Seenaptec Access Platform

Руководство администратора и пользователя

Версия продукта: `v1.7.0`

Рынок поставки: Российская Федерация. Язык издания: русский.

Идентификатор редакции документа

Код формата `RF` соответствует стране поставки (Российская Федерация), код `RU` — языку издания. Метка времени — момент генерации данной сборки PDF (UTC), отдельная дата создания документа не приводится.

`SAP-ADMIN-RF-RU-20261020T134444Z`

ООО «Синаптек»

https://www.seenaptec.com

Оглавление

Глава 1. О документе **4**
1.1. Назначение . . . 4
1.2. Структура . . . 4
1.3. Обозначения . . . 4
1.4. Актуальность . . . 5

Глава 2. Назначение системы **5**
2.1. Объектная модель управления доступом . . . 5
2.2. Какие задачи позволяет решать система . . . 5
2.3. Основные возможности . . . 6

Глава 3. Ключевые понятия и словарь **6**
3.1. Модель системы . . . 6
3.2. Словарь терминов и сокращений . . . 8

Глава 4. Как устроена система **11**
4.1. Сервер и браузер . . . 11
4.2. Обзор взаимодействия сервисов . . . 11
4.3. Обработка запроса доступа . . . 13
4.4. Хранение данных . . . 14
4.5. Контур ОПС (Modbus TCP) . . . 14
4.6. Адреса веб-интерфейса и API . . . 14

Глава 5. Технические характеристики **15**
5.1. Платформа и состав поставки . . . 15
5.2. Минимальные системные требования . . . 16
5.3. Рабочее место оператора . . . 16
5.4. Периферия и протокол . . . 16
5.5. Типы подключения линий . . . 17
5.6. Лимиты и резервирование . . . 17
5.7. Хранилища данных . . . 17
5.8. REST API и OpenAPI . . . 18
5.9. Технологии разработки и внешние зависимости . . . 18

Глава 6. Установка **18**
6.1. Подготовка к установке . . . 18
6.2. Подготовка брокера MQTT . . . 18
6.3. Установка пакета . . . 19
6.4. Конфигурация . . . 19
6.5. Проверка после установки . . . 19
6.6. Активация системы . . . 20
6.7. Первый вход и смена пароля по умолчанию . . . 20
6.8. Включение HTTPS . . . 20
6.9. Обновление пакета . . . 20

Глава 7. Первоначальная настройка системы **21**
7.1. Создание линии OSDP . . . 21
7.2. Поиск и регистрация устройств в системе . . . 22
7.3. Создание объекта доступа . . . 22
7.4. Создание персоны и выдача пропуска созданной персоне . . . 22
7.5. Проверка доступа и записи события в журнале . . . 23
7.6. Дальнейшая настройка системы . . . 23

Глава 8. Общие принципы интерфейса **24**
8.1. Вход в систему . . . 24
8.2. Компоновка рабочего экрана системы . . . 24

8.3. Верхняя строка и рабочие области . . . 25
8.4. Левая зона: панели . . . 26
8.5. Правая зона: карточка . . . 27
8.6. Панель инструментов . . . 28
8.7. Панель «События» . . . 28
8.8. Проверка выполнения команд — принцип «команда принята — не значит выполнена» . . . 29
8.9. Общие правила поведения интерфейса . . . 29
8.10. Полезные рекомендации по работе с интерфейсом . . . 30

Глава 9. Обзор системы **30**
9.1. Как открыть страницу . . . 31
9.2. Карточки состояния . . . 31
9.3. Показатели и дополнительные секции . . . 32
9.4. Список «Требуют внимания» . . . 33
9.5. Автоматическое обновление . . . 33
9.6. Панель инструментов . . . 33

Глава 10. Настройка / Обслуживание **34**
10.1. Панель «Оборудование» . . . 34
10.2. Линии . . . 35
10.3. Поиск и добавление устройств . . . 37
10.4. Устройства . . . 37
10.5. Массовые операции . . . 40
10.6. События оборудования и режим «Пусконаладка (LIVE)» . . . 40
10.7. Панель «Отладка» . . . 41
10.8. Системные инструменты (панель инструментов) . . . 41
10.9. Оборудование ОПС (панели UniPOS) . . . 44

Глава 11. Объекты доступа **46**
11.1. Типы объектов доступа . . . 46
11.2. Панель «Объекты доступа» . . . 47
11.3. Карточка объекта доступа . . . 48
11.4. Правила доступа объекта . . . 50
11.5. Привязка к устройствам . . . 50
11.6. Каталог правил: условия, периметры АПБ и списание кратности . . . 51
11.7. Производственный календарь . . . 52
11.8. Панель «Текущий доступ» . . . 53
11.9. Панель «События» . . . 53
11.10. Каталог «Маршруты» . . . 53
11.11. Каталог «Учёт присутствия» . . . 53
11.12. Объекты ОПС (пожарные зоны D, A, P) . . . 53

Глава 12. Пропуска **55**
12.1. Ключевой принцип: пропуск — документ . . . 55
12.2. Панель «Пропуска» . . . 56
12.3. Персона . . . 58
12.4. Выдача пропуска и заявки . . . 59
12.5. Шаблоны доступов и ограниченная выдача . . . 60
12.6. Панель «Идентификаторы» . . . 60
12.7. Панель «События» . . . 64
12.8. Дополнительные поля персонала . . . 65
12.9. Импорт персонала из файла . . . 65
12.10. Авто-очистка . . . 66

Глава 13. Журналы **66**
13.1. Устройство журнала . . . 66
13.2. Панель «Журналы»: поиск по истории . . . 67

13.3. Карточка события . . . 68
13.4. Тревоги . . . 69
13.5. Контроль целостности журнала системы . . . 69
13.6. Архивация . . . 70
13.7. Просмотр архивов . . . 70
13.8. Отчёты . . . 71

Глава 14. Безопасность **71**
14.1. Модель полномочий . . . 72
14.2. Панель «Операторы» . . . 73
14.3. Роли . . . 74
14.4. Панель «Сессии» . . . 74
14.5. Секреты . . . 74
14.6. Настройки безопасности . . . 75
14.7. Панель «События»: аудит платформы . . . 75
14.8. АРМ считывателей . . . 76
14.9. Профили карт . . . 77

Глава 15. Типовые сценарии **79**
15.1. Выдать пропуск посетителю по шаблону . . . 79
15.2. Заявка на пропуск и её выпуск . . . 79
15.3. Изъять пропуск, заблокировать персону . . . 79
15.4. Посмотреть, кто открыл дверь . . . 80
15.5. Принять тревогу . . . 80
15.6. Подключение пожарной панели UniPOS и импорт конфигурации . . . 80
15.7. Сбросить присутствие АПБ или сессию шкафа . . . 81
15.8. Заменить неисправное устройство . . . 81
15.9. Обновить микропрограмму устройства . . . 81
15.10. Сделать резервную копию и восстановиться . . . 81
15.11. Выборка событий за период . . . 82
15.12. Проверить целостность журнала и архив . . . 82

Глава 16. Возможные неисправности **82**
16.1. Не открывается веб-интерфейс . . . 83
16.2. Интерфейс открывается, но данные не обновляются . . . 83
16.3. Линия в состоянии «Нет связи», «Возможно обрыв» или «Неактивно» . . . 83
16.4. Устройство не отвечает или найдено не полностью . . . 83
16.5. Доступ не выдан, хотя пропуск активен . . . 83
16.6. Событие доступа не появляется вовсе . . . 84
16.7. Резервирование не в норме . . . 84
16.8. Тревога «Нарушение целостности журнала» . . . 85
16.9. Забыт пароль администратора . . . 85
16.10. Панель ОПС и её устройства в состоянии «НЕТ СВЯЗИ» . . . 85

Глава 17. Лицензия: активация и жизненный цикл **86**
17.1. Как устроено лицензирование . . . 86
17.2. Ключ активации и два идентификатора . . . 86
17.3. Активация чистой системы . . . 86
17.4. Просроченная лицензия и продление . . . 87
17.5. Обновление ПО и переходный период 14 дней . . . 87
17.6. Перенос, восстановление и повторная активация . . . 87
17.7. Код для поддержки (отпечаток инсталляции) . . . 88
17.8. Восстановление доступа по коду поставщика . . . 89
17.9. Типичные ситуации . . . 90

Глава 18. Интеграция через API **90**
18.1. Спецификации и Swagger UI . . . 90

18.2. Авторизация внешней системы . . . 91
18.3. Модель прав . . . 91
18.4. Права для типовых задач интеграции . . . 91
18.5. Особенности, которые следует учитывать . . . 92

Глава 19. Реквизиты и контакты **92**
Инновационный центр «Сколково» . . . 92

Глава 1. О документе

1.1. Назначение

Данное руководство предназначено для установки, первоначальной настройки, администрирования и эксплуатации системы контроля доступа **Seenaptec Access Platform (SAP)**.

В документе описаны архитектура и основные понятия системы, работа с веб-интерфейсом, настройка оборудования и объектов доступа, управление пропусками, обработка событий и тревог, резервное копирование и восстановление системы, диагностика неисправностей и интеграция через REST API.

Руководство не заменяет:

- проектную и рабочую документацию объекта; руководства по монтажу и электрическому подключению оборудования;
- документацию на преобразователи RS-485 и периферийные устройства; спецификацию REST API;
- регламенты информационной безопасности эксплуатирующей организации.

Руководство адресовано администраторам и операторам системы. Ориентировочное соответствие задач и глав:

Читатель	Основные главы
Системный администратор	4–6, 9–10, 14, 17
Инженер эксплуатации	4–5, 7, 9–10, 16
Администратор доступа	3, 9, 11, 15
Оператор бюро пропусков	3, 9, 12, 15
Оператор безопасности	8–9, 13, 15
Интегратор	3–4, 18

При первом знакомстве с системой прочитайте часть I целиком: она задаёт терминологию для всех остальных глав.

1.2. Структура

- **Часть I. Знакомство с системой** (главы 1–5) — назначение, ключевые понятия и словарь, устройство системы, технические характеристики.
- **Часть II. Установка и первый запуск** (главы 6–7) — установка серверной части и пример первоначальной настройки системы.
- **Часть III. Интерфейс и повседневная работа** (главы 8–14) — общие принципы интерфейса, стартовая страница «Обзор системы» и описание рабочих областей: «Настройка / Обслуживание», «Объекты доступа», «Пропуска», «Журналы», «Безопасность».
- **Часть IV. Сценарии и справка** (главы 15–19) — типовые сценарии по шагам, возможные неисправности, лицензия и её жизненный цикл, интеграция через API, реквизиты и контакты.

1.3. Обозначения

- Знак → обозначает последовательный переход между рабочими областями, панелями, секциями или командами интерфейса.
- Названия рабочих областей, панелей, кнопок и других экранных элементов приводятся в кавычках и соответствуют надписям в интерфейсе: рабочая область «Пропуска», панель «Оборудование», кнопка «Сохранить».

- Команды, адреса, имена файлов и значения параметров набраны моноширинным шрифтом: `sudo systemctl status srv_ctrl.service`, `http://localhost:8080/app/`, `seenaptec_acs.yaml`.
- Текст в угловых скобках обозначает значения, которое необходимо заменить фактическими данными. Угловые скобки вводить не требуется. Пример: `http://<адрес-сервера>:8080/app/`
- Пошаговые процедуры пронумерованы; после шагов указан ожидаемый результат.
- Врезки, начинающиеся словами **«Для знакомых с классическими СКУД»**, сопоставляют модель системы с привычными понятиями классических СКУД — уровнями доступа, картотекой, группами точек.
- Иллюстрации сняты с эталонного стенда; адрес и порт сервера на снимках могут отличаться от ваших.

1.4. Актуальность

Руководство соответствует Seenaptec Access Platform (SAP) **версии v1.7.0**. Версия установленной системы отображается в карточке «Продукт» стартовой страницы «Обзор системы» (раздел 9.3). Процедуры, названия элементов интерфейса и заявленные функции проверены для этой версии продукта. Всё изложенное в основных главах реализовано и доступно в поставке этой версии.

При использовании другой версии обратитесь к руководству соответствующей редакции. Названия элементов интерфейса, доступные функции и порядок выполнения процедур могут отличаться.

Перед выполнением процедур сравните версию установленной системы с версией, указанной на титульной странице. Для других версий используйте соответствующую редакцию руководства.

Глава 2. Назначение системы

2.1. Объектная модель управления доступом

Seenaptec Access Platform (SAP) объединяет в едином веб-интерфейсе систему контроля и управления доступом (**СКУД**) и подсистему мониторинга и управления пожарной сигнализацией и автоматикой (**ОПС** на базе адресных панелей UniPOS серии IFS7000 по протоколу Modbus TCP). В центре модели управления доступом находится защищаемый объект доступа: дверь, турникет, серверный шкаф или другое место, доступ к которому требуется ограничивать и контролировать, а в контуре пожарной безопасности — логические пожарные зоны обнаружения (`D`), оповещения (`A`) и автоматики (`P`).

Физический защищаемый объект представлен в системе логической сущностью — **объектом доступа**. Тип объекта определяет его режимы работы, доступные правила и набор компонент оборудования, с которыми он взаимодействует. Благодаря этому права доступа и настройки поведения не зависят непосредственно от конкретного считывателя, реле или экземпляра устройства.

Настройка выполняется «от объекта»: сначала администратор определяет, что защищается и как должен функционировать объект доступа, затем назначает, кто, с помощью каких идентификаторов, когда и при каких условиях может получить доступ.

Права назначаются как на отдельные объекты доступа, так и на наборы объектов, объединённые тегами. Пропуск связывает персону, идентификаторы, сроки действия и разрешённые объекты, а настройки объекта задают его режим и дополнительные ограничения. Итоговое решение о доступе принимается на основе данных пропуска, состояния объекта и действующих правил.

Для объектов, поддерживающих длительный доступ, система ведёт сессии доступа. Например, работа инженера с серверным шкафом может фиксироваться как сессия с началом, подтверждениями активности и её завершением.

Решения о доступе, изменения настроек, действия операторов и тревоги сохраняются в журнале событий. Сохранённые записи не редактируются средствами веб-интерфейса и REST API; целостность последовательности событий может быть проверена средствами системы.

2.2. Какие задачи позволяет решать система

Seenaptec Access Platform (SAP) предоставляет администраторам и операторам сведения и инструменты для управления доступом, мониторинга пожарной сигнализации и автоматики, контроля оборудования и расследования событий в едином окне.

Система позволяет определить:

- какие линии, устройства и компоненты СКУД, а также приёмно-контрольные приборы, шлейфы и адресные устройства ОПС зарегистрированы, установлена ли с ними связь и есть ли технические неисправности;
- какие объекты доступа созданы, к каким типам они относятся, с каким оборудованием взаимодействуют и в каком режиме они работают, а также в каком состоянии находятся пожарные зоны ОПС (`D`, `A`, `P`);
- какие персоны, идентификаторы и пропуска зарегистрированы, на какие объекты предоставлен доступ и при каких временных интервалах, расписаниях и ограничениях он действует;
- какое решение было принято при попытке доступа и какие данные или правила стали причиной разрешения либо отказа в доступе;
- какие персоны числятся находящимися внутри контролируемых периметров и какие сессии доступа считаются активными;
- какие события доступа, аудита и технического состояния зарегистрированы и какие тревоги требуют обработки;
- кем, когда и какие изменения внесены в конфигурацию системы, права доступа и системные данные;
- какие учётные записи операторов/администраторов созданы, какие роли и полномочия им назначены и какие операторские сессии активны.

Подробное описание страницы «Обзор системы» и соответствующих рабочих областей приведено в главах 9–14.

2.3. Основные возможности

Текущая версия Seenaptec Access Platform поддерживает:

- **оборудование** — тип подключения OSDP через USB- и IP-шлюзы, автоматизированный поиск устройств с поддержкой Seenaptec SecureBus (SSB), изменение внутренних настроек устройств AGRG, тестирование работоспособности, защищённый канал OSDP Secure Channel, резервирование линий, обновление микропрограмм устройств AGRG, массовые операции;
- **объекты доступа** — типы «дверь (вход/кнопка)», «дверь (вход/выход)», «серверный шкаф (1 дверь)», «серверный шкаф (2 двери)», «турникет», «шлагбаум», указание используемых компонент устройств, режимы идентификации (карта, карта + PIN, подтверждение), правила доступа, периметры с запретом повторного прохода (АПБ), условия-блокировки, маршруты, маркировка зон присутствия, шаблоны времени доступа и производственный календарь, панель текущего доступа;
- **пожарную сигнализацию и автоматику (ОПС)** — подключение адресных пожарных панелей UniPOS серии IFS7000 по протоколу Modbus TCP, автоматический опрос состава системных блоков, шлейфов и адресных извещателей/модулей, импорт пользовательских имён и привязок из XML-конфигурации ПО UniPOS, мониторинг и оперативное управление зонами обнаружения (`D`), оповещения (`A`) и автоматики (`P`);
- **бюро пропусков** — персоны с дополнительными полями и фотографией, идентификаторы, пропуска с объектами и тегами, маршрутами, сроками, режимами времени и лимитами проходов, шаблоны доступов и идентификаторов, заявки на пропуск, автоматический жизненный цикл;
- **журналы и тревоги** — единый журнал событий доступа, аудита и техсостояния, карточка события с участниками и изменениями «было/стало», тревоги с обязательным комментарием при принятии, отчёты, архивация с контролем целостности;
- **безопасность самой системы** — операторы, роли с разграничением прав по доменам и уровням, сессии, хранилище секретов, аудит платформы;
- **интеграцию** — REST API для всех областей системы со спецификациями OpenAPI и встроенным Swagger UI.

Доступ в систему предоставляется посредством веб-интерфейса через браузер; отдельное рабочее место или настольное приложение не требуется. Установка серверной части описана в главе 6, устройство системы — в главе 4.

Глава 3. Ключевые понятия и словарь

Глава описывает модель данных системы — как связаны объекты доступа, субъекты, пропуска и оборудование — и приводит словарь терминов, используемых в руководстве и веб-интерфейсе.

3.1. Модель системы

В основе Seenaptec Access Platform (SAP) лежат две линии сущностей, которые встречаются в точке принятия решения о доступе.

Физическая часть (уровень оборудования):

- **Сервер** — центральный компонент системы; вычислительный узел, на котором работают сервисы платформы и хранятся данные системы. Сервер обменивается с устройствами по линиям OSDP через локальные или сетевые преобразователи RS-485.
- **Линия** — настроенный в системе канал обмена по протоколу OSDP между сервером и адресными устройствами на шине RS-485. Линия использует USB- или сетевой преобразователь и может включать основной и резервный контуры связи.
- **Устройство** — адресное периферийное OSDP-устройство, зарегистрированное на линии. Устройство предоставляет функциональные компоненты, которые могут быть использованы объектами доступа (двери, турникеты, серверные шкафы и т.д.).
- **Компонент устройства** — функциональная часть устройства, доступная в системе для привязки к объекту доступа: считыватель, контакт (вход), реле (выход) и т.д.
- **Приёмно-контрольный прибор (панель ОПС)** — адресная пожарная панель UniPOS серии IFS7000, подключаемая к серверу по протоколу Modbus TCP и объединяющая системные блоки (`БП`, `БИО`, `БРВ`) и кольцевые **шлейфы сигнализации (Loop)** с **адресными устройствами ОПС** (пожарными извещателями, модулями ввода-вывода и устройствами управления автоматикой `FPE`).

Логическая часть (уровень управления доступом и пожарной безопасностью):

- **Персона** — сущность системы, представляющая субъекта доступа: например, сотрудника или посетителя. С персоной могут быть связаны идентификаторы и пропуска.
- **Идентификатор** — значение или физический носитель, предъявляемый при запросе доступа и связанный с персоной, например карта или ПИН.
- **Пропуск** — электронный документ, определяющий права персоны на доступ. Пропуск содержит разрешённые объекты или теги, срок действия, временной профиль и ограничения.
- **Объект доступа** — логическое представление защищаемой точки, например двери, турникета или серверного шкафа. Тип объекта определяет его режимы, правила и функциональные слоты.
- **Тег** — именованная метка объекта доступа. Если тег указан в пропуске, право распространяется на объекты, которым назначен этот тег.
- **Зона ОПС (`D`, `A`, `P`)** — логическая зона пожарной панели, группирующая извещатели, оповещатели и исполнительные модули: зона обнаружения (`D`, Detection), зона оповещения (`A`, Alarm/Notification) и зона автоматики (`P`, Automation/Protection).

Связь оборудования с объектами доступа

Компоненты устройств привязываются к функциональным слотам объекта доступа. Например, к слотам двери могут быть привязаны считыватель, реле замка, кнопка выхода, датчик состояния двери и т.д.

Объект доступа и выданные на него права не зависят от конкретного экземпляра оборудования. При замене устройства объект, пропуска и история событий сохраняются; необходимо восстановить или подтвердить привязки компонентов.

Решение о доступе принимается в момент предъявления идентификатора на считывателе, привязанном к объекту доступа. Система находит владельца идентификатора, проверяет его действующие пропуска, права на объект (напрямую или по тегу), временной режим, а также правила самого объекта — условия, запрет повторного прохода, требование подтверждения — и разрешает либо запрещает доступ. Результат вместе с причиной фиксируется в журнале событий.

