:04:00	Добавление	q	ESP-SMR-34	Экземпляр драйвера	Добавление экземпляра драйвера "Elsys Mobile"	

Поле	Старое значение	Новое значение
Имя	Мобильные точки доступа	
Адрес		0
Активно		Да
Часовой пояс		<Не указано>
Путь		Elsys Mobile
Тип		Виртуальное устройство 1

Рис. 2. Окно просмотра журнала аудита

Для каждой записи в журнале аудита указывается:

- Время возникновения события.
- Тип операции. Возможные значения:
  - *Доступ* — производился доступ к запрошенному объекту системы.
  - *Добавление* — произведено добавление объекта в систему.
  - *Изменение* — произведено изменение параметров объекта в системе.
  - *Удаление* — объект удалён из системы.
  - *Действие* — выполнено действие над объектом системы в терминах прикладной области.

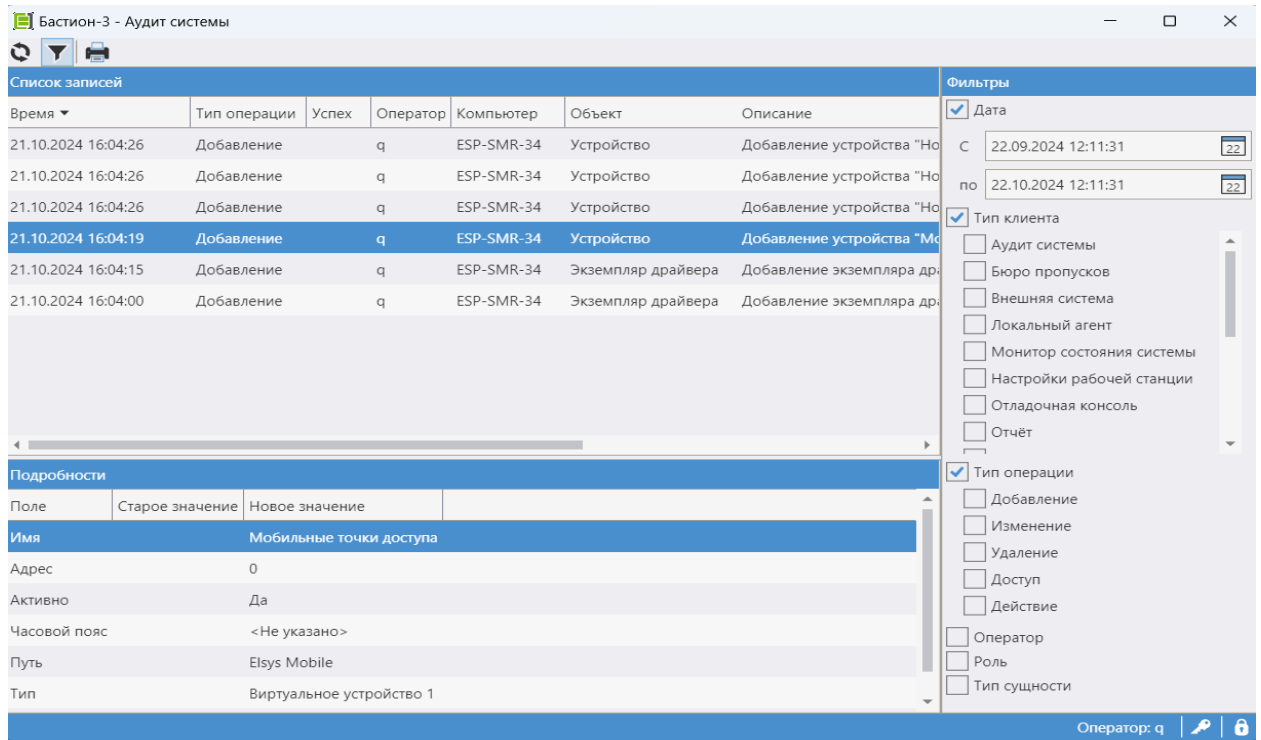
- *Оператор* — тот, кто произвел операцию. Здесь может быть указан как реальный оператор, так и технологическая учётная запись, от имени которой производилась операция.
- *Компьютер* — имя или адрес хоста, с которого производилась операция.
- *Объект* — тип объекта, над которым производилась операция.
- *Описание* — текстовое описание операции, произведённой с объектом. При наличии возможности, содержит текстовый идентификатор объекта.
- *Клиент* — клиентское приложение или модуль системы, через который была произведена операция.
- *Успех* — признак успешности завершения операции. Если поле пустое, это значит, что операция завершилась успешно. Для типа операции «Доступ» поле заполняется значениями «Успех» или «Отказ».
- *ID* — уникальный идентификатор сущности в системе, над которой произведена операция.
- *Доп. ID* — идентификатор дополнительной сущности, задействованной при выполнении операции.

Состав и взаимное расположение столбцов можно настроить, используя строку заголовка таблицы (можно включить / отключить отображение полей, настроить их порядок, ширину и сортировку).

В разделе «Подробности» журнала аудита версии 2024.3 добавлено отображение дополнительных полей, которые помогают однозначно идентифицировать сущность. Некоторые из этих полей дублируют информацию из столбца «Описание». Значения этих полей также будут нужны для передачи в сторонние системы через API.

В нижней части окна на Рис. 2 отображаются детали совершённой операции. Детали включают старые и новые значения изменённых параметров объекта.

Журнал аудита можно фильтровать. Для этого следует нажать кнопку «Фильтры» (Ctrl + Shift + F). После этого справа отобразится панель настройки фильтров (Рис. 3).



**Рис. 3. Панель настройки фильтров журнала аудита**

Фильтр можно настроить по всем значимым полям журнала аудита. После настройки фильтра следует нажать кнопку «Обновить» слева над таблицей с записями журнала.

## 5.2. Экспорт журнала аудита

В системе имеется возможность экспорта журнала аудита. Для выполнения экспорта следует предварительно настроить фильтр, после чего нажать кнопку «Печать» (Ctrl + P). При этом будет запрошен формат, в который следует выгрузить отображаемый журнал. Доступны следующие форматы: PDF, XLS, CSV, HTML, XML, ODT. После выбора формата следует нажать кнопку «Сгенерировать».

Печать журнала аудита возможна из экспортированных файлов во внешнем программном обеспечении.

## Приложения

### Приложение 1. История изменений

2024.1 (30.08.2024)

[+] Первая версия.