Схема связей

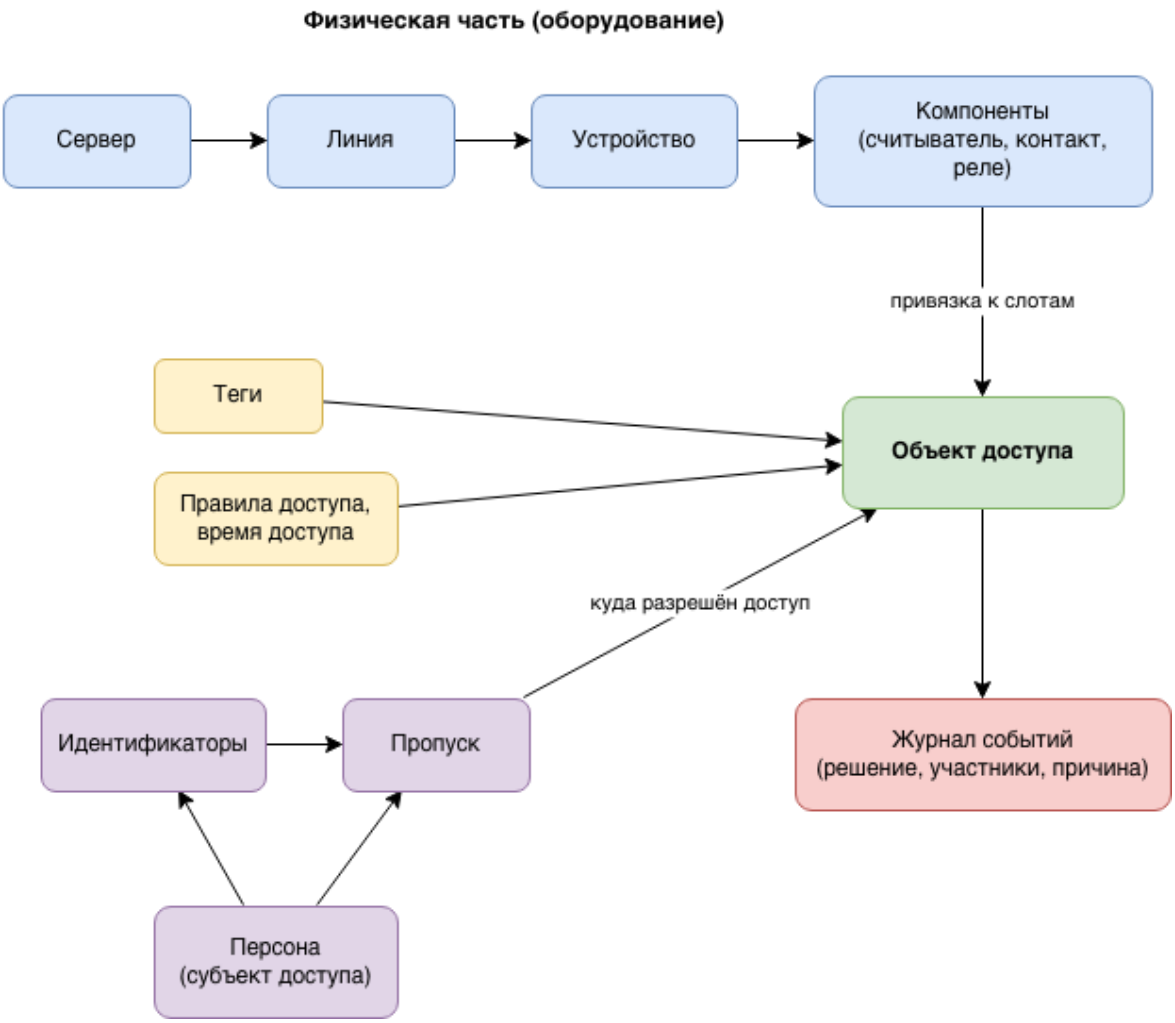


Рисунок 3.1 — Общая схема связей

Правила и ограничения на стороне объекта

Помимо прав, выданных пропуском, на решение влияют настройки объекта доступа:

- **время доступа** — три профиля длительности (нормальное, сокращённое, расширенное время) и производственный календарь;
- **правила доступа** — условия, которые требуется иметь или не иметь субъекту (например, допуск, инструктаж), и периметры с запретом повторного прохода (АПБ);
- **режим идентификации** — только карта, карта + PIN, карта + подтверждение (двойной контроль).

Операторы и персоны

Пользователи веб-интерфейса учитываются в системе как **операторы**. Для каждого оператора назначаются роль и соответствующие полномочия.

Оператор и персона являются разными сущностями. Например, сотрудник может одновременно работать в веб-интерфейсе и пользоваться пропуском для прохода через дверь, однако его учётная запись оператора и запись персоны хранятся и обрабатываются отдельно.Действия операторов регистрируются в журнале аудита.

3.2. Словарь терминов и сокращений

Термин	Описание
Аварийное открывание	Открывание объекта доступа самим устройством AGRG при потере связи с сервером: по кнопке аварийного открывания или по аварийным картам. Настраивается в карточке объекта доступа (раздел 11.3).
Адресное устройство ОПС	Пожарный извещатель (дымовой, тепловой, комбинированный, газовый, ручной), модуль ввода-вывода или устройство управления автоматикой (`FPE`) на шлейфе сигнализации или встроенном блоке (`БИО`/`БРВ`).
АПБ (запрет повторного прохода)	Правило периметра: субъект, вошедший в периметр, не может войти повторно, не выйдя (и наоборот). Режим может быть жёстким (запрет) или мягким (только запись в журнал).
АРМ считывателя	Автоматизированное рабочее место с настольным считывателем карт: программа-агент на компьютере оператора, подключённая к серверу. Применяется для чтения, эмиссии и инициализации карт (раздел 14.8).
Аудит	Категория журнала: события изменения данных и настроек — кто, что и когда изменил, с перечнем полей «было/стало».
Время доступа	Временной интервал, в течение которого на объекте доступа разрешён доступ. У каждого объекта есть нормальное, сокращённое и расширенное время доступа; применяемый профиль задают пропуск и шаблон времени объекта.
Журнал событий	Упорядоченная по времени лента записей о событиях доступа, аудита и технического состояния. Сохранённые записи не редактируются и защищены хешированием; единственный изменяемый слой — операторские метки.
Заявка на пропуск	Черновик пропуска: резервирует номер и данные, но не даёт доступа до выпуска пропуска. Поддерживает разделение обязанностей: одни операторы готовят заявки, а бюро пропусков подтверждает пропуск и определяет объекты доступа.
Зона ОПС (`D`, `A`, `P`)	Логическая зона панели ОПС: зона обнаружения (`D`, Detection), зона оповещения (`A`, Alarm/Notification) и зона автоматики (`P`, Automation/Protection).
Идентификатор	Карта, PIN-код или другой предъявляемый код, по которому система определяет субъекта доступа. Учитывается в панели «Идентификаторы» независимо от того, выдан ли пропуск.
Карточка	Правая часть рабочей области с подробностями выбранной сущности: сервера, линии, устройства, объекта доступа, пропуска, персоны или записи журнала.
Компонент устройства	Функциональная часть устройства — считыватель, контакт (вход), реле (выход), — которую можно привязать к слоту объекта доступа.
Линия	Канал связи OSDP между сервером и группой устройств, объединённых общей физической линией RS-485; подключается через USB- или сетевой преобразователь.
Маршрут	Именованный набор проходных объектов доступа. Назначенный на пропуск, маршрут даёт доступ ко всем своим точкам без разделения на вход и выход. Каталог маршрутов — в разделе 11.10.
Метка	Операторская пометка на событии журнала для расследований. Добавление и снятие метки само фиксируется в журнале.
Объект доступа	Место, где контролируется доступ, — дверь, турникет, шкаф, зона хранения. В системе — логическая сущность из функциональных слотов, поведение которой определяет тип объекта доступа; на объект назначаются права и правила.
Оператор	Учётная запись для работы с веб-интерфейсом системы. Полномочия оператора определяются его ролью.
Панель	Область в левой части рабочей области со списком, деревом или лентой: например, панель «Оборудование» или панель «События».
Панель инструментов	Выдвижная область у правого края экрана со справочниками и настройками текущей рабочей области: шаблоны, правила, отчёты, системные операции. Открывается кнопкой с шестерёнкой в правом нижнем углу.
Периметр	Именованная зона для правил АПБ и учёта присутствия: считыватели объектов задают входы и выходы периметра, система отслеживает присутствие субъектов внутри.
Персона	Запись о субъекте доступа: сотрудник, посетитель или носитель «на предъявителя». Персона может иметь идентификаторы, пропуска, фотографию и дополнительные поля.
Правило доступа	Условие или ограничение, назначаемое объекту доступа: требование наличия либо отсутствия условия у субъекта или участие объекта в периметре АПБ.

Термин	Описание
Приёмно-контрольный прибор (панель ОПС)	Адресная пожарная панель UniPOS серии IFS7000, подключаемая по протоколу Modbus TCP. Объединяет системные блоки (`БП`, `БИО`, `БРВ`), кольцевые шлейфы сигнализации и логические пожарные зоны.
Производственный календарь	Календарь рабочих, выходных и праздничных дней, учитываемый в шаблонах времени доступа.
Профиль карт	Именованное описание защищённой зоны карты: технология (MIFARE Classic/Plus, DESFire), ключи чтения и записи из хранилища секретов, расположение кода. Библиотека профилей — в рабочей области «Безопасность» (раздел 14.9).
Пропуск	Набор условий доступа, назначаемый персоне: объекты доступа, теги или маршруты, срок действия, время доступа, разрешённые идентификаторы и ограничения — например, лимит проходов.
Рабочая область	Раздел веб-интерфейса верхнего уровня. Всего их пять: «Пропуска», «Объекты доступа», «Журналы», «Настройка / Обслуживание», «Безопасность». В текущей версии интерфейса рабочие области названы «инструментами».
Роль	Набор полномочий оператора: уровни прав по доменам системы (оборудование, объекты доступа, персоны и пропуска, безопасность, журнал).
Секрет	Именованное защищённое значение в хранилище рабочей области «Безопасность»: пароль резервной копии, ключ OSDP, ключ карты, сертификат HTTPS. Значение секрета нельзя прочитать из интерфейса — его можно только использовать.
Сервер	Центральный узел системы; в дереве оборудования — корневая запись, к которой относятся линии.
Сессия доступа	Длительный эпизод доступа с началом, подтверждениями и завершением — прежде всего для шкафов: кто открыл, каким пропуском, когда было последнее подтверждение. Активные сессии видны в панели «Текущий доступ».
Сессия оператора	Период работы оператора в веб-интерфейсе от входа до выхода; при длительном отсутствии активности завершается автоматически. Активные сессии видны в рабочей области «Безопасность».
СКУД	Система контроля и управления доступом.
Слот (функциональный слот)	Функциональный элемент объекта доступа — считыватель, замок, датчик, кнопка. Состав слотов задаёт тип объекта доступа; к слоту привязывается компонент устройства. Слоты бывают обязательными и необязательными.
Событие	Единичная запись журнала: попытка доступа, изменение настроек, смена состояния оборудования, действие сервиса или оператора.
Субъект доступа	Субъект — человек, транспортное средство или другой объект, — в отношении которого выполняется контроль доступа; представлен в системе персоной.
Тег	Метка, объединяющая несколько объектов доступа для назначения прав: пропуску можно выдать доступ по тегу вместо перечисления каждого объекта.
Текущий доступ	Панель рабочей области «Объекты доступа»: кто сейчас находится в периметрах и какие сессии доступа открыты.
Тип объекта доступа	Набор слотов, правил их взаимодействия и режимов работы, определяющий поведение объекта доступа. Тип выбирается при создании объекта; перечень типов — в разделе 11.1.
Тревога	Событие журнала, требующее реакции оператора. Активные тревоги показываются колокольчиком в верхней строке интерфейса и принимаются с обязательным комментарием.
Условие	Именованный признак субъекта, используемый правилами доступа: условие можно устанавливать при проходе, требовать его наличие или отсутствие.
Устройство (периферийное устройство)	Адресное периферийное устройство на линии OSDP; состоит из компонентов — считывателей, контактов, реле. Решения о доступе устройство не принимает — их принимает сервер.
Шаблон доступа	Заготовка пропуска: правила периода и срока действия, объекты, теги, время доступа и кратность — для быстрой выдачи однотипных пропусков.
Шаблон идентификатора	Заготовка для выпуска карт: вид карты и правило срока действия.
Шлейф сигнализации (Loop)	Кольцевая адресная линия панели ОПС, объединяющая извещатели и модули ввода-вывода (до 210 адресных устройств на шлейф).

Термин	Описание
Эмиссия идентификатора	Запись кода в защищённую зону карты на настольном считывателе с одновременным созданием идентификатора в системе (раздел 12.6).
MQTT	Протокол обмена сообщениями между сервисами платформы. Требуется отдельный брокер MQTT в среде установки.
OpenAPI / Swagger UI	Машиночитаемое описание REST API и интерактивная страница для просмотра и вызова методов; в поставке: `http://<хост>:8080/api-docs/`.
OSDP	Open Supervised Device Protocol — открытый протокол обмена с периферийными устройствами контроля доступа; разработан ассоциацией SIA, работает поверх RS-485.
OSDP Secure Channel	Защищённый (шифрованный) канал обмена с устройством по OSDP; поддерживается установка и ротация ключей.
REST API	Программный интерфейс поверх HTTP для настройки, данных доступа и журнала; см. главу 18.
Seenaptec Access Platform	Платформа контроля доступа, которую описывает это руководство.
SQLite	Встраиваемая СУБД в виде файлов `*.sqlite`; используется в поставке как хранилище данных — отдельный сервер базы данных не нужен.
SSB (Seenaptec SecureBus)	Проприетарный режим работы с поддерживаемыми OSDP-устройствами: автоматизированный поиск, назначение адресов и согласование скорости линии.
systemd	Подсистема управления службами Linux; платформа запускается как служба `srv_ctrl.service`.

Глава 4. Как устроена система

4.1. Сервер и браузер

Серверные компоненты Seenaptec Access Platform (SAP) устанавливаются на рабочую станцию под управлением рекомендованной версии ОС Linux. Требования к рабочей станции приведены в разделе 5.2.

Операторы работают с системой через поддерживаемый веб-браузер. Установка отдельного клиентского приложения не требуется: веб-приложение загружается с сервера и выполняется в браузере оператора. Требования к рабочему месту приведены в разделе 5.3.

Все операторы используют единый адрес веб-интерфейса. Доступные рабочие области и операции определяются назначенными ролями и полномочиями. Адреса и порты системы по умолчанию приведены в разделе 4.6.

Для эксплуатации системы с удалённых рабочих мест рекомендуется использовать HTTPS. Порядок включения HTTPS приведён в разделе 6.8.

Серверные компоненты — сервисы — взаимодействуют с периферийным оборудованием СКУД и панелями ОПС, реализуют основную логику платформы и хранят конфигурацию, данные доступа, данные пожарной сигнализации и журнал событий. Состав сервисов описан в разделе 4.2, порядок формирования решения о доступе — в разделе 4.3, а работа контура ОПС — в разделе 4.5.

4.2. Обзор взаимодействия сервисов

Платформа состоит из нескольких сервисов, каждый из которых отвечает за свою часть работы. Все они устанавливаются одним пакетом и запускаются автоматически.

Сервис	Назначение
`srv_ctrl`	Управление запуском: читает конфигурацию, запускает сервисы, следит за состоянием, перезапускает при сбоях. В systemd — `srv_ctrl.service`.

Сервис	Назначение
`scud-server`	Центральный сервис («Сервер приложения»): веб-интерфейс, REST API, журнал, конфигурация, данные доступа и подсистемы ОПС, OpenAPI.
`srv_osdp`	Линия OSDP («Сервер OSDP линии N»): опрос, поиск, команды, события. На линию — свой экземпляр; при резервировании линия обслуживается одним экземпляром, работающим с двумя портами кольца (основным и резервным).
`srv_ops`	Панель ОПС («Сервер ОПС панели N»): опрос адресной пожарной панели UniPOS серии IFS7000 по протоколу Modbus TCP, автоопределение состава, управление зонами и устройствами, передача состояний и событий. На каждую включённую панель ОПС запускается свой экземпляр.
`srv_behavior`	Логика объектов доступа («Сервер поведений»): решения о доступе, сессии, периметры, состояния.
`srv_discover`	Поиск сетевых преобразователей RS-485 («Сервер обнаружения устройств») при настройке линий.

Рабочими сообщениями — событиями, командами и состояниями — сервисы обмениваются через **брокер MQTT**. Брокер — внешняя зависимость: он не входит в пакет платформы и разворачивается в среде установки отдельно (типовой вариант — Eclipse Mosquitto). Браузер с сервисами по MQTT не взаимодействует: веб-интерфейс получает данные от `scud-server` по HTTP.

Обзорная схема

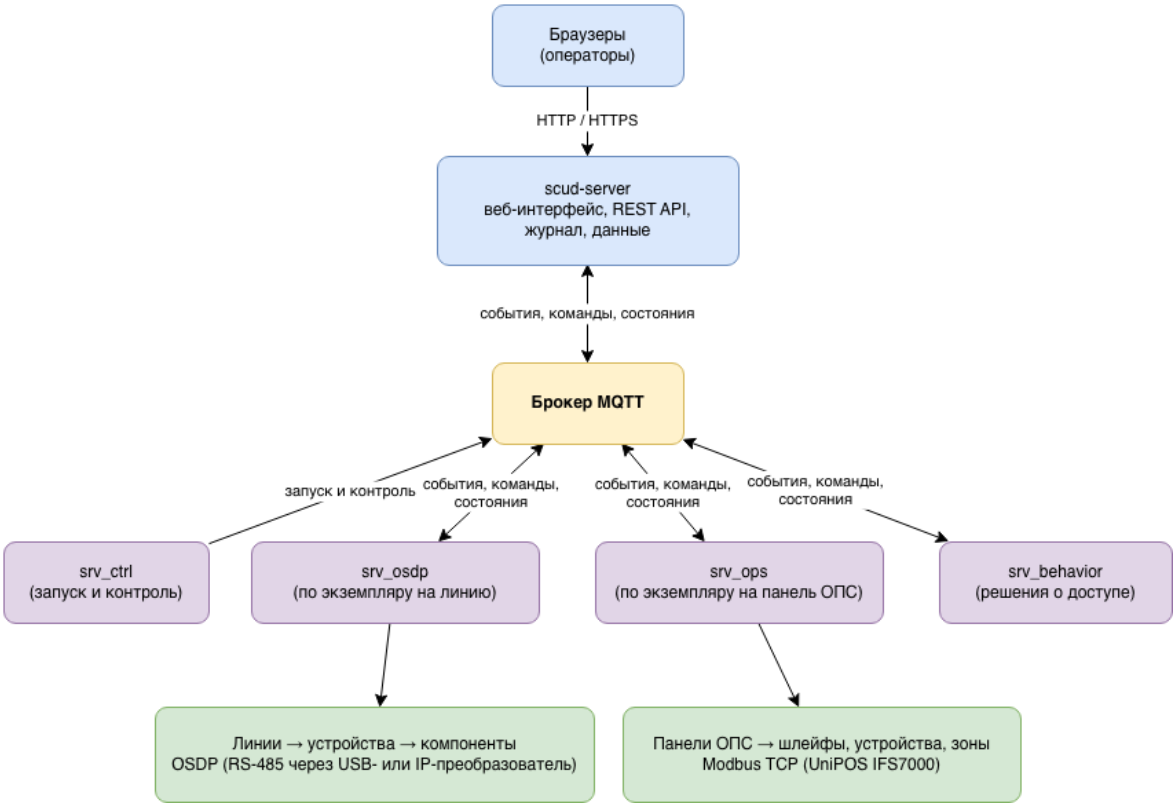


Рисунок 4.2 — Обзорная диаграмма взаимодействия сервисов

Схема намеренно обзорная: для повседневной работы достаточно понимать, что браузер общается с центральным сервисом, а тот через внутренний обмен управляет линиями и получает события. Состояние сервисов видно в веб-интерфейсе — в секции «Управление сервисами» рабочей области «Настройка / Обслуживание».

4.3. Обработка запроса доступа

Ниже описан типовой сценарий запроса доступа при предъявлении карты.

Считыватель получает код карты, после чего периферийное устройство передаёт событие по линии OSDP экземпляру `srv_osdp`, обслуживающему эту линию. По конфигурации считывателя система определяет связанный объект доступа и направление запроса.

`srv_osdp` передаёт сообщение о запросе через брокер MQTT сервису `srv_behavior`. Сервис последовательно:

1. определяет персону, связанную с идентификатором;
2. проверяет состояние персоны и идентификатора;
3. находит подходящие действующие пропуска;
4. проверяет право доступа на объект напрямую или через тег;
5. проверяет срок действия, расписание и ограничения пропуска;
6. применяет режим и правила объекта, включая условия доступа, АПБ и требование подтверждения.

По результату проверки `srv_behavior` формирует решение: разрешить или запретить доступ. Если требуется дополнительный фактор, система ожидает его предъявления и формирует окончательное решение после завершения всех обязательных проверок.

Решение передаётся через брокер MQTT экземпляру `srv_osdp`. При положительном решении `srv_osdp` отправляет периферийному устройству команду, соответствующую типу и режиму объекта.

Сессия двери и групповой проход. У двери с датчиком положения открытие створки создаёт сессию: пока створка открыта, предъявления карт других персон регистрируются как их собственные проходы — с полной проверкой

прав, учётом АПБ и кратности, но без повторного срабатывания замка; PIN при такой регистрации не запрашивается, поскольку дверь уже открыта. Предъявление без права на объект в открытой сессии фиксируется критическим событием «Доступ запрещён» с тревогой «Проход без разрешения». Если дверь открыта по подтверждению (двойной контроль или сопровождение гостя), сессия запоминает подтверждающего: следующие персоны с признаком «Требует подтверждения» и гости того же сопровождающего регистрируются без нового подтверждения, а предъявление персоны, которую подтверждающий сессии не покрывает, отклоняется с той же тревогой. Повторное предъявление карты самого подтверждающего регистрирует его собственный проход.

Команды оператора из веб-интерфейса выполняются **асинхронно**. Принятая команда — ещё не выполненная операция; фактический результат подтверждается изменением состояния периферических устройств или событием в журнале.

Решение, его причина и связанные участники сохраняются в журнале событий. Подтверждения выполнения команды и изменения состояния объекта регистрируются отдельными событиями, если соответствующие данные поступили от оборудования.

Поведение системы при неизвестном идентификаторе, отсутствии действующего пропуска, недоступности серверных сервисов или потере связи с устройством приведено в главе 16.

4.4. Хранение данных

Данные системы хранятся на сервере в файлах встраиваемой СУБД **SQLite** — отдельный сервер базы данных устанавливать не нужно. Файлы разделены по областям: конфигурация оборудования и объектов доступа, подсистема ОПС (панели, шлейфы, устройства и зоны), персоны и пропуска, журнал событий, операторы и параметры безопасности, оперативное состояние доступа. Такое разделение упрощает резервное копирование и перенос: штатный механизм резервного копирования (глава 10) сохраняет и восстанавливает эти файлы. Журнал событий устроен по принципу «только добавление»: сохранённые записи не изменяются, что делает его пригодным для аудита и контроля целостности (глава 13).

4.5. Контур ОПС (Modbus TCP)

Подсистема пожарной сигнализации и автоматики (**ОПС**) работает параллельно с контуром СКУД и обслуживается отдельными экземплярами сервиса **`srv_ops`** (в интерфейсе — **«Сервер ОПС панели N»**). Центральный сервис запускает по одному изолированному процессу `srv_ops` на каждую включённую панель ОПС UniPOS серии IFS7000.

Работа контура ОПС строится в четыре этапа:

1. **Подключение и автоопределение состава.** Экземпляр `srv_ops` устанавливает соединение с панелью UniPOS по протоколу Modbus TCP (по умолчанию порт `502`, `Unit ID = 255`), считывает паспорт прибора функцией `0x2B / 0x0E` (модель `7000M`, `7000-1MC` или `7000M-1L`, серийный номер, версия прошивки) и при опросе состава автоматически определяет установленные системные блоки (`БП`, `БИО`, `БРВ`), кольцевые шлейфы, адресные устройства и настроенные в приборе зоны (`D`, `A`, `P`).
2. **Непрерывный опрос состояний.** С заданным интервалом (по умолчанию 1000 мс) `srv_ops` опрашивает регистры состояния системных блоков, шлейфов, адресных устройств и зон функциями `0x03` / `0x04`, а при появлении новых записей в памяти прибора вычитывает текстовый архив панели функцией `0x14`.
3. **Публикация состояний и событий через MQTT.** При изменении битовых флагов (пожарная тревога, предтревога, предупреждение или пуск оповещения и автоматики, неисправность, обход, режим теста, потеря связи) `srv_ops` публикует обновлённое состояние и событие-дельту через брокер MQTT в `scud-server`. При обрыве связи по TCP панель и все её дочерние элементы в интерфейсе переходят в достоверный статус `НЕТ СВЯЗИ`.
4. **Единый журнал и разграничение прав.** Центральный сервис `scud-server` принимает состояния и события от `srv_ops`, обновляет карточки в рабочих областях «Настройка / Обслуживание» (раздел 10.9), «Объекты доступа» (раздел 11.12) и в «Обзоре системы» (глава 9), записывает события в единый журнал с категорией «ОПС» (глава 13) и проверяет полномочия оператора с учётом потолка прав на подсистему ОПС (глава 14).

4.6. Адреса веб-интерфейса и API

Веб-интерфейс и служебные ресурсы Seenaptec Access Platform (SAP) доступны через сервер `scud-server`.

В адресах ниже замените `<адрес-сервера>` IP-адресом сервера. Угловые скобки вводить не требуется. При обращении непосредственно с сервера можно использовать имя `localhost`.

По умолчанию для HTTP используется порт `8080`.

Ресурс	Назначение	Адрес по умолчанию
Веб-интерфейс	Работа операторов и администраторов	`http://<адрес-сервера>:8080/app/`
Проверка готовности	Проверка доступности серверного приложения средствами мониторинга или диагностики	`http://<адрес-сервера>:8080/health`
Swagger UI	Интерактивный просмотр и вызов методов REST API	`http://<адрес-сервера>:8080/api-docs/`
Документация API	Спецификации OpenAPI и сопутствующая документация	`http://<адрес-сервера>:8080/docs/`

Для первоначальной настройки в доверенной сети может использоваться HTTP. Для постоянной эксплуатации и подключения с удалённых рабочих мест следует настроить HTTPS.

После включения HTTPS веб-интерфейс по умолчанию доступен по адресу:

`https://<адрес-сервера>:8443/app/`

Доступные ресурсы, порты и правила аутентификации зависят от конфигурации сервера. Не предоставляйте служебные страницы `/health`, `/api-docs/` и `/docs/` из недоверенных сетей без предусмотренной защиты и сетевых ограничений.

Порядок настройки HTTPS приведён в разделах 6.8 и 10.8.

Глава 5. Технические характеристики

Сводка для инженеров и технических специалистов. Пошаговые процедуры установки — в главе 6, пусконаладки — в главах 7 и 10.

5.1. Платформа и состав поставки

Seenaptec Access Platform (SAP) устанавливается на рабочую станцию под управлением поддерживаемой версии Linux. Программные компоненты поставляются в виде пакета .deb для архитектур amd64 и arm64.

Параметр	Значение
Операционная система	Linux семейства Debian, использующих `systemd` и пакетный менеджер APT (Debian, Ubuntu, Astra Linux, Linux Mint)
Формат пакета установки	`.deb`
Поддерживаемые архитектуры	`amd64`, `arm64`
Система управления службами	`systemd`
Основная служба	`srv_ctrl.service`
Программные файлы	`/opt/skd`
Файл конфигурации	`/etc/skd/seenaptec_acs.yaml`
Учётные данные сервисов	`/etc/skd/credentials/`
Данные системы	`/var/lib/skd`
Порт HTTP по умолчанию	`8080`
Порт HTTPS по умолчанию	`8443`, если HTTPS включён
Внешняя зависимость	Брокер MQTT, устанавливаемый отдельно

Каталог `/opt/skd` содержит программные файлы поставки. Конфигурация, учётные данные сервисов и данные системы хранятся отдельно от программных файлов.

При штатном обновлении пакета сохраняются:

- файл конфигурации `/etc/skd/seenaptec_acs.yaml`;
- учётные данные из `/etc/skd/credentials/`;
- данные из `/var/lib/skd`.

Перед обновлением создайте резервную копию данных и конфигурации в соответствии с разделом, посвящённым резервному копированию и восстановлению.

5.2. Минимальные системные требования

Минимальная конфигурация сервера для развёртывания платформы:

Компонент	Минимальные требования
Процессор (ARM) (Протестировано)	4 ядра уровня Cortex-A76, 2,4 ГГц, 64-бит ARMv8 — например Broadcom BCM2712 (Raspberry Pi 5)
Процессор (x86)	Intel Core i3 современных поколений, 4 ядра, или сопоставимый AMD (например, Ryzen 3)
Оперативная память	2 ГБ
Диск	8 ГБ (Размер данных под журнал зависит от политики архивирования)
Сеть	Ethernet 10/100 МБит. Сеть обязательна: система клиент-серверная — веб-интерфейс и обмен через брокер MQTT работают по сети

5.3. Рабочее место оператора

Параметр	Значение
Рабочее место	Браузер; установка клиентского ПО не требуется
Поддерживаемые браузеры	Google Chrome, Firefox, Яндекс Браузер, Microsoft Edge, Safari (актуальные выпуски)
Протокол	HTTP; HTTPS с загрузкой сертификата из веб-интерфейса

5.4. Периферия и протокол

Элемент	Описание
Протокол устройств	OSDP; часть функций требует расширения - Seenaptec Secure Bus (SSB)
Защита обмена	OSDP Secure Channel: первичное подключение по ключу по умолчанию (SCBK-D), установка рабочего ключа, режим автоматической ротации ключей (зависит от оборудования)
Seenaptec SecureBus (SSB)	Автоматизированный поиск совместимых AGRG OSDP-устройств на линии: обнаружение по серийным номерам, назначение адресов, согласование скорости (зависит от оборудования), настройки оборудования
Обновление микропрограмм	Запись микропрограммы OSDP-устройства из веб-интерфейса (OSDP File Transfer), с проверкой контрольной суммы и версии после записи
Протокол и оборудование ОПС	**Modbus TCP** (порт `502` по умолчанию); адресные приёмно-контрольные приборы **UniPOS серии IFS7000** (`7000M`, `7000-1MC`, `7000M-1L`)
Зоны и конфигурация ОПС	Логические зоны обнаружения (`D`), оповещения (`A`) и автоматики (`P`); автоопределение состава по Modbus (`0x2B/0x0E`, `0x03`, `0x04`, `0x14`) и импорт конфигурации `.xml` из ПО UniPOS

5.5. Типы подключения линий

Для подключения оборудования могут использоваться следующие типы адаптеров:

Тип в интерфейсе	Подключение
`USB->485`	Локальный USB-преобразователь RS-485 (последовательный порт сервера)
`TCP->485 (Другой)`	TCP-подключение к произвольному сетевому преобразователю Ethernet–RS-485, с поддержкой TCP server режима работы.
`TCP->485 (DR134)`	TCP-подключение к преобразователю модели USR-DR134 с учётом его особенностей

Для поиска сетевых преобразователей в локальной сети предусмотрен отдельный инструмент «Настройка сетевых адаптеров» (глава 10).

5.6. Лимиты и резервирование

Показатель	Значение
Максимум устройств на одной линии	64 (адреса OSDP 0–63)
Сервис на линию	Один экземпляр `srv_osdp`; при резервировании тот же экземпляр обслуживает оба порта кольца (основной и резервный)
Резервирование линии	Основной и резервный порт (контур связи) для одного участка RS-485; переключение при разрыве шины или отказе преобразователя/канала
Кластер и шлейфы панелей ОПС	До 8 панелей UniPOS IFS7000 в кластере (`Номер панели в кластере` 1–8); до 2/4 шлейфов сигнализации на панель (до 10 на модульных `7000M`), до 210 адресных устройств на шлейф
Сервис на панель ОПС	Один изолированный экземпляр `srv_ops` («Сервер ОПС панели N») на каждую включённую панель

Резервирование реализуется путем подключения к обоим концам физической линии 485 двух адаптеров одного типа. Резервирование включается автоматически, когда в параметрах линии указан резервный порт. Оба порта обслуживает один экземпляр `srv_osdp`: в норме опрос идёт через основной порт, при разрыве шины устройства каждого сегмента переводятся на доступный им порт. Подробное описание состояний резервирования — в главе 10.

5.7. Хранилища данных

Данные хранятся в файлах SQLite в каталоге данных сервера, с разделением по областям:

Область	Содержимое
Конфигурация	Сервер, линии, устройства, объекты доступа, привязки, шаблоны
Подсистема ОПС	Пожарные панели UniPOS, системные блоки, шлейфы, адресные устройства, зоны (`D`, `A`, `P`), импортированные имена из `.xml`
Данные доступа	Персоны, идентификаторы, пропуска, теги, шаблоны доступов
Журнал	События доступа, аудита и техсостояния (только добавление)
Операторы и безопасность	Учётные записи, роли, сессии, секреты
Оперативное состояние	Присутствие в периметрах, сессии, счётчики

Резервное копирование и восстановление выполняются штатным механизмом из веб-интерфейса (глава 10); резервная копия включает файлы данных и конфигурацию.

5.8. REST API и OpenAPI

Ресурс	Адрес по умолчанию (браузер на сервере)
Проверка готовности	`http://localhost:8080/health`
Веб-интерфейс	`http://localhost:8080/app/`
OpenAPI, интерактивно (Swagger UI)	`http://localhost:8080/api-docs/`
Спецификации и документация API	`http://localhost:8080/docs/`

Доступны REST API оборудования, данных доступа, журнала и безопасности; доступ внешних систем разграничивается той же ролевой моделью, что и доступ операторов (глава 18). Для обращения с другого компьютера замените `localhost` на IP-адрес или DNS-имя сервера; номер порта может отличаться, если он изменён в конфигурации.

5.9. Технологии разработки и внешние зависимости

Серверные компоненты Seenaptec Access Platform (SAP) разработаны на языке Go. Низкоуровневая реализация протокола OSDP выполнена на языке C.

Сервисы платформы запускаются и контролируются системой инициализации `systemd`.

Для обмена командами, событиями и состояниями между сервисами требуется внешний брокер MQTT. Брокер не входит в установочный пакет Seenaptec Access Platform и устанавливается отдельно. Он может работать на сервере платформы или на другом доступном сетевом узле.

Требования к брокеру MQTT и порядок его подготовки приведены в разделе 6.2

Глава 6. Установка

Глава описывает установку серверной части Seenaptec Access Platform (SAP) на Linux, проверку работоспособности, активацию системы и первый вход в веб-интерфейс. Технические характеристики поставки приведены в главе 5; пусконаладка оборудования — в главах 7 и 10; жизненный цикл лицензии — в главе 17.

6.1. Подготовка к установке

Перед установкой системы подготовьте:

- рабочую станцию аппаратной архитектуры `amd64` или `arm64`, соответствующую требованиям раздела 5.2 с поддерживаемым дистрибутивом Linux, использующим `systemd`и поддерживающим установку пакетов формата DEB;
- учётную запись пользователя с возможностью выполнять команды через `sudo`;
- установочный пакет Seenaptec Access Platform (SAP) для архитектуры сервера;
- ключ активации, полученный у поставщика системы (без ключа активации серверные компоненты можно установить и запустить, однако вход в веб-интерфейс и настройка системы будут недоступны);
- работающий брокер MQTT, доступный в сети организации;
- рабочее место оператора/администратора с поддерживаемым веб-браузером для первоначальной настройки системы.

Брокер MQTT является внешней зависимостью и не входит в установочный пакет платформы. Он может работать на сервере Seenaptec Access Platform (SAP) или на отдельном сетевом узле. Требования к брокеру и порядок его подготовки приведены в разделе 6.2.

Для подключения оборудования потребуются USB–RS-485 или Ethernet–RS-485-преобразователи. Их можно подключить после установки пакетов платформы, на этапе пусконаладки.

6.2. Подготовка брокера MQTT

Сервисы платформы обмениваются рабочими сообщениями через брокер MQTT (глава 4). Разверните брокер по правилам вашей организации или средствами дистрибутива Linux; типовой вариант — Eclipse Mosquitto:

```
sudo apt install mosquitto
```

Брокер может работать как на том же сервере (типовой адрес `tcp://localhost:1883`), так и на отдельном узле. Убедитесь, что брокер запущен и принимает соединения от хоста, на который устанавливается платформа.

6.3. Установка пакета

Установите пакет под архитектуру сервера:

```
sudo apt install ./seenaptec-acs_<версия>_amd64.deb
```

Пакет размещает файлы и регистрирует службу так:

Что	Где
Программные файлы (неизменяемая часть)	`/opt/skd`
Файл конфигурации	`/etc/skd/seenaptec_acs.yaml`
Учётные данные сервисов	`/etc/skd/credentials/`
Каталог данных	`/var/lib/skd`
Служба systemd	`srv_ctrl.service` (включается и запускается автоматически)

Службы работают от отдельного системного пользователя `skd`, который создаётся при установке. Пользователю автоматически выдаются права на последовательные порты (группа `dialout`) — отдельной настройки прав на USB-преобразователи не требуется. Сервису поиска сетевых преобразователей назначается сетевая привилегия `CAP_NET_RAW`.

6.4. Конфигурация

Параметры платформы находятся в файле `/etc/skd/seenaptec_acs.yaml`. Для запуска обычно достаточно проверить два параметра:

- `MQTT.location` — адрес брокера MQTT, например `tcp://localhost:1883`;
- `SRV_BACK.combined.addr` — адрес и порт HTTP-сервиса, по умолчанию `:8080`.

Линии и оборудование в конфигурационном файле описывать не нужно — они настраиваются из веб-интерфейса (глава 10). После изменения конфигурации перезапустите службу:

```
sudo systemctl restart srv_ctrl.service
```

6.5. Проверка после установки

1. Проверьте состояние службы управления запуском:

   ```
   sudo systemctl status srv_ctrl.service
   ```

   Ожидаемое состояние — `active (running)`.

2. Проверьте готовность HTTP-сервиса:

   ```
   curl -i http://localhost:8080/health
   ```

   Ожидается ответ с кодом 2xx.

3. Откройте веб-интерфейс в браузере: `http://<адрес-сервера>:8080/app/`. На неактивированной системе должен открыться экран «Активация системы» (см. ниже).

Если какой-либо шаг не проходит, обратитесь к главе 16 («не открывается интерфейс»): типовые причины — не запущена служба, недоступен брокер MQTT, порт занят или закрыт межсетевым экраном.

6.6. Активация системы

При первом обращении к веб-интерфейсу вместо экрана входа показывается экран **«Активация системы»** с пояснением «Введите ключ активации, полученный от поставщика. Будет создан оператор admin с паролем по умолчанию» и единственным полем «Ключ активации».

Ключ активации выдаёт поставщик системы (порядок получения и всё, что связано с лицензией, — в главе 17). Ключ состоит из шести групп по четыре символа (цифры и латинские буквы A–F), например `0107-0000-002A-9F3C-1B77-D041`. Вводить его можно с дефисами или без, строчными или заглавными буквами — форма сама приводит ввод к каноническому виду. Кнопка «Активировать» становится доступной, когда введены все 24 символа.

После успешной активации:

- система привязывается к лицензии из ключа;
- автоматически создаётся оператор `admin` с паролем по умолчанию `123456` — полные права во всех областях системы;
- показывается обычный экран «Вход в SKD» с подсказкой: «Система активирована. Вход по умолчанию: admin / 123456 — после входа смените небезопасный пароль».

Если ключ не подходит, форма поясняет причину: «Неверный ключ активации. Проверьте ввод» (опечатка или чужой ключ) либо «Слишком много попыток активации. Повторите через N с» (защита от подбора).

6.7. Первый вход и смена пароля по умолчанию

Войдите под `admin` / `123456`. Пароль по умолчанию одинаков во всех поставках, поэтому система считает его небезопасным: **каждый вход с паролем `123456` записывается в журнал как тревожное событие** — тревога будет подниматься при каждом входе, пока пароль не сменён (глава 14). Смените пароль сразу после первого входа.

Как проходит смена, зависит от настройки «Требовать смену пароля, назначенного администратором» (рабочая область «Безопасность» → «Настройки безопасности», глава 14):

- **настройка включена** — сразу после логина показывается экран «Смените пароль»: текущий пароль, новый пароль дважды, кнопка «Сменить пароль». Работа в системе возможна только после смены; новый пароль не может совпадать с паролем по умолчанию (`123456`) и должен удовлетворять политике безопасности пароля;
- **настройка выключена** (по умолчанию) — доступ в систему предоставляется, но тревожные события при входе продолжаются до смены пароля. Сменить пароль можно в карточке оператора `admin`: рабочая область «Безопасность» → панель «Операторы» → `admin` → поле смены пароля.

Дальнейшие учётные записи, роли и параметры парольной политики настраиваются в рабочей области «Безопасность» (глава 14). При последующих обращениях к системе показывается обычный экран «Вход в SKD» с полями «Логин» и «Пароль».

6.8. Включение HTTPS

По умолчанию веб-интерфейс работает по HTTP. HTTPS включается из веб-интерфейса без обратного прокси: в рабочей области «Настройка / Обслуживание» на панели инструментов есть секция «Доступ по HTTPS», для загрузки сертификата (процедура — в главе 10). После включения интерфейс HTTPS становится доступным по адресу `https://<адрес-сервера>:8443/app/` дополнительно к интерфейсу HTTP.

6.9. Обновление пакета

Чтобы обновить платформу, установите новый пакет поверх текущего — тем же способом, что и при установке. При обновлении сохраняются:

- файл конфигурации `/etc/skd/seenaptec_acs.yaml`;
- учётные данные в `/etc/skd/credentials/`;
- данные системы в `/var/lib/skd`.

Служба перезапускается автоматически. Перед обновлением сделайте резервную копию штатным механизмом (глава 10).

Отдельные обновления меняют поколение ключей активации — в этом случае после обновления действует переходный период 14 дней, в течение которого нужно получить у поставщика и ввести новый ключ (раздел 17.5). Повседневных обновлений это не касается: если поколение не менялось, никаких действий с лицензией не требуется.

Глава 7. Первоначальная настройка системы

В этой главе приведён последовательный пример первоначальной настройки Seenaptec Access Platform (SAP) — от создания линии OSDP до регистрации первого события доступа.

В ходе примера выполняются следующие действия:

- создание линии OSDP;
- поиск и регистрация периферийного устройства;
- создание объекта доступа;
- привязка компонентов устройства к объекту;
- создание персоны и выдача ей пропуска;
- проверка доступа и события в журнале.

Перед началом работы убедитесь, что:

- установка системы выполнены в соответствии с главой 6;
- система активирована;
- выполнен вход в систему под учётной записью с необходимыми полномочиями;
- пароль оператора `admin`, установленный по умолчанию, изменён;
- преобразователь в RS-485 подключён к серверу и определяется операционной системой;
- периферийные устройства подключены к линии и на них подано питание;
- известна скорость обмена, настроенная на устройствах линии.

В примере используется линия RS-485, подключённая через USB–RS-485-преобразователь, и устройство AGRG, предоставляющее компоненты для управления дверью: считыватель, релейный выход замка и вход кнопки выхода.

Подробное описание оборудования, объектов доступа, пропусков и журнала событий приведено в главах 10–13.

7.1. Создание линии OSDP

Перед началом убедитесь, что USB–RS-485-преобразователь подключён к серверу и определяется операционной системой.

1. Откройте рабочую облать «Настройка / Обслуживание» и перейдите на панель «Оборудование».
2. Нажмите «Добавить» → «Линия».
3. В диалоговом окне «Добавить линию» укажите:

- **Тип адаптера** — `USB–RS-485`;
- **Основной порт** — последовательный порт преобразователя, например `/dev/ttyUSB0`;
- **Номер линии** — уникальный номер линии в системе;
- **Скорость** — скорость обмена, настроенная на подключённых устройствах.

4. Нажмите «Создать».

Результат: линия создана и добавлена в список оборудования.

Проверка результата: состояние связи линии должно измениться на «Активно», а в последствии «Неактивно». Состояние «Неактивно» возникает при отсутствии трафика на линииспустя некоторое время , что верно для пустой линии.

Если отображается состояние «Нет связи», проверьте:

- выбранный последовательный порт;
- скорость обмена;
- подключение и питание преобразователя;
- подключение и питание устройств;
- параметры линии RS-485.

Рекомендации по диагностике приведены в главе 16.

7.2. Поиск и регистрация устройств в системе

Перед началом поиска убедитесь, что линия находится в состоянии «Активно»/«Неактивно», а подключённые устройства включены и используют установленную для линии скорость обмена.

1. В рабочей области «Настройка / Обслуживание» на панели «Оборудование» выберите ранее созданную линию.
2. Запустите поиск:

- для поиска устройств AGRG с поддержкой SSB нажмите **«SSB-поиск на текущей линии»**;
- для поиска других устройств OSDP откройте карточку линии и выберите **«Адресный поиск»**.

3. В открывшемся диалоговом окне нажмите кнопку **«Поиск»**.
4. Дождитесь завершения поиска. Найденные устройства отобразятся в таблице с доступными сведениями, включая их серийный номер и адрес OSDP.
5. Проверьте список найденных устройств. Если обнаружены не все устройства, проверьте их питание, корректность подключения, адреса и скорость обмена, затем повторите поиск. Для SSB поиска при большом количестве устройств на линии возможен пропуск части устройств, в этом случае повторите поиск до тех пор пока все устройства не будут найдены.
6. Отметьте устройства, которые требуется добавить в конфигурацию, и нажмите **«Применить выбор»**.
7. Если устройство сохранено со статусом «Новое», откройте его карточку и нажмите **«Принять»**.

Результат: выбранные устройства добавлены в список оборудования.

Проверка: для зарегистрированных устройств отображаются состояние «Настроено» и состояние связи «Активно».

Если устройство не найдено или связь с ним не устанавливается, воспользуйтесь рекомендациями главы 16.

7.3. Создание объекта доступа

Перед началом создания объекта доступа убедитесь, что оконечное устройство зарегистрировано в системе, находится на связи, а его компоненты корректно отображаются в системе.

1. Откройте рабочую область «Объекты доступа».
2. Нажмите **«Добавить объект доступа»**.
3. В открывшемся окне укажите:

- **Название** — например, `Вход А`;
- **Уникальный код** — используется если есть код в проекте монтажа. Может быть использован для автоматической привязки объектов доступа к оборудованию по схеме проекта;
- **Тип** — например `Дверь (вход/кнопка)`.

4. Нажмите кнопку **«Добавить»**.
5. Выберите созданный объект и в его карточке откройте секцию «Привязка к устройствам».
6. Назначьте созданному объекту соответствующие компоненты периферийного устройства:

- **Считыватель** — считыватель карты;
- **Замок** — релейный выход, управляющий замком;
- **Кнопка выхода** — дискретный вход, к которому подключена кнопка выхода.

7. Нажмите кнопку **«Принять изменения»**.

Результат: объект доступа создан и связан с компонентами периферийного устройства.

Проверка: для объекта отображаются состояние «Настроено», состояние связи «Активно» и режим «Дежурный». Объект готов к обработке запросов доступа.

7.4. Создание персоны и выдача пропуска созданной персоне

Перед началом создания персоны подготовьте физический идентификатор (карту/метку/брелок), который будет выдан персоне, и определите срок его действия.

1. Откройте рабочую область «Пропуска».
2. Нажмите кнопку **«Новая персона»**.

3. Укажите фамилию, имя и отчество персоны, при необходимости добавьте фотографию, выберите шаблон дополнительных полей и заполните его поля.
4. Нажмите кнопку **«Создать и выдать пропуск»** (либо нажмите **«Создать»**, выберите созданную персону в списке и нажмите кнопку **«Выдать пропуск выделенной персоне»**).
5. В окне выдачи пропуска:

- добавьте карту: приложите её к любому считывателю или введите код карты вручную;
- укажите дату начала и дату окончания действия пропуска;
- в поле **«Время доступа»** выберите значение **«Без ограничения»** или любое другое требуемое значение;
- в разделе **«Объекты доступа»** выберите объект (например `Вход А`).

6. Проверьте корректность введённых данных и нажмите кнопку **«Сохранить»**.

Результат: персоне выдан пропуск с назначенным идентификатором и правом доступа к объекту `Вход А`.

Проверка: в списке пропусков отображается созданный пропуск со статусом «Активно», указанным администратором сроком действия и объектом доступа `Вход А`.

7.5. Проверка доступа и записи события в журнале

Перед началом проверки убедитесь, что объект `Вход А` находится в состоянии «Настроено», связь с оборудованием активна, а выданный пропуск действителен на момент проведения проверки.

1. Откройте рабочую область «Объекты доступа» и выберите объект `Вход А`.
2. В панели «События» включите режим отображения событий выбранного объекта.
3. Приложите выданную карту к считывателю.
4. Проверьте реакцию оборудования: при положительном решении замок объекта доступа должен разблокироваться в соответствии с настройками объекта.
5. Убедитесь, что в панели «События» появилась запись:

- результат — «Доступ разрешён»;
- причина — «Разрешено по пропуску»;
- участники — объект доступа, персона, пропуск и идентификатор.

6. Откройте рабочую область «Журналы» и найдите ту же запись в общей ленте (категория «Доступ»).

Результат: система распознала идентификатор, разрешила доступ к объекту `Вход А` и зарегистрировала событие в журнале.

Для проверки отказа в доступе приложите к считывателю отсутствующую в систему карту: в журнале должно появится событие «Доступ запрещён» с причиной «Доступ запрещён: идентификатор не найден».

Если событие доступа не появилось: проверьте по порядку связь линии и оконечного устройства, привязку считывателя к объекту, является ли пропуск активным и то, что сигнал считывания пропуска доступен в режиме «Пусконаладка (LIVE)».

Рекомендации по диагностике приведены в главе 16.

7.6. Дальнейшая настройка системы

Первоначальная настройка Seenaptec Access Platform (SAP) завершена: оборудование подключено, объекты доступа настроены, пропуска созданы и выданы, а события доступа успешно регистрируются в журнале событий.

Продолжить настройку системы вы можете в соответствии с вашими требованиями к объекту:

- расписания доступа, условия, периметры и правила АПБ — ознакомьтесь с главой 10;
- шаблоны доступа, заявки на пропуска и дополнительные поля персон —ознакомьтесь с главой 11;
- учётные записи операторов, роли и полномочия — ознакомьтесь с главой 13;
- настройка HTTPS, резервное копирование и обслуживание системы — ознакомьтесь с главой 9.

Глава 8. Общие принципы интерфейса

Все рабочие области веб-интерфейса Seenaptec Access Platform (SAP) построены по одной схеме. Глава описывает общие элементы и приёмы работы; стартовой странице «Обзор системы» посвящена глава 9, а каждая рабочая область отдельно описана в главах 10–14.

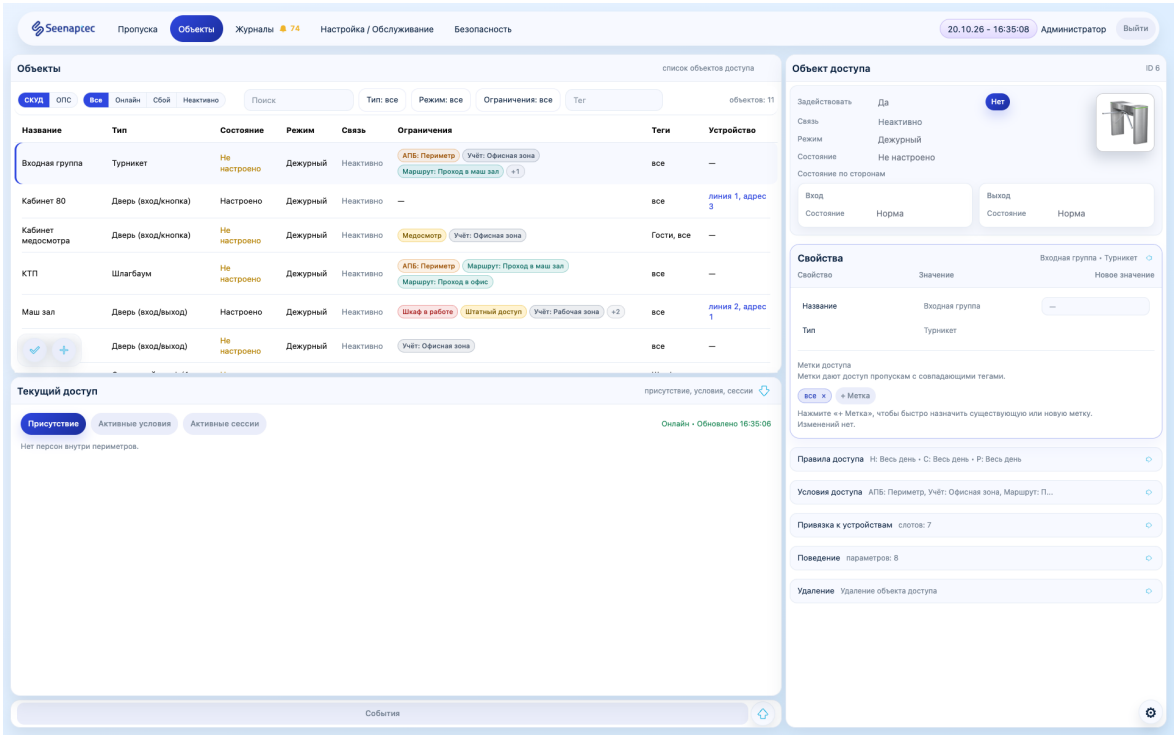
8.1. Вход в систему

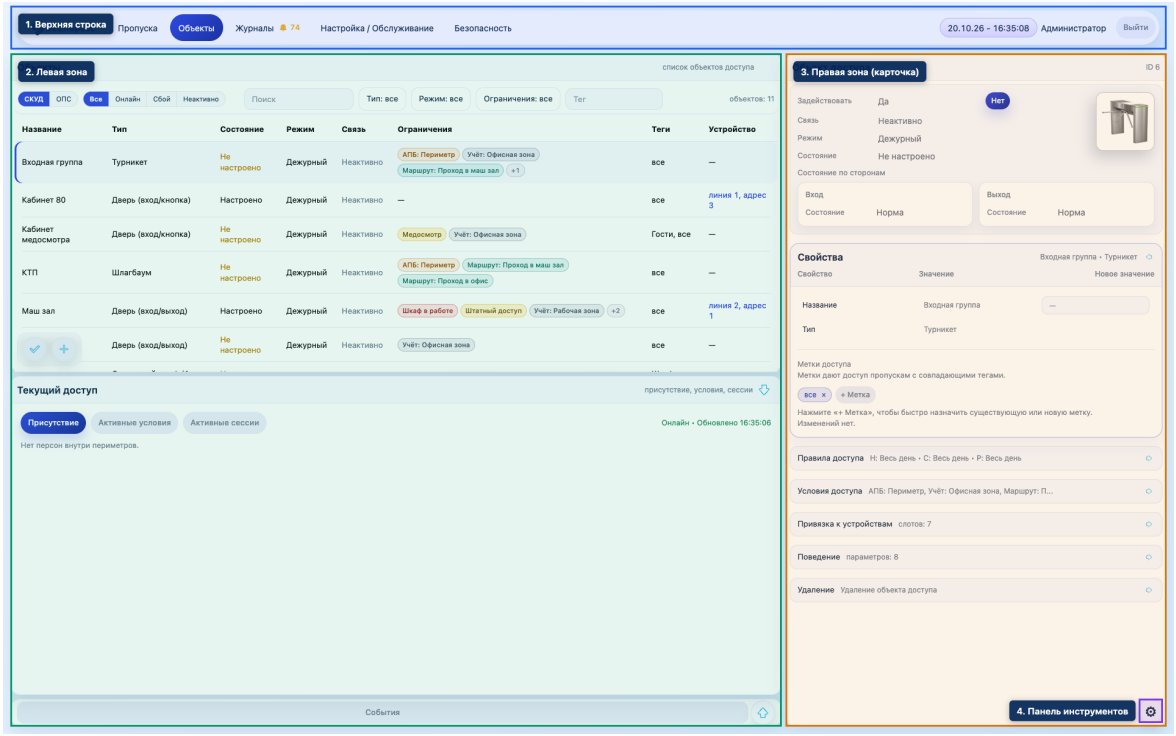
Веб-интерфейс открывается по адресу `http://<адрес-сервера>:8080/app/`. Перед началом работы запрашивается логин и пароль оператора (экран «Вход в SKD»). При самом первом запуске, пока система не активирована, вместо входа показывается экран «Активация системы» — ввод ключа активации (см. главы 6 и 17).

Набор доступных рабочих областей, панелей и действий зависит от роли оператора: например, оператор бюро пропусков может не видеть рабочую область «Настройка / Обслуживание». В этой и последующих главах интерфейс описан в полном составе — как его видит администратор.

Имя текущего оператора отображается в правой части верхней строки; там же находится кнопка «Выйти», завершающая сессию.

8.2. Компоновка рабочего экрана системы





Рабочий экран включает четыре основные области:

1. **Верхняя строка** — содержит кнопки перехода между рабочими областями системы, индикатор наличия/отсутствия тревожных сообщений, текущие дату и время, имя оператора и кнопку выхода из системы.
2. **Левая зона** — содержит панели со списками, деревьями объектов и лентами событий. В зависимости от выбранной рабочей области может отображаться одна панель или несколько панелей, расположенных одна под другой.
3. **Правая зона** — содержит карточку выбранной системной сущности, например линии, устройства, объекта доступа, персоны или пропуска.
4. **Панель инструментов** — появляется от правого края экрана и содержит справочники, параметры и дополнительные операции выбранной рабочей области.

При включении режима массовых операций - справа появляется панель выбора и настройки действия, применяющегося ко всем выбранным элементам списка.

Состав и содержимое областей зависят от выбранной рабочей области и полномочий оператора.

Чтобы изменить ширину левой и правой зон, перетащите вертикальный разделитель между ними. Если в левой зоне открыты две панели, измените их высоту с помощью горизонтального разделителя.

Выбранное расположение областей сохраняется в браузере и восстанавливается при следующем открытии веб-интерфейса оператором.

8.3. Верхняя строка и рабочие области

В верхней строке расположены пять кнопок рабочих областей:

Рабочая область	Назначение	Панели левой зоны
«Пропуска»	Персоны, идентификаторы, выдача пропусков	«Пропуска», «События», «Идентификаторы»
«Объекты доступа»	Двери, шкафы, правила и текущий доступ (`СКУД`) / пожарные зоны `D`, `A`, `P` (`ОПС`)	«Объекты доступа» («Зоны ОПС»), «Текущий доступ», «События»
«Журналы»	Исторический анализ событий, тревоги, отчёты	«Журналы», «Тревоги»

Рабочая область	Назначение	Панели левой зоны
«Настройка / Обслуживание»	Оборудование СКУД и ОПС, пусконаладка, системные операции	«Оборудование», «События», «Отладка»
«Безопасность»	Операторы, роли, сессии, секреты, аудит платформы	«Операторы», «События», «Сессии»

Активная рабочая область подсвечена. Слева от названий рабочих областей расположен логотип системы — щелчок по нему открывает стартовую страницу «Обзор системы» (глава 9); справа — переключатель подсистем **`СКУД | ОПС`**, текущие дата и время, имя оператора и кнопка выхода из системы.

Переключатель подсистем `СКУД | ОПС`. В правой части верхней строки отображается компактная пилюля переключения активной подсистемы (если в системе включены обе подсистемы и роль оператора имеет доступ к обеим):

- в рабочей области **«Настройка / Обслуживание»** переключатель меняет дерево левой панели «Оборудование» между контуром **СКУД** (сервер, линии RS-485 и периферийные OSDP-устройства) и контуром **ОПС** (пожарные панели UniPOS, системные блоки, шлейфы и адресные извещатели/модули, см. раздел 10.9), одновременно переключая контекст нижней панели «События» и выбор источника живой трассы (`srv_osdp` или `srv_ops`) в панели «Отладка»;
- в рабочей области **«Объекты доступа»** (при активной подсистеме ОПС в шапке кнопка отображается как **«Объекты»**) переключатель переводит рабочее пространство между объектами доступа СКУД и пожарными зонами ОПС (`D`, `A`, `P`, см. раздел 11.12), автоматически фильтруя нижнюю панель «События» по соответствующей подсистеме;
- в рабочей области **«Журналы»** пилюля расширяется до трёх позиций **`Все | СКУД | ОПС`** и служит быстрым фильтром событий и тревог по подсистеме (глава 13).

Если в системе активна только одна подсистема или роль оператора ограничена одной подсистемой (раздел 14.3), переключатель `СКУД | ОПС` автоматически скрывается.

Индикатор тревог. Если в системе есть активные непринятые тревоги, на кнопке рабочей области «Журналы» отображается жёлтый значок колокольчика со счётчиком количества тревог. Появление новой тревоги сопровождается звуковым сигналом. Нажмите значок, чтобы из любого раздела системы открыть панель «Тревоги» рабочей области «Журналы». Если активных тревог нет, значок не отображается.

8.4. Левая зона: панели

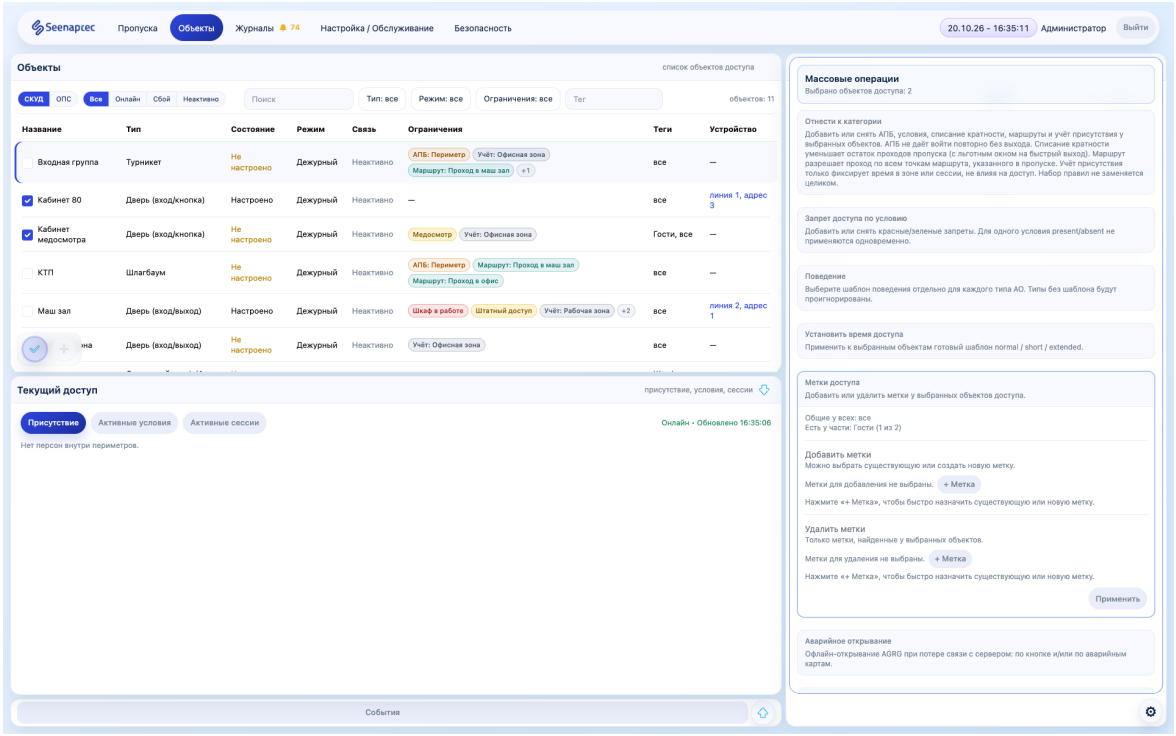
У каждой рабочей области может быть несколько левых панелей (см. таблицу выше). Первая панель — основная, она открыта всегда. Любую другую панель можно открыть **под ней** — прикрепить во вторую зону: свёрнутые панели показаны кнопками в нижней части левой зоны, щелчок по названию или по кнопке прикрепления разворачивает панель. Открытая нижняя панель сворачивается кнопкой откренления в её заголовке или щелчком по свободному месту заголовка. Выбранная комбинация панелей запоминается отдельно для каждой рабочей области.

Панели устроены единообразно:

- **список или дерево** — строки с ключевыми колонками и цветовой индикацией состояний (например, зелёное «Активно», красное «Нет связи»); щелчок по строке выбирает сущность и открывает её карточку в правой зоне;
- **кнопки действий** — в нижнем левом углу панели расположен блок кнопок для операций над списком.

Создание сущностей выполняется кнопкой «+» в нижнем блоке панели: она открывает диалог создания — например, «Добавить линию», «Добавить объект доступа», «Добавить персону», «Добавить пропуск». Диалог запрашивает минимально необходимые поля; остальное настраивается затем в карточке. Рядом с «+» расположены: включение режима массовых операций, специальные действия рабочей области (например, «SSB поиск на текущей линии» или «Настройка сетевых адаптеров» в панели «Оборудование»).

Включение режима массовых операций выполняется кнопкой «V» в нижнем блоке панели: она открывает справа панель выбора массовых операций.



Удаление сущностей выполняется не из списка: одиночное — из карточки (секция или кнопка «Удаление» / «Удалить …» в её нижней части), групповое — в панели массовых операций режима выбора.

Опасные операции всегда запрашивают подтверждение с перечислением затрагиваемых записей.

8.5. Правая зона: карточка

Карточка показывает выбранную сущность и состоит из **секций** — тематических блоков с заголовками: например, у пропуска это «Информация», «Идентификация», «Пропуск»; у устройства — паспорт, компоненты, настройки. Секции сворачиваются и разворачиваются щелчком по заголовку; стрелка у заголовка показывает состояние секции. Набор открытых секций запоминается на рабочем месте отдельно для каждого типа карточки (персона, устройство, событие журнала и т. д.) и применяется ко всем записям этого типа, переживая перезагрузку страницы. Состав секций зависит от типа сущности и описан в главах 10–14.

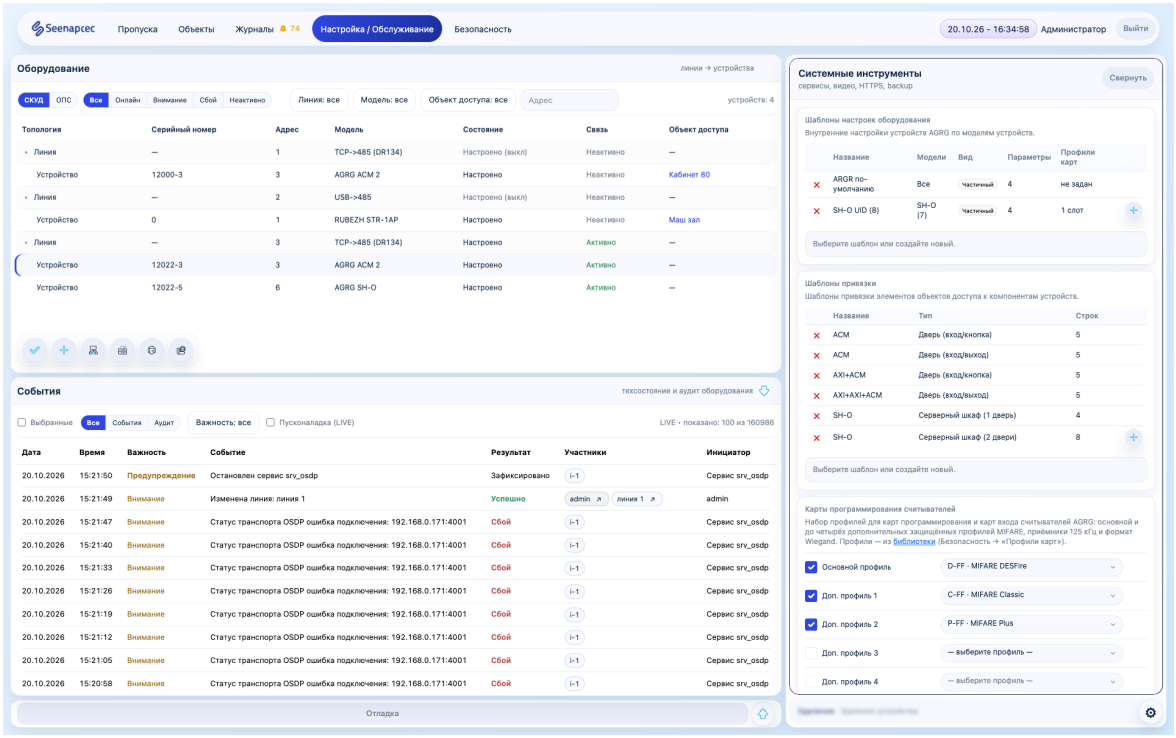
Карточка работает в модели «обзор + редактирование»:

- в обычном состоянии секция показывает текущие значения — карточку можно спокойно читать, ничего не меняя;
- в большинстве случаев, новое значение вводится в отдельное поле, чтобы было видно до и после; изменение любого поля переводит секцию в изменённое состояние: появляются кнопки сохранения и отмены, возможен ввод новых значений сразу для нескольких полей; до сохранения изменения на сервер не записываются;
- у справочных списков (шаблоны, роли, правила) редактор открывается явной кнопкой «Редактировать» и работает по той же схеме.

Результат сохранения подтверждается сообщением; изменение фиксируется в журнале аудита с перечнем полей «было/стало».

Кнопки с желтым фоном подразумевают посылку команд оборудованию.

8.6. Панель инструментов



Чтобы открыть панель инструментов, нажмите кнопку с шестерёнкой у правого нижнего края экрана. Панель содержит справочники и настройки выбранной рабочей области. Состав полей данных панелей инструментов зависит от полномочий оператора.

Состав панели:

- **«Обзор системы»** — «Язык», «Оформление», «Подсистемы», «Поддержка», «Восстановление доступа», «Пороги внимания» (раздел 9.6);
- **«Пропуска»** — «Шаблоны доступов», «Шаблоны идентификаторов», «Дополнительные поля персонала», «Автоочистка»;
- **«Объекты доступа»** — «Правила доступа», «Шаблоны поведения», «Шаблон времени доступа», «Производственный календарь»;
- **«Журналы»** — «Построение отчётов», «Архивация»;
- **«Настройка / Обслуживание»** — системные инструменты: шаблоны настроек и привязки оборудования, «Микропрограммы устройств», «Бэкап / восстановление», «Доступ по HTTPS», «Управление сервисами»;
- **«Безопасность»** — «Роли», «Секреты», «Настройки безопасности».

Для изменения параметров в открытой панели используется общая модель работы со справочниками: выберите запись, внесите изменения и нажмите кнопку **«Сохранить»**. Чтобы отменить несохранённые изменения, нажмите кнопку **«Сбросить»**.

Чтобы закрыть панель инструментов:

- нажмите кнопку **«Свернуть»** на панели;
- повторно нажмите кнопку с шестерёнкой у правого нижнего края экрана;
- нажмите любую панель в левой зоне.

При переходе к любой другой рабочей области панель сворачивается автоматически.

8.7. Панель «События»

Панель «События» отображает как новые, так и ранее зарегистрированные события, относящиеся к выбранной рабочей области. Новые записи добавляются автоматически, без обновления страницы.

Состав событий зависит от выбранной рабочей области и активного положения переключателя `СКУД | ОПС`:

- **«Объекты доступа»** — в режиме СКУД отображаются события доступа и изменения объектов доступа, в режиме ОПС — события пожарных зон (D, A, P), тревоги, пуски, обходы и действия операторов над зонами;
- **«Пропуска»** — события доступа персон, а также изменения персон, идентификаторов и пропусков;
- **«Настройка / Обслуживание»** — в режиме СКУД отображаются изменения состояния линий и OSDP-устройств, в режиме ОПС — события связи, опроса состава, неисправностей и команд по панелям UniPOS, шлейфам и адресным устройствам;
- **«Безопасность»** — события аудита платформы.

Для работы с лентой событий:

- используйте фильтры по периоду, важности, типу события и тексту;
- включите переключатель **«Выбранные»**, чтобы отобразить события сущности, выбранной в основной панели например, история конкретного объекта доступа или конкретного пропуска;
- нажмите событие, чтобы открыть его карточку с датой и временем, инициатором, результатом, причиной и изменениями значений «было/стало»;
- нажмите значок участника, чтобы отфильтровать события по связанному объекту доступа, устройству, пропуску, персоне или идентификатору;
- нажмите стрелку на значке участника, чтобы открыть его карточку. При переходе в другую рабочую область в заголовке панели появляется кнопка возврата к предыдущему представлению;
- нажмите **«Открыть в Журналах»**, чтобы перейти к выбранному событию рабочей области «Журналы».

Активные фильтры отображаются над лентой. Чтобы удалить фильтр по участнику, нажмите его обозначение.

В записи события сохраняются подписи участников, действовавшие на момент регистрации. Поэтому событие остаётся понятным даже после удаления связанной сущности.

В панели «События» рабочей области «Настройка / Обслуживание» дополнительно доступен режим **«Пусконаладка (LIVE)»**. В этом режиме отображаются низкоуровневые сигналы оборудования, которые не сохраняются в журнале. Подробнее — в разделе 10.6.

8.8. Проверка выполнения команд — принцип «команда принята — не значит выполнена»

Некоторые операции выполняются асинхронно. После нажатия кнопки система сначала принимает команду, а затем передаёт её соответствующему сервису или оборудованию. Поэтому сообщение об успешном приёме команды не подтверждает завершение операции.

К асинхронным операциям относятся, например:

- открытие двери;
- перезапуск сервиса;
- поиск устройств;
- обновление микропрограммы устройства.

Проверяйте выполнение команды по одному или нескольким признакам:

- **изменение состояния** — в карточке и списке отображается новое состояние объекта, например линия переходит в состояние «Активно»;
- **событие о результате** — в панели «События» появляется запись об успешном выполнении команды или ошибке;
- **индикатор выполнения** — для длительной операции отображаются её текущий статус исполнения и итоговый результат.

Не рекомендуется считать операцию завершённой только на основании сообщения об успешном приёме команды.

Если после сообщения об успешном приёме системой команды состояние операции не изменилось и событие о результате успешного/неуспешного завершения операции не появилось, проверьте связь сервера с линией и оконечным устройством. Не отправляйте команду повторно до завершения проверки статуса операции. Подробнее о диагностике оборудования — в главе 10.

8.9. Общие правила поведения интерфейса

- **Живое обновление.** Списки, состояния и ленты обновляются автоматически. Это касается и собственных действий оператора: результат сохранения сразу отражается во всех панелях, где участвует изменённая запись, —

например, выдача идентификатора в карточке персоны немедленно видна и в панели «Идентификаторы», и в списке пропусков. Если связь браузера с сервером прервана, актуальность данных не гарантируется; текущие дата и время сервера в верхней строке служат индикатором живого соединения.

- **Несохранённые изменения.** При попытке уйти от несохранённых изменений (выбрать другую запись, закрыть редактор) интерфейс запрашивает подтверждение сброса.
- **Подтверждения в правой зоне.** Подтверждения действий появляются поверх правой зоны с кнопками отмены и продолжения; опасные действия выделены цветом.
- **Права оператора.** Кнопки и секции, недоступные по роли, скрываются или блокируются с пояснением. Полномочия описаны в главе 14.
- **Единый словарь.** Все надписи интерфейса используют термины главы 3; состояния и причины решений отображаются едиными формулировками и в панелях, и в журнале.

8.10. Полезные рекомендации по работе с интерфейсом

Связанные сущности можно открывать непосредственно из списков, карточек и событий, в том числе с переходом в другую рабочую область.

Основные способы перехода:

- стрелка на значке участника в панели «События» или рабочей области «Журналы» открывает связанную персону, пропуск, идентификатор, объект доступа, устройство, линию или сервер;
- значение в колонке «Устройство» списка объектов доступа открывает устройство в рабочей области «Настройка / Обслуживание»;
- значение в колонке «Объект доступа» дерева оборудования открывает объект в рабочей области «Объекты доступа»;
- кнопка **«Открыть в Журналах»** открывает выбранное событие в рабочей области «Журналы».

После перехода слева в заголовке основной панели появляется кнопка возврата с подсказкой **«Вернуться в … с прежним выбором»**. Она возвращает к исходной рабочей области и восстанавливает:

- выбранную запись;
- открытую карточку;
- состав открытых панелей;
- выбранное событие в журнале или ленте событий.

Система запоминает только последний переход. Кнопка возврата исчезает после ручного переключения рабочей области в верхней строке или перехода по индикатору тревог.

Выполнение операций из разных разделов

Некоторые операции доступны из нескольких разделов интерфейса. Выберите способ, соответствующий текущей задаче:

- привязать оборудование к объекту доступа можно из карточки объекта, из карточки устройства или с помощью групповой операции;
- добавить идентификатор можно из панели «Идентификаторы» или из карточки персоны;
- выдать пропуск можно из панели «Пропуска», по заявке или на основе шаблона доступа.

Независимо от выбранного способа результат операции одинаково сохраняется в системе и регистрируется в журнале аудита.

Глава 9. Обзор системы

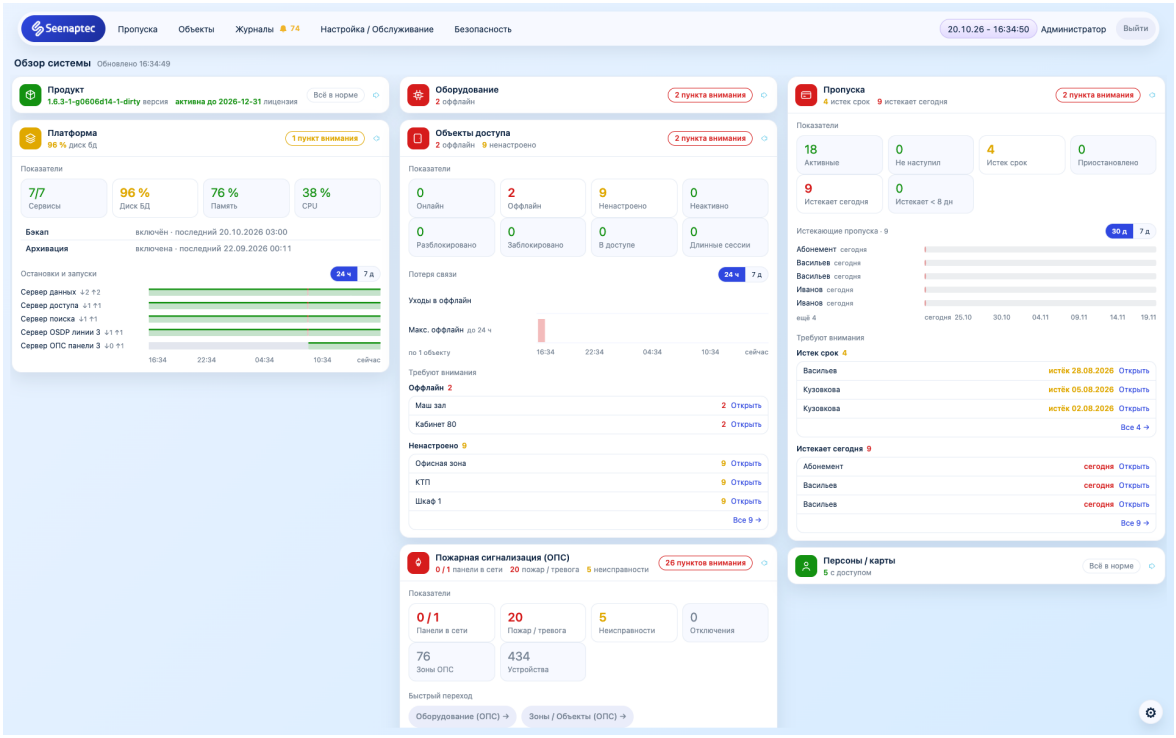
«Обзор системы» — стартовая страница веб-интерфейса: сводка состояния всей системы на одном экране. Страница отвечает на два вопроса — «всё ли в порядке» и «что требует внимания прямо сейчас» — и даёт переходы к месту проблемы. Рабочие области, к которым ведут эти переходы, описаны в главах 10–14.

9.1. Как открыть страницу

- Щелчком по логотипу системы в левом верхнем углу экрана. Повторный щелчок возвращает в рабочую область, из которой страница была открыта. На узком экране, где верхняя строка свёрнута в меню, «Обзор системы» — первый пункт этого меню.
- Страница открывается сама после входа в систему, а также при самом первом запуске интерфейса на рабочем месте.
- При перезагрузке страницы браузера восстанавливается последняя открытая рабочая область: если перед перезагрузкой был открыт «Обзор системы», вернётся он.

Страница доступна всем ролям; состав карточек не зависит от прав оператора. Отдельные секции панели инструментов (раздел 9.6) показываются по правам.

9.2. Карточки состояния



Экран занимают карточки по ключевым областям системы:

Карточка	Что оценивает
Продукт	версия и сборка ПО, идентификатор сервера, срок лицензии
Платформа	сервисы сервера, диск базы данных, память и процессор хоста, резервное копирование и архивация журнала
Оборудование	связь с устройствами и качество линий
Объекты доступа	связь с объектами доступа, нештатные состояния (разблокированные и длинные сессии)
Пожарная безопасность	связь с панелями ОПС, дежурный режим, пожарные тревоги, неисправности и обходы зон и устройств ОПС (отображается при включённой подсистеме ОПС)
Пропуска	активные и проблемные пропуска, истекающие сроки
Персоны/карты	персоны и идентификаторы: блокировки, просроченные карты, отказы в доступе

Карточки раскладываются в одну–три колонки в зависимости от ширины окна.

Статус карточки показан цветом значка и бейджа у названия:

- **зелёный** — «в норме»;
- **жёлтый** — предупреждение: система работает, но есть на что посмотреть;
- **красный** — требуется вмешательство;
- **серый** — «нет данных»: показатель посчитать нельзя (например, не настроено ни одной линии); на общий статус не влияет.

Статус карточки — худший из статусов её показателей. Рядом с названием — бейдж «N пунктов внимания» либо «Всё в норме».

Сворачивание. Карточки с проблемами раскрыты сразу, здоровые свёрнуты. Щелчок по заголовку раскрывает или сворачивает карточку; сделанный выбор сохраняется, пока открыта страница (автоматическое обновление его не сбрасывает). После перезагрузки страницы карточки снова раскрываются по состоянию.

9.3. Показатели и дополнительные секции

Внутри раскрытой карточки — секция «Показатели»: строки «название — значение», значение окрашено в цвет статуса. При наличии проблем ниже появляется секция «Требуют внимания» (раздел 9.4).

«Продукт» — версия и дистрибутив, название и цветовая схема бренда, разработчик и правообладатель, сборка (дата, коммит, версия Go), идентификатор сервера. Показатель «Лицензия» следит за сроком действия: жёлтый, когда до конца срока меньше 30 дней, красный — меньше 7 дней (пороги настраиваются, раздел 9.6). Жизненный цикл лицензии — глава 17.

«Платформа» — «Сервисы» (сколько сервисов системы работает из общего числа), «Диск БД», «Память», «CPU», «Бэкап» (давность последней резервной копии), «Архивация» журнала. Дополнительная секция «Остановки и запуски» — график работы сервисов за последние 24 часа или 7 дней (включая **Сервер приложения**, **Сервер поведений**, **Сервер обнаружения устройств**, **Сервер OSDP линии N** и **Сервер ОПС панели N**).

«Оборудование» — сводка по устройствам: «Онлайн», «Оффлайн», «Замена», «Отключено». Показатель «Качество связи» перечисляет до трёх самых проблемных линий с точечным состоянием:

Состояние линии	Статус	Что означает
«отключена»	жёлтый	линия отключена административно
«порт недоступен»	красный	издатель линии работает, но транспорт не поднялся
«нет связи»	красный	порт жив, обмена с устройствами нет
«возможно обрыв»	жёлтый	опрос идёт, но шина молчит минуту и дольше — вероятен обрыв (раздел 10.1)
«ошибок N %»	жёлтый / красный	доля ошибочных ответов на линии: жёлтый от 5 %, красный от 20 %

Дополнительная секция «Потеря связи» — почасовой график уходов устройств в оффлайн за 24 часа или 7 дней.

«Объекты доступа» — сводка по объектам: «Онлайн», «Оффлайн», «Ненастроено», «Неактивно»; нештатные состояния: «Разблокировано», «Заблокировано», «В доступе», «Длинные сессии» (объект удерживают открытым дольше порога — по умолчанию 60 минут). Своя секция «Потеря связи» — в разрезе объектов доступа.

«Пожарная безопасность» (подсистема ОПС) — сводка по пожарным панелям UniPOS и зонам: сколько панелей на связи («Панели на связи» / «Нет связи»), находится ли контур в дежурном режиме, сколько зафиксировано активных пожарных тревог и предтревог («Пожар / Тревоги»), технических неисправностей («Неисправности») и отключений/обходов («Отключено / Обход») по зонам (`D`, `A`, `P`), шлейфам и адресным устройствам. При появлении пожара, потери связи с панелью или неисправности карточка автоматически раскрывается и выводит конкретные панели, зоны и датчики в список «Требуют внимания» с быстрым переходом в «Объекты доступа» (режим `ОПС`) или «Настройку / Обслуживание» (режим `ОПС`).

«Пропуска» — «Активные», «Не наступил», «Истек срок», «Приостановлено», «Истекает сегодня», «Истекает < N дн» (порог настраивается, по умолчанию 7 дней). Дополнительная секция «Истекающие пропуска» — ближайшие пять пропусков с датами окончания в окне 30 или 7 дней.

«Персоны/карты» — персоны: всего, с доступом, заблокировано, «на территории»; карты: всего, свободно, просрочено, заблокировано и потеряно. Дополнительная секция «Отказы в доступе» — неизвестные карты и персоны с наибольшим числом отказов за 24 часа или 7 дней.

Дополнительные секции с графиками загружаются при раскрытии карточки и при смене периода; в общее автоматическое обновление страницы они не входят.

9.4. Список «Требуют внимания»

Секция появляется в карточке, когда у неё есть проблемные показатели. Для каждого такого показателя перечисляются первые три объекта с точечным состоянием — например, «Линия 5 (возможно обрыв)». Если объектов больше трёх, список завершает ссылка «Все N →».

- **«Открыть»** у объекта — переход к нему в соответствующей рабочей области: к строке линии в «Настройке / Обслуживании», к карточке объекта доступа, пропуска или персоны.
- **«Все N →»** — переход к полному списку проблемных объектов в рабочей области.

При переходе из обзора рабочая область запоминает точку возврата: кнопка возврата в её панели приводит обратно на «Обзор системы».

Если проблем нет, вместо списка показывается «Всё в норме».

9.5. Автоматическое обновление

- Данные страницы обновляются автоматически каждые 60 секунд; момент последнего обновления показан в шапке страницы («Обновлено …»).
- Автоматические запросы служебные: они проверяют сессию, но не продлевают её. По истечении окна неактивности (раздел 14.6) потребуется повторный вход, даже если страница всё это время обновлялась.
- Дополнительно раз в 30 секунд браузер отправляет служебный запрос `/health`, чтобы соединение через прокси-сервер платформы не простаивало; на работу оператора и сессию это не влияет.
- Если данные загрузить не удалось, страница показывает сообщение об ошибке и кнопку «Повторить».

9.6. Панель инструментов

Панель инструментов открывается кнопкой с шестерёнкой у правого нижнего края экрана (общий приём описан в разделе 8.6). Состав секций:

«Язык» — переключение языка интерфейса (`Русский` / `English`). Выбор сохраняется в браузере оператора и сразу переключает подписи интерфейса и словари журнала событий без перезагрузки страницы.

«Оформление» — тема интерфейса («Светлая» / «Тёмная») и фон страницы для тёмной темы («Графит», «Индиго», «Бирюза», «Без фона»). Настройка хранится в настройках сервера и применяется для всех ролей и всего веб-интерфейса, включая экран входа. Изменения вступают в силу после нажатия «Сохранить»; «Сбросить» возвращает тему и фон по умолчанию.

«Подсистемы» — включение и отключение функциональных контуров платформы на уровне инсталляции: **«Контроль и управление доступом (СКУД)»** и **«Охранно-пожарная сигнализация (ОПС)»** (как минимум одна подсистема должна оставаться включённой). Если обе подсистемы включены, в верхней строке интерфейса отображается переключатель `СКУД | ОПС`, а на странице обзора — карточки обеих подсистем.

«Поддержка» — идентификаторы инсталляции для обращения в поддержку: Server ID, код инсталляции (отпечаток) и серийный номер. Кнопка «Скопировать всё» копирует все три значения одним блоком — его удобно вставить в письмо или заявку; блок «Состав отпечатка» показывает устройства ядра, по которым построен код. Как устроен отпечаток, когда он появляется и когда меняется, — раздел 17.7.

«Восстановление доступа» — настройка входа по одноразовому коду поставщика, если пароль администратора утрачен. Секция доступна операторам с правами на чтение или управление операторами; изменение настроек требует полного права. Подробно — раздел 17.8.

«Пороги внимания» — пороги, по которым показатели обзора становятся жёлтыми (в подписях полей — «янтарь») и красными:

Поле	По умолчанию
«Лицензия истекает, янтарь» / «…, красный»	30 / 7 дн.
«Пропуска истекают»	7 дн.
«Долгая сессия разблокировки»	60 мин
«Диск БД, янтарь» / «…, красный»	80 / 90 %
«Память, янтарь»	85 %
«CPU, янтарь»	90 %

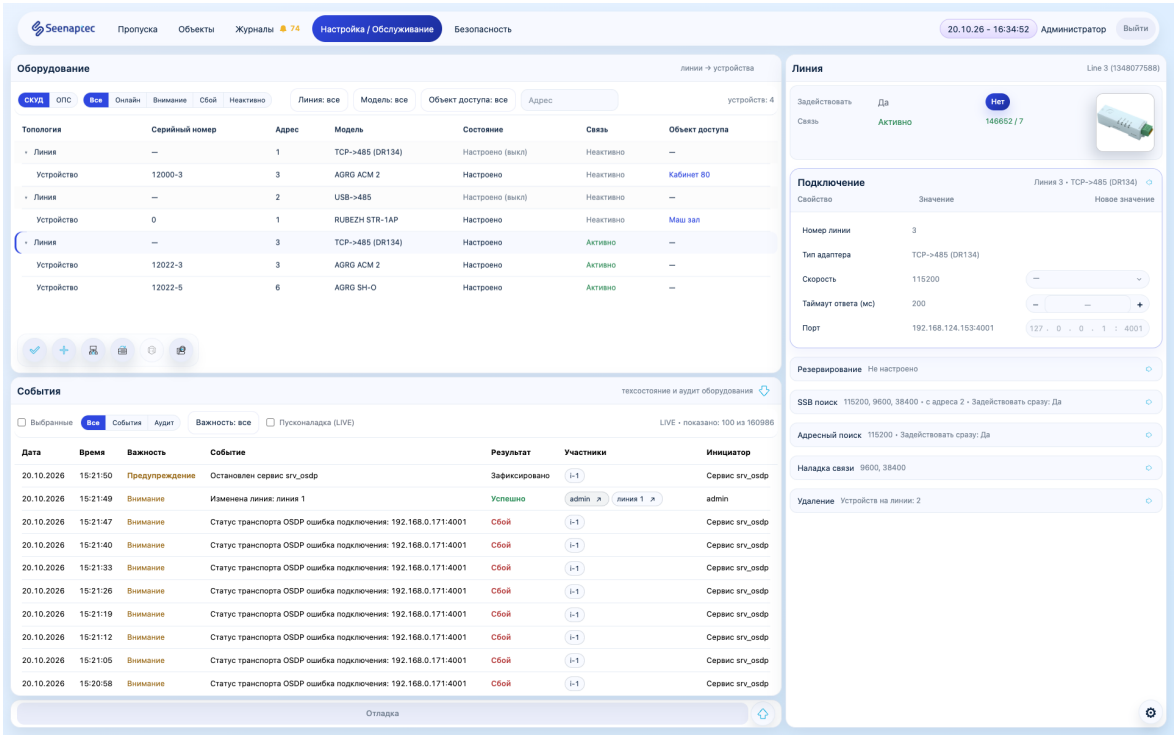
Пороги системные: хранятся в настройках сервера и действуют для всех ролей. После сохранения показатели пересчитываются сразу, перезагрузка страницы не нужна. Пороги качества связи линий (5 % и 20 % ошибок) в панель не вынесены и не настраиваются.

Глава 10. Настройка / Обслуживание

Рабочая область «Настройка / Обслуживание» — рабочее место инженера: подключение и обслуживание оборудования, пусконаладка, диагностика и системные операции. Левые панели области — «Оборудование», «События», «Отладка»; на панели инструментов собраны системные инструменты: шаблоны, микропрограммы, резервное копирование, HTTPS, управление сервисами.

10.1. Панель «Оборудование»

Панель показывает дерево оборудования «линии → устройства». Колонки списка: «Топология», «Серийный номер», «Адрес», «Модель», «Состояние», «Связь», «Объект доступа».



- Для **линии** в колонке «Адрес» показан номер линии, в «Модель» — тип адаптера, в «Состояние» — «Настроено» или «Настроено (выкл)».
- Для **устройства** — серийный номер, OSDP-адрес, производитель и модель, состояние жизненного цикла, состояние связи и имена привязанных объектов доступа; щелчок по колонке «Объект доступа» открывает объект в

рабочей области «Объекты доступа» (при нескольких привязанных — первый), вернуться назад можно кнопкой возврата в заголовке панели (раздел 8.10).

Состояния устройства: «Новое» (найдено поиском, ждёт подтверждения), «Изменено» (устройство сообщило о ревизии — изменении паспорта или состава), «Настроено» (записано в конфигурацию системы), «Неизвестно» (не было физического обмена, данные об устройстве не получены); суффикс «(выкл)» означает, что оборудование в данный момент вручную выключено из работы.

Состояния связи: «Активно» (обмен идёт; при работе в защищённом канале выделяется синим цветом), «Нет связи», «Возможно обрыв» (только у линии: адаптер работает, опрос идёт, но ни одно устройство не отвечает дольше минуты — вероятен обрыв шины или обесточены все устройства; показывается жёлтым), «Неактивно» (линия выключена), «Не обслуживается» (остановлен сервис линии), «Приостановлено» (например, на время поиска), «Порт недоступен» (нет связи с адаптером) . У линии с резервированием в строке дополнительно показан бейдж режима кольца: «Разрыв: опрос по сегментам», «Работает основной адаптер» или «Работает резервный адаптер» (при отказе одного из контуров бейдж называет работающий), «Линия недоступна» (в норме, когда кольцо цело, бейдж не показывается). Состояние связи кольцевой линии определяется фактом опроса: пока обмен идёт хотя бы через один порт (в том числе при разрыве шины по сегментам и при работе через резервный адаптер), линия и её устройства остаются «Активно», а отказ конкретного порта виден на его индикаторе в карточке линии; «Порт недоступен» показывается, только когда недоступны оба порта.

Над списком расположены фильтры по линии, модели, состоянию, связи, объекту доступа и адресу; справа — счётчик «устройств: N».

Кнопки действий панели (внизу слева):

- «Режим выбора устройств» — включает множественный выбор для массовых операций (раздел 10.5);
- «Добавить» — меню «Линию» / «Устройство» (устройство добавляется на выбранную линию);
- «Настройка сетевых адаптеров» — поиск и настройка сетевых преобразователей RS-485 (раздел 10.3);
- «SSB поиск на текущей линии» (раздел 10.3);
- «Создать/привязать объекты доступа группой» — групповое создание объектов доступа по устройствам согласно данным проекта (по серийным номерам) (глава 11).

10.2. Линии

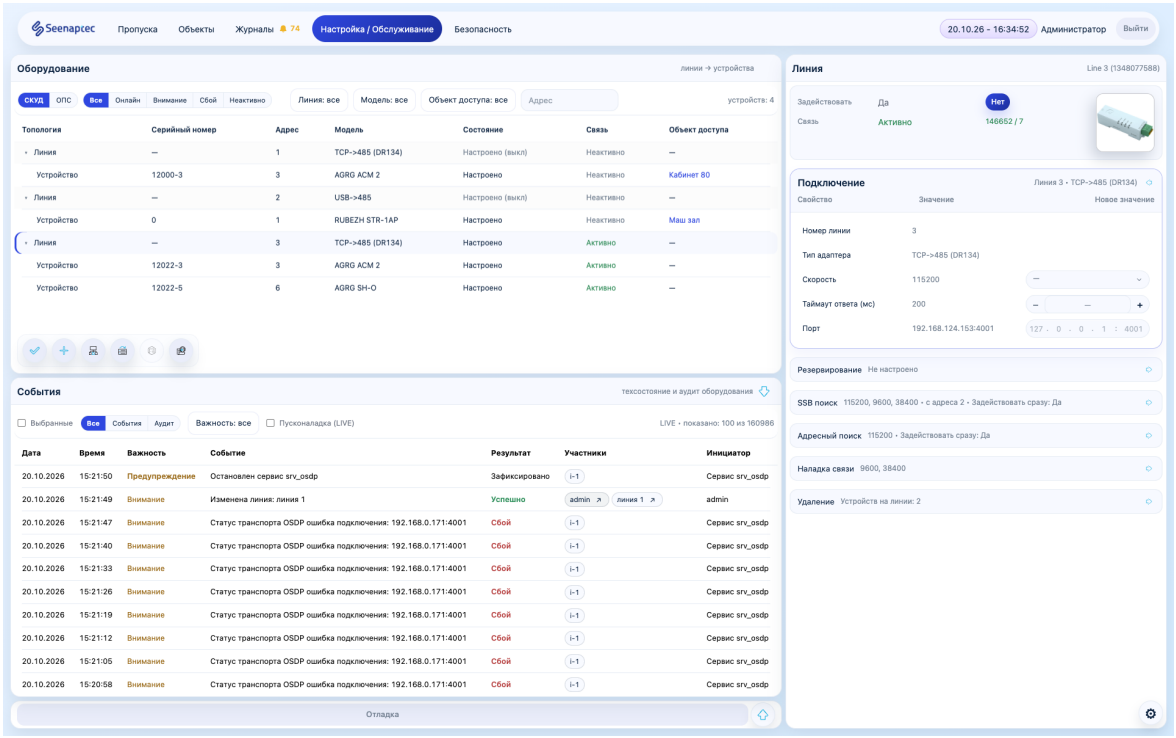
Создание линии

Кнопка «Добавить» → «Линию» открывает диалог «Добавить линию»:

- «Тип адаптера» — `USB->485`, `TCP->485 (Другой)`, `TCP->485 (DR134)` (характеристики типов — в главе 5);
- «Основной порт» — имя последовательного порта (например, `/dev/ttyUSB0`) или адрес `host:port` для TCP;
- «Резервный порт» — если он указан, резервирование включается автоматически;
- «Номер линии»;
- «Скорость» — для сетевых преобразователей, согласующих скорость самостоятельно, показывается «Не применяется».

Новая линия создаётся в активном состоянии. После создания сервис `srv_osdp` линии запускается автоматически; готовность видна по состоянию связи «Активно».

Карточка линии



В верхней части карточки — переключатель «Задействовать» для ручного выключения, текущее состояние связи со статистикой обмена и, при включённом резервировании, строка «Кольцо»: бейдж режима и индикаторы портов «Основной»/«Резервный» (подключение, активность приёма, эхо). Точки индикатора: «подключение» — порт жив; «приём» — с порта недавно принимались данные; «эхо» — кадры, отправленные через этот порт, недавно были услышаны с противоположного конца кольца. При отказе порта все его точки гаснут сразу; после восстановления порта «эхо» загорается только по факту первого подтверждённого кадра.

Секции карточки:

- **«Подключение»** — номер линии и тип адаптера (только чтение), скорость, время ожидания ответа (поле «Таймаут ответа (мс)»), порт.
- **«Резервирование»** — включение и резервный порт. Основной порт наследуется из настроек линии; параметры переключения настраивать не требуется — таймауты и задержки миграции заданы в системе.
- **«SSB поиск»** и **«Адресный поиск»** — запуск поиска устройств (раздел 10.3).
- **«Наладка связи»** — перевод устройств на скорость линии (для оборудования, поддерживающего смену скорости).
- **«Удаление»** — линия удаляется только когда на ней нет устройств.

Кнопок запуска и остановки самой линии нет: линия либо задействована, либо нет; обслуживающие её сервисы управляются отдельно (раздел 10.8).

Резервирование

Резервирование защищает один участок RS-485, доступный по двум контурам связи (раздельные преобразователи и трассы), объединённым в кольцо. Оба контура обслуживает один экземпляр `srv_osdp` линии: в норме все устройства опрашиваются через основной порт, резервный порт при этом слушает шину и контролирует её целостность по эху отправленных кадров. При разрыве шины («Разрыв: опрос по сегментам») устройства каждого сегмента автоматически переводятся на доступный им порт; при отказе основного контура целиком (отказ преобразователя, потеря TCP-связи) опрос переносится на резервный порт («Работает резервный адаптер»). После восстановления сегмента устройства возвращаются на основной порт автоматически, с выдержкой против частых переключений. Для эксплуатации достаточно итогового состояния в списке и карточке: бейдж режима кольца, индикаторы портов и состояние связи; у устройства, опрашиваемого через резервный порт, в списке и карточке показан чип «Резервный». Разрывы, восстановления и смены маршрута опроса фиксируются в событиях техсостояния.

10.3. Поиск и добавление устройств

SSB поиск

Для поддерживаемых AGRG OSDP-устройств используется автоматизированный поиск Seenaptec SecureBus: обнаружение по серийным номерам, назначение адресов и согласование скорости. Кнопка «SSB поиск на текущей линии» открывает диалог с таблицей найденного (адрес, серийный номер, производитель/модель, скорость, статус). Перед применением можно выбрать режим соединения (включая перевод в защищённый канал) и шаблон настройки оборудования по типам; кнопка «Применить выбор» принимает отмеченные устройства в конфигурацию. Если появились не все ожидаемые устройства, запустите поиск повторно.

Запуск SSB-поиска доступен и из секции «SSB поиск» карточки линии: там задаются перебираемые скорости, начальный адрес («Адресовать с») и признак «Задействовать сразу».

Адресный поиск

Для стороннего OSDP-оборудования используется секция «Адресный поиск» карточки линии: перебор диапазона адресов («Начальный адрес» — «Конечный адрес») на выбранных скоростях. Обнаруженные устройства появляются в блоке результатов и добавляются в конфигурацию.

Ручное добавление

Кнопка «Добавить» → «Устройство» открывает диалог «Добавить устройства на линию»: перечислите OSDP-адреса списком или диапазоном (например, `1–8, 10, 12–15`) — диалог покажет, сколько записей будет создано и какие адреса заняты. Созданные записи задействуются сразу; связь появится, когда устройства ответят на опрос.

Настройка сетевых адаптеров

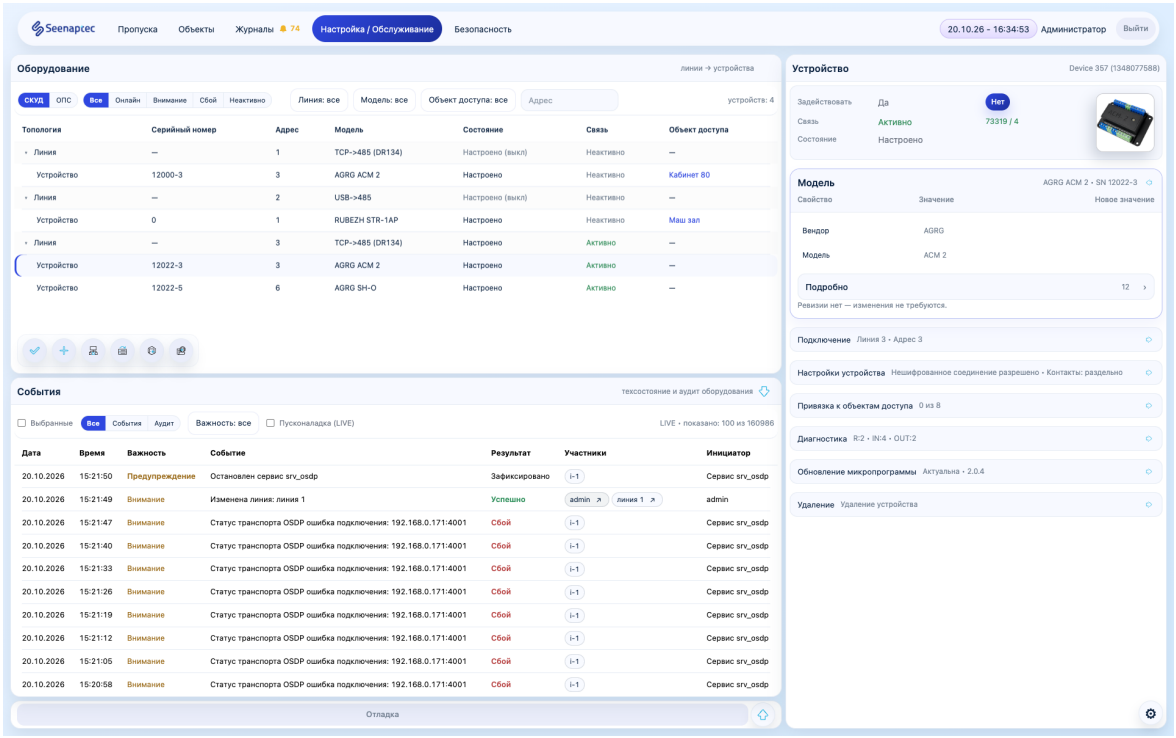
Кнопка «Настройка сетевых адаптеров» открывает инструмент поиска сетевых преобразователей RS-485 (на данный момент поддерживается только модель DR134) в локальной сети: поиск, проверка и назначение IP-адресов, загрузка соответствий «серийный номер → IP» из CSV и создание линий с ролями основного и резервного контуров. Адаптеры с адресом из текущей подсети сервера настраиваются обычным образом; найденные адаптеры с адресом из другой подсети также доступны для настройки — команда доставляется точечно по MAC-адресу (на серверах macOS/Linux), такие строки помечаются в списке информационной подписью «другая подсеть». У адаптера, уже добавленного в систему, остаётся доступной смена IP-адреса, например для переноса в текущую подсеть.

10.4. Устройства

Принятие нового устройства

Устройство, найденное поиском, сохраняется в состоянии «Новое» и остаётся неактивным до подтверждения. Карточка нового устройства показывает линию, OSDP-адрес, режим поиска, серийный номер и модель; кнопка «Принять» вводит устройство в конфигурацию.

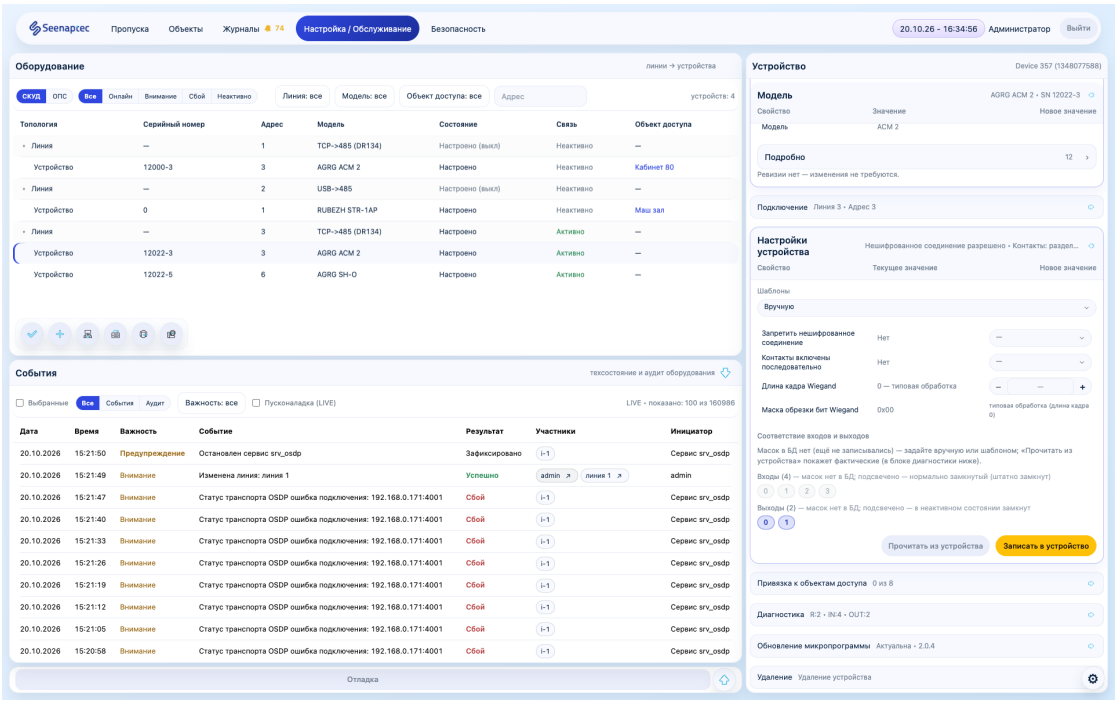
Карточка устройства



В верхней части — «Задействовать», состояние связи, состояние жизненного цикла и изображение устройства. Секции:

- **«Модель»** — паспорт: производитель, модель; в развёрнутом виде — версия, серийный номер, версия микропрограммы и перечень возможностей устройства. Если устройство сообщило **ревизию** — изменение паспорта или состава компонентов, — секция предлагает «Принять изменения» либо «Сбросить»; если изменения разрывают существующие привязки, подтверждение выполняется кнопкой «Принять и разорвать связи» с переходом к привязкам.
- **«Подключение»** — линия и адрес на линии (со сменой адреса командой на устройство), а также управление защищённым каналом OSDP Secure Channel. Режимы: «Не шифрованный», «Совместимый (SCBK-D)», «Установка первого ключа», «Полностью шифрованный», «Полностью шифрованный с автоматическим ключом» (автоматическая ротация). Показываются рабочий и ожидающий ключи, статус шифрования и время следующей ротации; предусмотрен сброс ключа устройства с подтверждением.
- **«Настройки устройства»** — параметры оборудования AGRG. Секция работает на устройствах с микропрограммой версии 2.0.0 и выше: на более ранней версии показывается заглушка с предложением обновиться, а пока версия не опрошена — предложение дождаться опроса паспорта. Значения хранятся в базе данных системы и показаны в колонке «Текущее значение»; правка выполняется в колонке «Новое значение». Кнопка **«Записать в устройство»** отправляет настройки в устройство и при успехе сохраняет их в базу; **«Сбросить»** отменяет несохранённую правку. Кнопка **«Прочитать из устройства»** выполняет диагностическое чтение: фактические значения показываются плашкой «Прочитано из устройства (диагностика)» с отметками «совпадает с БД» / «расходится с БД» — чтение ничего не сохраняет и не меняет текущую правку. Параметры: «Запретить нешифрованное соединение», «Контакты включены последовательно», а также обрезка транспортных бит Wiegand — «Версия Wiegand» (длина кадра в битах, 0 — обрезка выключена) и «Маска обрезки бит Wiegand» (какие биты кадра отбрасываются при формировании кода карты, например паритетные). Здесь же — редактор **«Соответствие входов и выходов»**: полярность каждого входа («нормально разомкнутый» / «нормально замкнутый») и состояние каждого выхода в неактивном состоянии задаются поточечно, кнопками с номерами точек (нумерация с нуля: вход 0, выход 0 и т. д. — как в остальных разделах системы). Полярность входа на устройстве складывается с флагом «Инверсия» слота в настройках поведения объекта доступа (раздел 11.3): включённые на обоих уровнях инверсии компенсируют друг друга. Для считывателей SH-O в секции задаётся и цепочка чтения карт — блок **«Профили карт»**: упорядоченный список защищённых профилей карт из библиотеки (раздел 14.9), которые устройство пробует сверху вниз, и чтение по UID. Настройки можно сохранить как шаблон и при-

менять к однотипным устройствам (раздел 10.8). Устройство может отклонить параметры как неприменимые в его текущем состоянии: тогда операция сразу завершается ошибкой «Параметры неприменимы» с пояснением, а не таймаутом ожидания ответа. Например, «Запретить нешифрованное соединение» нельзя включить, пока в устройстве не установлен ключ шифрования, — сначала установите ключ в секции «Подключение».



- **«Привязка к объектам доступа»** — соответствие компонентов устройства слотам объектов доступа (глава 11); сводка показывает «N из M» привязанных компонентов.
- **«Диагностика»** — живое состояние и прямое управление компонентами: считыватели (последний код, управление индикацией и звуком), контакты (тампер, питание, входы), реле (импульс 0,5–2 с, включение и выключение). Без связи управление недоступно.
- **«Обновление микропрограммы»** — сравнение полученной текущей версии устройства с файлами каталога микропрограмм и запись в устройство (раздел 10.8): этапы «Подготовка», «Загрузка образа», «Проверка контрольной суммы», «Передача в устройство», «Активация», «Проверка версии после записи», «Завершено».
- **«Удаление»** — удаление устройства из конфигурации; связанные объекты доступа сохраняются, их привязки разрываются. Для устройств AGRG с микропрограммой версии 1.x здесь же доступна кнопка «Сброс к заводским настройкам»: после подтверждения в диалоге устройство сбрасывается к заводским настройкам и удаляется из системы — используйте при выводе оборудования с объекта. Сброс подтверждается самим устройством: если оно не ответило или отвергло команду, удаление не выполняется.

Команды устройствам выполняются асинхронно (глава 8): результат подтверждайте по состоянию и событиям.

Замена устройства

Привязки к объектам доступа связаны с записью устройства в конфигурации, а не с конкретным экземпляром оборудования, поэтому при замене неисправного устройства удалять запись не нужно. Смонтируйте новое устройство на ту же линию с тем же OSDP-адресом; если новое устройство отвечает по другому адресу, измените адрес в записи старого устройства (секция «Подключение» → «Сохранить» — изменяется запись конфигурации, команда на устройство не отправляется).

Когда по адресу записи начинает отвечать другое оборудование, сервер получает паспорт, отличающийся от сохранённого, и фиксирует **ревизию**: устройство переходит в состояние «Изменено», секция «Модель» показывает поступившие изменения. Если новое устройство той же модели, принятие ревизии («Принять изменения») обновляет паспорт — серийный номер и версию микропрограммы, — а привязки к объектам доступа сохраняются: дополнительных

действий не требуется. Если модель другая и изменение состава компонентов разрывает привязки, подтверждение выполняется кнопкой «Принять и разорвать связи», после чего привязка корректируется в карточке объекта доступа (по шаблону привязки или вручную, глава 11).

Если запись работала в защищённом канале, новому устройству нужно установить ключ — проверьте статус шифрования в секции «Подключение».

10.5. Массовые операции

Кнопка «Режим выбора устройств» включает множественный выбор в списке; правая зона заменяется панелью «Массовые операции» со счётчиком выбранного. Одновременно активна одна секция:

Секция	Операция
«Режим соединения»	Задействование и перевод режима Secure Channel (включая ключи) для группы устройств
«Создать/привязать объект доступа»	Создание и привязка объектов доступа по выбранным устройствам; привязка — по шаблону привязки (подставляется автоматически) или вручную
«Шаблоны настроек оборудования»	Применение шаблонов настроек по группам «производитель/модель»
«Микропрограмма»	Групповая запись микропрограммы (файл подбирается из каталога автоматически)
«Удаление»	Удаление выбранных устройств

Ход выполнения виден индикаторами в колонке «Состояние» списка («Выбрано», «Ожидает», «Применяется» и итог по каждой операции).

10.6. События оборудования и режим «Пусконаладка (LIVE)»

Панель «События» отображает:

- изменения состояния линий и устройств;
- запуск и остановку сервисов;
- изменения настроек оборудования с указанием прежних и новых значений;
- результаты операций и сведения об ошибках.

Фильтры, переключатель **«Выбранные»** и переходы по значкам участников описаны в разделе 8.7.

Режим «Пусконаладка (LIVE)»

Режим **«Пусконаладка (LIVE)»** предназначен для проверки поступления сигналов от оборудования во время монтажа и диагностики.

Чтобы включить режим, установите чекбокс **«Пусконаладка (LIVE)»** в панели «События». В ленте дополнительно отобразятся низкоуровневые сигналы, в том числе:

- считывание идентификатора;
- нажатие клавиши;
- изменение состояния входа или выхода;
- изменение состояния защищённого канала;
- этапы обновления микропрограммы устройства.

Такие записи имеют префикс **«LIVE •»**, отображаются только при включённом режиме и не сохраняются в журнале.

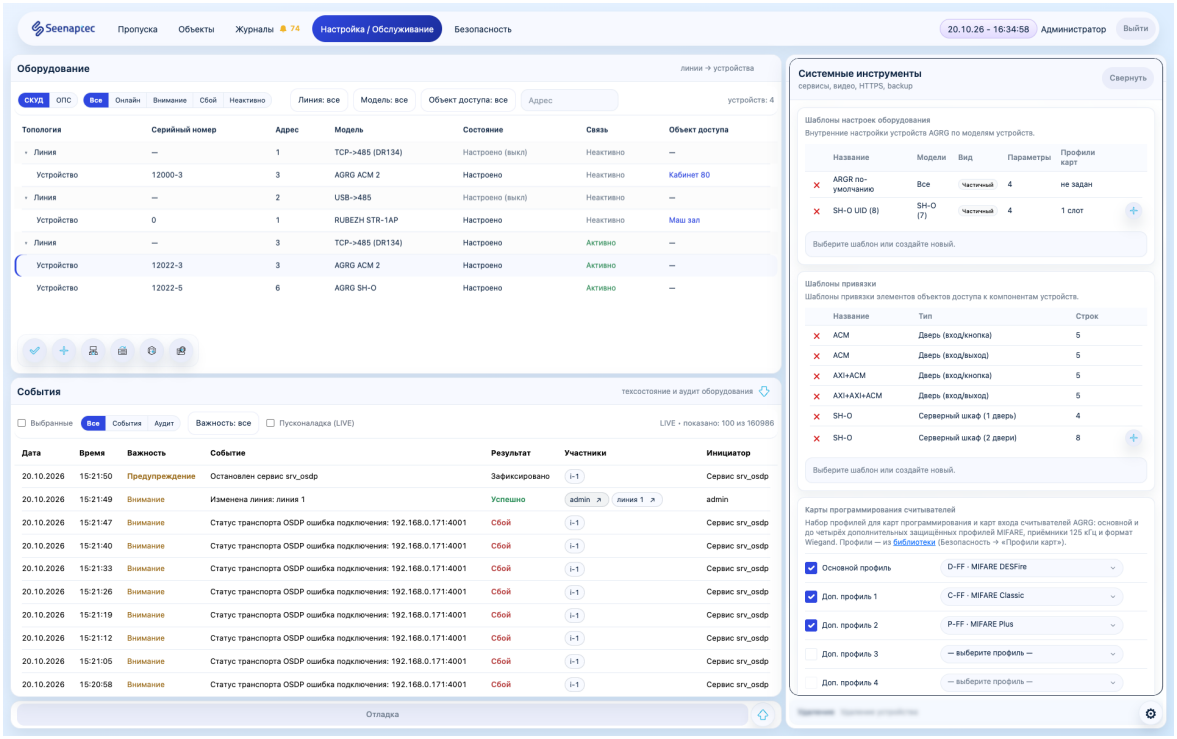
Для проверки считывателя включите режим, предъявите карту и убедитесь, что в ленте появилась запись с кодом считанного идентификатора. Появление записи подтверждает поступление сигнала на сервер, но не подтверждает разрешение доступа или выполнение команды оборудованием.

После завершения проверки отключите режим **«Пусконаладка (LIVE)»**.

10.7. Панель «Отладка»

Панель показывает журналы работы сервиса, обслуживающего выбранный узел оборудования: в режиме `СКУД` — экземпляра `srv_osdp` выбранной линии или устройства, в режиме `ОПС` — экземпляра `srv_ops` выбранной пожарной панели (раздел 10.9). Доступны поиск по подстроке, фильтр по уровню (`EMERG…DEBUG`), очистка и сохранение лога в файл. Линия с резервированием обслуживается одним экземпляром `srv_osdp`, поэтому её журнал единый — события обоих портов кольца идут в общем потоке. Публикация журнала работы включается переключателем «MQTT»; при выключенной публикации панель сообщает об этом. Панель предназначена для углублённой диагностики; для повседневной эксплуатации достаточно состояний и событий. События могут быть записаны в файл и переданы в техническую поддержку.

10.8. Системные инструменты (панель инструментов)



«Шаблоны настроек оборудования»

Именованные наборы настроек устройств (AGRG): параметры секции «Настройки устройства» (включая обрезку транспортных бит Wiegand), соответствие входов и выходов, а для шаблонов строго под считыватели SH-O — цепочка профилей карт. Шаблон создаётся из настроек устройства или в редакторе секции и применяется при SSB-поиске, из карточки устройства и в массовых операциях. Соответствие входов и выходов шаблон хранит поточечно — как редактор «Соответствие входов и выходов» в карточке устройства. Применение шаблона требует микропрограмму версии 2.0.0 или выше: устройство с более ранней версией отклоняет операцию с подсказкой обновиться.

«Шаблоны привязки»

Заготовки соответствия «компонент устройства → слот объекта доступа» для типовых схем подключения — рекомендуемый способ привязки оборудования к объектам доступа. Используются в карточке объекта доступа (переключатель «Режим привязки»), при создании объектов по выбранным устройствам и при групповом создании (глава 11); шаблон можно создать и из уже собранной вручную привязки.

«Карты программирования считывателей»

Ввод считывателей AGRG в эксплуатацию картами: карта входа переводит заводской или сброшенный считыватель в режим программирования на 30 секунд, и в это окно карта программирования записывает в него профили карт объекта. Секция готовит оба вида карт; рабочий (уже запрограммированный) считыватель режим программирования

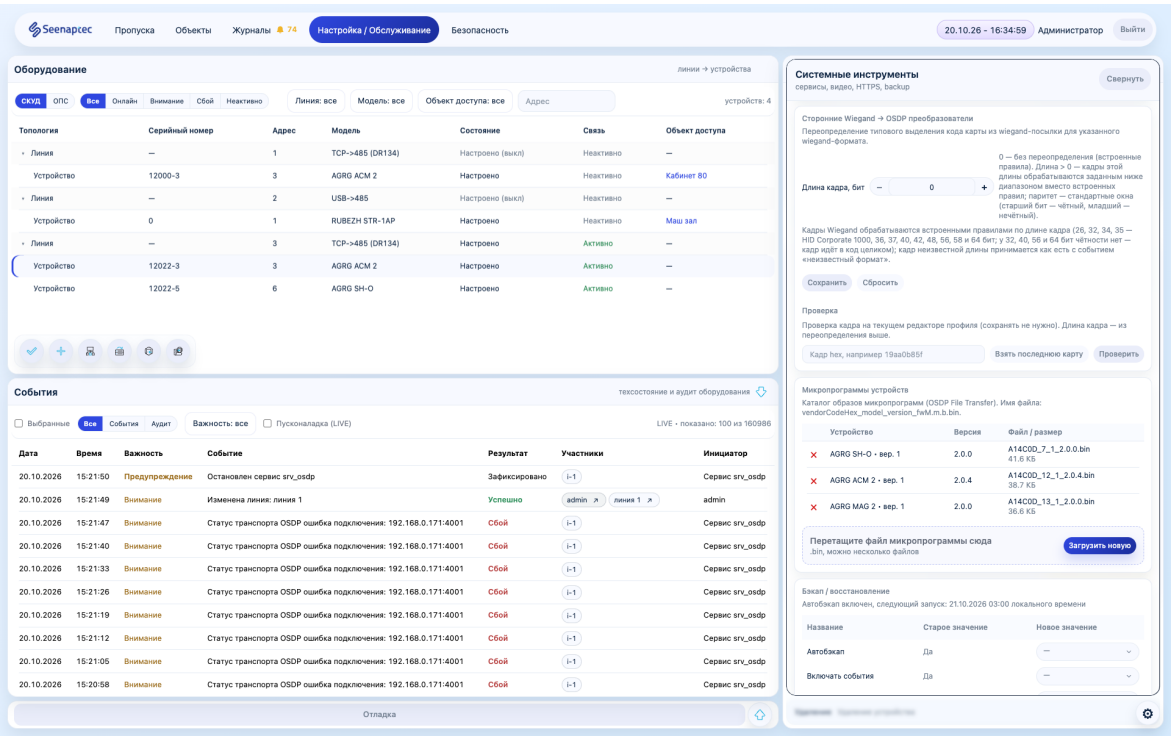
открывает картой входа по любому профилю набора. Работа с секцией требует области прав «Оборудование: Карты программирования считывателей»; выпуск выполняется на АРМ считывателя с назначенным рабочим местом (раздел 14.8) и включённым разрешением «Карты программирования» в его карточке.

В секции задаётся единый набор профилей: основной защищённый профиль MIFARE, до четырёх дополнительных и приёмники карт 125 кГц — профили выбираются из библиотеки (раздел 14.9); для набора выбирается общий формат Wiegand (26, 34 или 58 бит со стандартными битами чётности). Кнопка **«Создать карту»** сохраняет набор и открывает диалог выпуска; кнопка «Сбросить» возвращает набор к сохранённому состоянию. В диалоге выбирается цель выпуска (поле «Целевой профиль (тип изделия)»):

- **«Карта входа нового считывателя»** — для заводского или сброшенного считывателя;
- **«Карта входа по профилю …»** — для настроенного считывателя, по одному из профилей набора;
- **«Карта программирования»** — несёт профили набора считывателю; предъявляется в окне режима программирования после карты входа.

Выпуск — один проход: диалог сам готовит носитель (приводит чистую или чужую карту к нужному ключевому состоянию: заводские ключи — для карты входа нового считывателя, ключи профиля набора — для карты входа по профилю, ключ производителя — для карты программирования) и следом записывает содержимое. Держите карту на считывателе до завершения; ход операции показывает лента диалога. Данные записываются с блока 4 (сектор 1); нулевой сектор карты не изменяется. Каждый выпуск фиксируется в журнале.

«Сторонние Wiegand → OSDP преобразователи»



Переопределение типового выделения кода карты из Wiegand-посылки — для сторонних преобразователей «Wiegand → OSDP», через которые к линии подключены считыватели других производителей. По умолчанию система применяет встроенные правила для известных длин кадра; переопределение задаётся, когда формат кадра нестандартный:

- **«Длина кадра, бит»** — длина принимаемого кадра; значение 0 отключает переопределение (действуют встроенные правила), допустимы значения 2–64;
- **диапазон бит** — какие биты кадра образуют код карты; нумерация бит идёт с нуля справа, от младшего; по умолчанию — полный кадр;
- **лента бит** — наглядная схема кадра: старший бит слева, паритетные биты помечены «P», биты кода выделены, отброшенные приглушены; диапазон можно задать перетаскиванием по ленте.

Ниже работает проверка: введите сырой кадр в шестнадцатеричном виде или подставьте кадр последнего считывания кнопкой «Взять последнюю карту» — система покажет, какой код карты получится при текущих настройках редактора.

Сохранять профиль для проверки не нужно.

Сохранение изменённого профиля требует подтверждения: новый профиль меняет интерпретацию считываемых кадров, и коды карт, заведённые по старому профилю, перестанут совпадать с новыми считываниями. Сохранённые коды автоматически не пересчитываются — переход на новый формат выполняется перевыпуском идентификаторов (раздел 12.6) или повторным импортом с указанием интерпретации (раздел 12.9).

«Микропрограммы устройств»

Каталог файлов микропрограмм на сервере: загрузка файла (перетаскиванием или кнопкой «Загрузить новую»), удаление. Имя файла кодирует производителя, модель и версию — по нему система подбирает подходящую микропрограмму для устройства. Запись в устройства выполняется из карточки устройства или массовой операцией.

«Бэкап / восстановление»

Резервное копирование конфигурации и данных системы:

- настройки автоматического копирования: «Автобэкап», «Включать события» (журнал в составе копии), «Включать секреты» (перенос секретов в составе копии), «Папка backup», «Хранить файлов», «Время старта»;
- «Пароль» — резервная копия шифруется выбранным секретом из хранилища «Безопасности»; переключатель «Без шифрования» создаёт открытый файл (для изолированных стендов). Пароль не отображается в интерфейсе;
- «Включать секреты» — в копию попадают все секреты системы (включая ключ активации) и мастер-ключ хранилища. Такая копия всегда шифруется, поэтому настройка доступна только после того, как задан «Пароль». Файл с секретами помечен в списке копий пометкой «содержит секреты» — храните его как пароль;
- «Сделать backup сейчас» — ручной запуск;
- восстановление: выбор файла копии («Выбрать backup»). Для зашифрованной копии — блок «Пароль резервной копии»: если в настройках задан пароль, он подставляется автоматически; иначе введите пароль вручную. Тот же блок используется при открытии зашифрованного архива журнала (глава 13). Кнопка «Восстановить» запускает восстановление; после него сервисы перезапускаются, панель показывает их состояние до полной готовности. При восстановлении копии с секретами система дополнительно предупредит: текущие секреты и мастер-ключ будут перезаписаны.

Правила восстановления, связанные с лицензией (подробно — раздел 17.6):

- восстановить можно только копию **этой же инсталляции**: копия, снятая с другой инсталляции (с другим идентификатором сервера лицензии), отклоняется;
- восстановление на чистую, ещё не активированную систему разрешено — так выполняется перенос на новый сервер; после восстановления система попросит повторно ввести ключ активации этой инсталляции. Исключение — копия с включённым переносом секретов: ключ активации восстанавливается из копии, повторный ввод не требуется.
- база данных текущих сессий присутствия или работы с объектами доступа не сохраняется в бэкап. После восстановления сессии будут сброшены за исключением инициируемых оборудованием (например взлом).

Создание копий и восстановление фиксируются в журнале; сбой резервного копирования — событие критической важности.

«Доступ по HTTPS»

Включение HTTPS без обратного прокси: переключатель «HTTPS», порт (по умолчанию 8443) и сертификат. Сертификат загружается в хранилище секретов кнопкой «Добавить HTTPS сертификат в store» и выбирается из списка; статус показывает «HTTPS сохранен, ожидает применения» и затем «HTTPS принимает подключения». Изменения конфигурации HTTPS фиксируются в аудите.

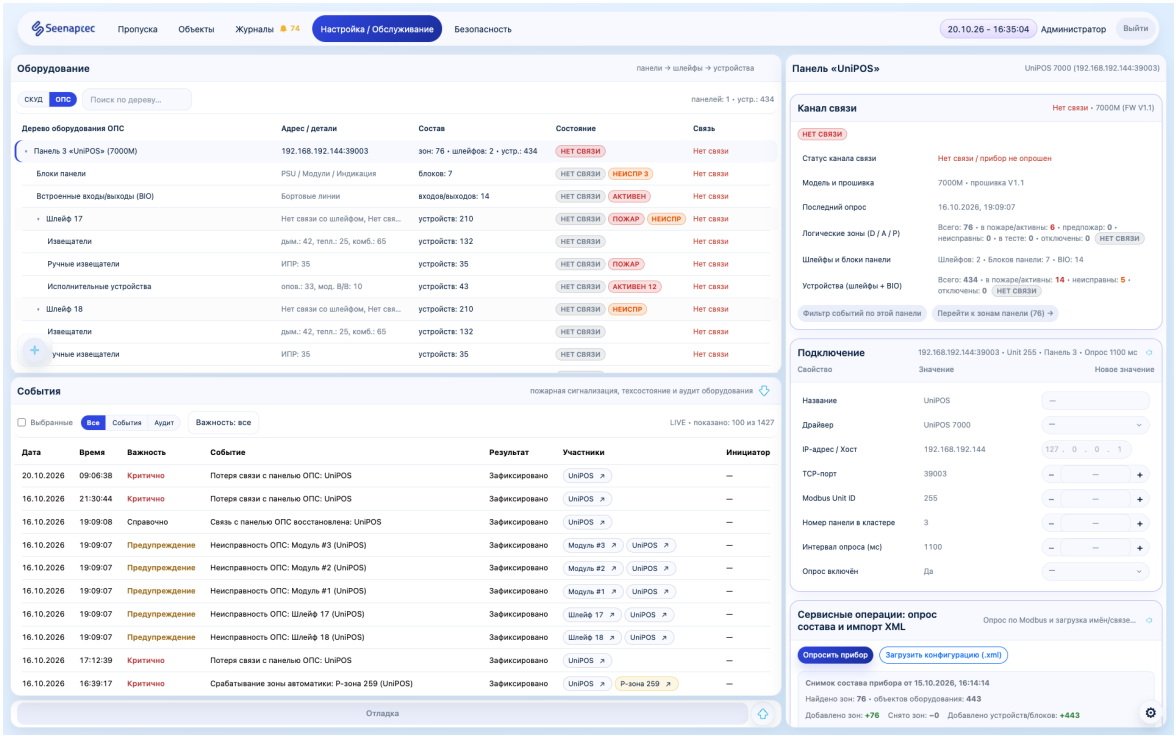
«Управление сервисами»

Список сервисов платформы с состояниями и командами «Запустить» / «Остановить» / «Перезапустить»: «Сервер приложения» («Сервер данных»), «Сервер поведений» («Сервер доступа»), «Сервер обнаружения устройств», «Сервер OSDP линии N» (включая резервируемые линии) и «Сервер ОПС панели N». Команды асинхронны: запрос фиксируется в аудите, фактический запуск и остановка — событиями техсостояния.

На панели инструментов есть также секция «Видео сервер» — здесь задаётся адрес видеосервера и загружается список камер. Пока адрес видеосервера не задан, видеоинтеграция считается не настроенной, и все связанные с видео элементы интерфейса (секция «Наблюдение» и привязка камер в карточках объектов доступа) скрыты; сама секция «Видео сервер» остаётся доступной. Подробно интеграция с видеоподсистемой в текущей редакции руководства не описывается, и будет доступна в ближайших версиях ПО.

10.9. Оборудование ОПС (панели UniPOS)

Для настройки и диагностики пожарной сигнализации и автоматики переключите пилюлю **`СКУД | ОПС`** в правой части верхней строки в положение **`ОПС`**. Рабочая область «Настройка / Обслуживание» переключится на контур оборудования ОПС: в левой панели «Оборудование» откроется дерево пожарных панелей UniPOS серии IFS7000, а нижние панели «События» и «Отладка» перейдут на поток событий и трассу сервиса `srv_ops`.



Дерево оборудования ОПС и индикация связи

В режиме `ОПС` левая панель «Оборудование» выстраивает иерархию физического состава приборов с колонками `Название`, `Тип`, `Адрес` и `Состояние`:

1. **Панель ОПС** — корневой узел прибора UniPOS IFS7000 (`7000M`, `7000-1MC`, `7000M-1L`). Чтобы зарегистрировать новую панель, нажмите кнопку **«+»** («Добавить панель ОПС») в нижней части панели «Оборудование» и укажите название, IP-адрес, TCP-порт (по умолчанию `502`) и номер панели в кластере (`1`–`8`).
2. **Системные блоки и шлейфы** — дочерние узлы панели, автоматически создаваемые после опроса состава:
   - блок питания (`БП`);
   - блоки индикации и оповещения (`БИО`) и блоки релейных выходов / входов (`БРВ`);
   - кольцевые шлейфы сигнализации (`Шлейф 1`, `Шлейф 2` и т. д.).
3. **Адресные устройства ОПС** — извещатели (дымовые, тепловые, комбинированные, газовые, ручные `ИПР`), модули ввода-вывода и устройства управления автоматикой (`РЕ`), сгруппированные внутри шлейфов и блоков `БИО`/`БРВ` по функциональному назначению: **«Извещатели»**, **«Оповещение»**, **«Управление автоматикой (РЕ)»** и **«Входы и выходы»**.

Индикация связи и состояний в дереве:

- у панели и шлейфов активный обмен с прибором подсвечивается зелёным статусом **«В сети»** / **«Активно»**;

- у системных блоков и адресных устройств штатное дежурное состояние отображается спокойным текстом **«Норма»** без цветовой перегрузки, а нештатные режимы выделяются цветом: **«Пожар»** / **«Предтревога»** (красный), **«Неисправность»** / **«КЗ»** / **«Обрыв»** (янтарный), **«Тест»** и **«Отключено (обход)»**;
- при потере TCP-соединения с панелью сама панель и **все её дочерние блоки, шлейфы и адресные устройства** автоматически переходят в статус **«НЕТ СВЯЗИ»** (последние известные состояния до обрыва сохраняются только как справочная помета в карточке и не маскируют потерю связи).

Карточка панели ОПС

При выборе панели ОПС в правой зоне открывается её карточка, состоящая из четырёх секций:

1. **«Канал связи»** — несворачиваемая сводка в верхней части карточки. Отображает текущее состояние связи (`В сети`, `Нет связи`, `Отключена`), сетевой адрес `IP:порт` и `Unit ID`, номер панели в кластере (`1`–`8`), паспорт прибора (модель `IFS7000`, серийный номер, версию прошивки, считанные по Modbus `0x2B / 0x0E`), время последнего успешного опроса и сводку обнаруженного состава (количество блоков, шлейфов, адресных устройств и зон).
2. **«Подключение»** — сворачиваемая таблица настроек в формате `Свойство | Значение | Новое значение`:
   - `Название` — отображаемое имя панели;
   - `Опрос включён` — включение или административное отключение опроса панели сервисом `srv_ops`;
   - `IP-адрес` и `TCP-порт` — 4-октетное поле ввода IPv4-адреса и порт Modbus TCP (по умолчанию `502`);
   - `Modbus Unit ID` — адрес узла Modbus (для панелей UniPOS IFS7000 по умолчанию `255`);
   - `Номер панели в кластере` — номер прибора в сети UniPOS (`1`–`8`);
   - `Период опроса, мс` и `Таймаут ответа, мс` — интервал циклического чтения регистров (по умолчанию `1000` мс) и время ожидания ответа (по умолчанию `2500` мс). После ввода новых значений нажмите **«Сохранить»** для применения настроек (или **«Сбросить»** для отмены правок).
3. **«Сервисные операции»** — команды обслуживания прибора:
   - **«Опросить состав»** — запускает инвентаризацию панели по Modbus TCP: сервис опрашивает слоты системных блоков, шлейфы, адресные устройства и зоны (`D`, `A`, `P`) и строит дерево оборудования без потери ранее назначенных UUID и имён;
   - **«Сброс тревог и неисправностей»** — отправляет на панель команду сброса защёлкнутых режимов пожарной тревоги и неисправностей;
   - **«Загрузить XML-конфигурацию»** — импортирует проектный файл `.xml`, выгруженный из штатного ПО конфигурирования UniPOS. При импорте система автоматически переносит пользовательские названия пожарных зон (`D`, `A`, `P`), шлейфов, выходов `БИО` и всех адресных устройств, а также привязывает извещатели и модули к своим зонам.
4. **«Удаление»** — удаление панели ОПС и связанного с ней дерева объектов после подтверждения в правой зоне.

Карточки системных блоков, шлейфов и адресных устройств

- **Карточка системного блока (`БП`, `БИО`, `БРВ`) и карточка шлейфа (`Шлейф N`)** содержат сводку состояния узла и несворачиваемую секцию **«Состав»**, в которой перечислены все входящие в блок или шлейф подблоки, каналы и адресные устройства с их адресами, типами, привязанными зонами и текущими состояниями. Щелчок по строке устройства в таблице «Состав» открывает карточку этого устройства.
- **Карточка адресного устройства ОПС** показывает паспорт извещателя или модуля (категория, подтип — например, оптический дымовой, тепловой дифференциальный, ручной извещатель, модуль реле или устройство `FPE`, номер шлейфа и адрес на шлейфе, привязанная зона ОПС, детальные флаги состояния и запылённости/ошибки измерения) и секцию **«Управление»** с оперативными командами:
  - **«Включить в работу»** — возвращает устройство из обхода или теста в штатный дежурный режим;
  - **«Тест»** — переводит устройство в сервисный режим проверки;
  - **«Отключить (обход)»** — временно исключает неисправный или обслуживаемый датчик/модуль из формирования тревог.

Диагностика Modbus TCP в панели «Отладка»

При выборе панели ОПС (или любого её шлейфа/устройства) нижняя панель **«Отладка»** подключается к живому потоку диагностических сообщений экземпляра `srv_ops` («Сервер ОПС панели N»). При включённом переключателе **«MQTT»** и уровне детализации `DEBUG` в ленте в реальном времени отображается трасса обмена кадрами **Modbus TCP (MBAP)**:

- **TX** — отправленные запросы с указанием кода функции, Unit ID, номера транзакции (tx), начального адреса регистров (addr), количества регистров (qty) и полного HEX-дампа пакета;
- **RX** — успешные ответы панели с временем выполнения запроса (dur), размером полезных данных и HEX-дампом;
- **RX EXC** — ответы-исключения Modbus (например, Illegal Data Address) с кодом исключения, длительностью и HEX-дампом;
- **ERR** — ошибки сокета, таймауты чтения или рассогласование заголовка MBAP.

В трассе видны все четыре типа используемых команд Modbus: чтение паспорта прибора **0x2B / 0x0E** (Read Device Identification), чтение регистров хранения и входных регистров **0x03** (Read Holding Registers) и **0x04** (Read Input Registers), а также вычитка записей текстового архива панели **0x14** (Read File Record). Трассу можно отфильтровать по подстроке (например, 0x14, RX EXC или ERR) и выгрузить в текстовый файл для анализа.

Глава 11. Объекты доступа

Рабочая область «Объекты доступа» — рабочее место администратора доступа: логические точки доступа, их правила и оперативная картина «кто где». Левые панели области — «Объекты доступа», «Текущий доступ», «События»; на панели инструментов — «Правила доступа», «Шаблоны поведения», «Шаблон времени доступа», «Производственный календарь», «Маршруты», «Учёт присутствия».

11.1. Типы объектов доступа

Объект доступа — логическая сущность, для которой настраиваются права, правила и режимы доступа. Его **тип** определяет всё поведение в системе: какие слоты для оборудования есть у объекта, какие режимы и правила к нему применимы (например, периметры АПБ — у дверей и турникетов, сессии — у серверных шкафов). Оборудование привязывается к слотам отдельно и позже: объект можно создать до монтажа, а оконечные устройства — заменить без потери прав и истории (раздел 10.4). Права всегда назначаются на объект, а не на контроллер (как в устаревших системах СКУД) или считыватель, и все решения о доступе принимает сервер, а не периферийная плата контроллера СКУД.

Такой подход позволяет:

- создать объект до монтажа оборудования;
- заменить оконечное устройство без повторного назначения прав доступа;
- сохранить настройки и историю объекта при замене оборудования.

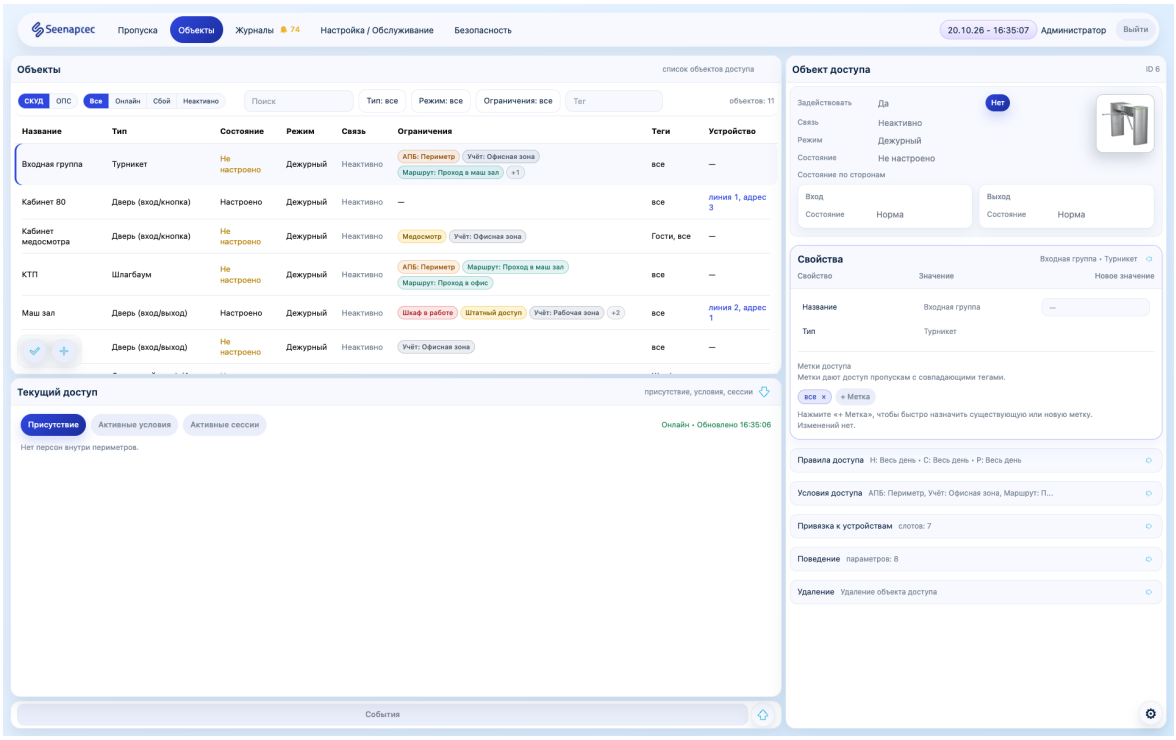
Тип объекта выбирается при его создании и определяет набор функциональных слотов, доступные параметры, режимы и правила.

Тип объекта	Назначение и особенности
«Дверь (вход/кнопка)»	Считыватель на входе и кнопка выхода. Слоты: считыватель, замок, кнопка выхода, датчик положения двери, датчик аварийного открывания. Поддерживает правила АПБ и режимы управления дверью.
«Дверь (вход/выход)»	Проход по идентификатору в обе стороны; кнопки выхода нет. Слоты: считыватели входа и выхода, общий замок, датчик положения двери, датчик аварийного открывания. Направление и ответ определяются считывателем предъявления. Поддерживает правила АПБ и режимы управления дверью.
«Турникет»	Отдельные слоты для считывателей и исполнительных механизмов входа и выхода, датчик прохода. Регистрируется результат: «Проход совершён» или «Проход не совершён».
«Серверный шкаф (1 дверь)»	Слоты: считыватель, замок, датчик двери, датчик ручки. Работа учитывается как сессия доступа — с началом, завершением и последним подтверждением.

Тип объекта	Назначение и особенности
«Серверный шкаф (2 двери)»	Передняя и задняя двери, общий объём. На каждую сторону — считыватель, замок, датчик двери, датчик ручки. Право действует на шкаф целиком. Одна сессия: открытие любой стороны — начало; обе закрыты — завершение. Сторона в событии и состоянии: «Передняя» или «Задняя».
«Шлагбаум»	Одна стрела на въезд и выезд. Слоты: считыватели въезда и выезда, привод стрелы, датчики проезда; опционально — датчик безопасности и датчик положения стрелы. Режим привода и состав датчиков задаются параметрами объекта. Регистрируется результат проезда.

Права доступа назначаются объекту, а не контроллеру, считывателю или другому компоненту оборудования. После привязки компонентов объект используется для обработки запросов доступа и регистрации связанных событий.

11.2. Панель «Объекты доступа»



Колонки списка: «Название», «Тип», «Состояние», «Режим», «Связь», «Ограничения», «Теги», «Устройство». Значения различаются по смыслу:

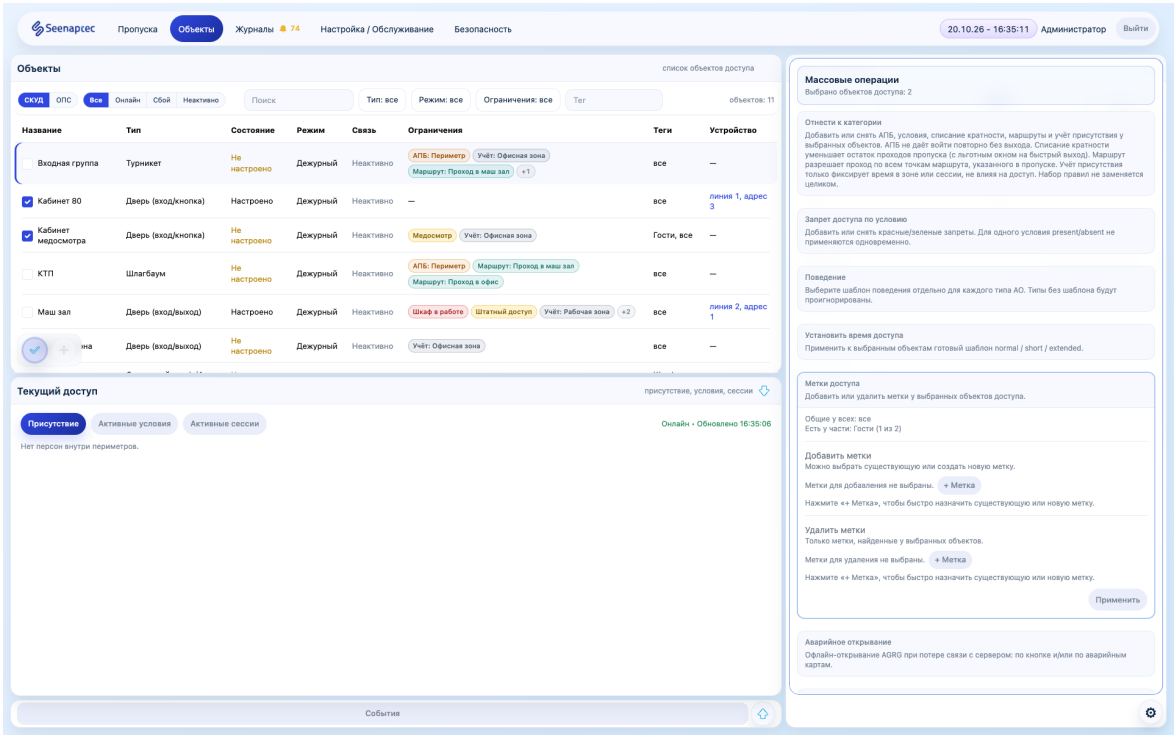
- **«Состояние»** — готовность конфигурации: «Настроено» (все обязательные слоты привязаны), «Не настроено», «Неактивно» (работа объекта доступа остановлена вручную);
- **«Режим»** — текущий режим работы: «Дежурный», «Открыт доступ», «Открыта ручка», «Разблокирован(а)», «Заблокирован(а)»; тревожные режимы выделяются цветом;
- **«Связь»** — итог по обязательным устройствам объекта: «Активно», «Нет связи», «Неактивно»;
- **«Ограничения»** — значки назначенных правил (периметры, условия, списание кратности);
- **«Теги»** — первые несколько тегов объекта доступа;
- **«Устройство»** — привязанное устройство; щелчок открывает его в «Настройке / Обслуживании», вернуться к списку объектов можно кнопкой возврата в заголовке панели (раздел 8.10).

Над списком — поиск и фильтры по типу, состоянию, режиму, связи, ограничениям и тегам.

Создание. Кнопка «Добавить объект доступа» открывает диалог: «Название», «Уникальный код», «Тип» и метки доступа. Групповое создание по списку устройств выполняется в «Настройке / Обслуживании» — кнопка «Создать/привязать объекты доступа группой». В строке задают код или название, серийные номера, тип и шаблон привязки — вручную или из CSV. После проверки объекты создаются и привязываются пакетом.

Режим выбора включает массовые операции над объектами: назначение категории, запрет доступа по условию, применение шаблона поведения, установка времени доступа, метки, аварийное открывание, удаление.

Массовая операция **«Аварийное открывание»** включает или выключает аварийное открывание на выбранных объектах: режим «Включить» / «Выключить» и независимые отметки «По кнопке (офлайн)» и «По аварийным картам (офлайн)». Объекты, не поддерживающие операцию (тип без аварийного открывания, неподходящая топология привязки, микропрограмма ниже 2.0.0), отсеиваются из списка с пояснением причины. Операция применяется асинхронно: итог смотрите в секции «Аварийное открывание» карточки объекта (раздел 11.3).



11.3. Карточка объекта доступа

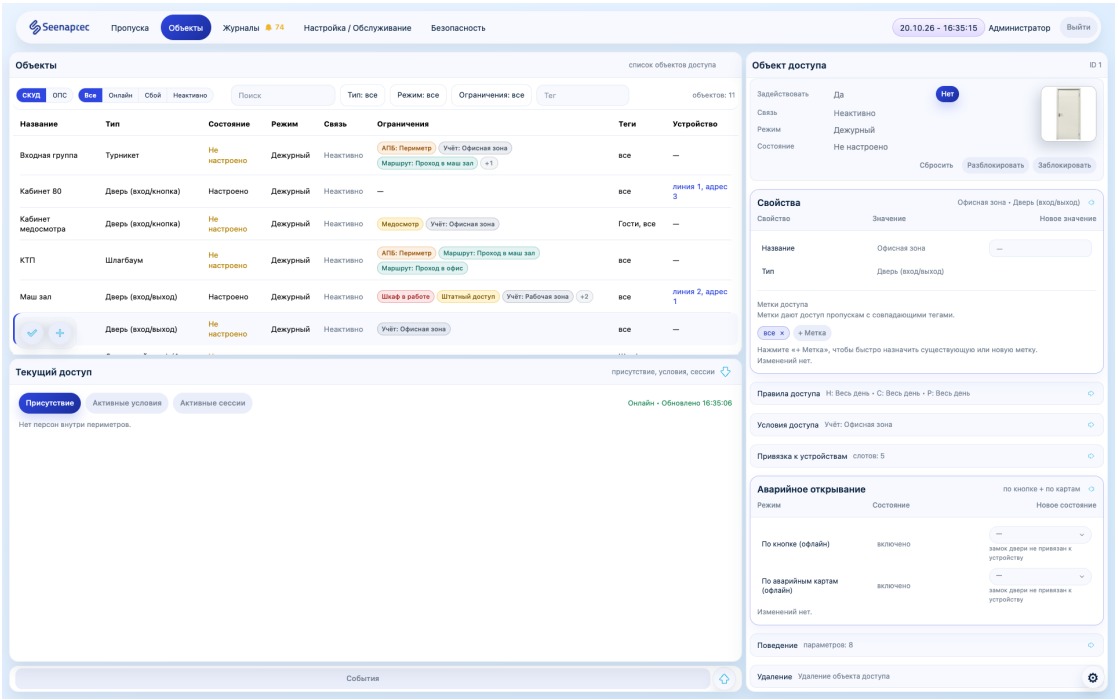
Верхний блок карточки — оперативный статус: «Задействовать», «Связь», «Режим», «Состояние». Для типов с операторскими режимами (дверь, шкаф, и т. д.) здесь же — прямое управление режимом: «Разблокировать» (постоянно открытый доступ), «Заблокировать» (запрет доступа), «Сбросить» (возврат в дежурный режим). Команды выполняются асинхронно; смена режима подтверждается состоянием и событием журнала. Кнопки разового открытия нет: разовый доступ предоставляется по идентификатору.

Секции карточки:

- **«Свойства»** — название и тип, а также метки доступа: «Метки дают доступ пропускам с совпадающими тегами» — способ выдавать права на группу объектов одним тегом (глава 3). > **Для знакомых с классическими СКУД.** Тег заменяет «группу доступа» («уровень доступа»), но устроен наоборот. В классической системе группа — это список точек, зашитый в настройки карты: изменился список — нужно перезаписывать карты или уровни. Здесь метка живёт на объекте: пропуску выдаётся доступ «по тегу», а состав группы меняется на стороне объектов — повесили метку на новую дверь, и все пропуска с этим тегом получили её автоматически. Для типов объектов с направлениями доступ по тегу можно сузить **классом доступа**: например, тег на турникетах — «только вход» или «только выход» (класс выбирается при выдаче пропуска, раздел 12.4). Действует правило приоритета: **если объект указан в пропуске явно, для этого объекта работает только явное указание** — теги для него не

рассматриваются; тег даёт доступ лишь к объектам, не перечисленным в пропуске напрямую.

- **«Правила доступа»** — идентификация и время доступа (раздел 11.4).
- **«Условия доступа»** — категории и запреты из каталога правил (раздел 11.4).
- **«Привязка к устройствам»** — соответствие слотов объекта компонентам устройств (раздел 11.5).
- **«Поведение»** — параметры работы: времена ожидания, предупреждения; заполняются вручную или шаблоном поведения; настройки можно сохранить как шаблон для однотипных объектов. Для каждого входного слота («Датчик двери», «Кнопка выхода» и т. д.) задаётся флаг **«Инверсия»**, переворачивающий трактовку значения входа, — способ подключить датчик с другой полярностью без перенастройки устройства. По умолчанию флаги выключены: кнопки работают на замыкание (нормально разомкнутые), датчик двери нормально замкнутый; тогда обрыв линии кнопки дверь не открывает, а обрыв линии датчика двери читается как вскрытие. Учитывайте обратную сторону: включённая инверсия кнопки под нормально замкнутый контакт переносит реакцию на обрыв линии в открытие двери. Инверсия слота складывается с поточечной полярностью входа на устройстве AGRG (раздел 10.4): включённые на обоих уровнях инверсии компенсируют друг друга. Отдельные параметры: **«Задержка запирания по датчику двери»** (у турникета — «Задержка запирания по датчику прохода») — пауза от 0 до 5000 мс между закрытием по датчику и запиранием замка, по умолчанию 0; **«Авторизованный выход по кнопке»** (только у односторонней двери) — выход по кнопке персонифицируется: после нажатия кнопки система ждёт предъявления карты на входном считывателе, пока дверь не закрылась, и записывает в журнал проход конкретного субъекта, по умолчанию выключен; **«Звуковой сигнал авторизованного выхода»** — подтверждение предъявления звуком считывателя, по умолчанию включён.
- **«Аварийное открывание»** — настройка аварийного открывания объекта на устройствах AGRG. Секция доступна при микропрограмме версии 2.0.0 и выше (на более ранней — заглушка с предложением обновиться) и при подходящей топологии привязки: считыватель и замок объекта подключены к одному устройству, и на устройстве не более одного объекта с замками. Два независимых аспекта — строки «По кнопке (офлайн)» и «По аварийным картам (офлайн)»: колонка «Состояние» показывает текущее значение из базы, в колонке «Новое состояние» выбирается «включить» / «выключить»; правка сохраняется кнопками «Сохранить» / «Сбросить». Включение «по аварийным картам» требует аварийных идентификаторов на объекте — карт вида «Аварийная», не более трёх (раздел 12.6); выключение доступно всегда. Применение на устройство подтверждается эхом: статус строки показывает «применено», «ожидание применения» или «ошибка применения» (причину смотрите в журнале). Срабатывания, произошедшие на устройстве без связи с сервером, доезжают в журнал после восстановления связи (раздел 13.1).



- **«Удаление»** — удаление объекта с разрывом привязок.

В карточке также может быть секция «Наблюдение» (видео). Она и остальные видео-элементы карточки — привязка камеры и параметры видеозаписи в секциях «Привязка к устройствам» и «Поведение» — отображаются только при настроенной видеоинтеграции, то есть при заданном адресе видеосервера в секции «Видео сервер» рабочей области «Настройка / Обслуживание» (глава 10). Сама видеоинтеграция в текущей редакции руководства не описывается.

11.4. Правила доступа объекта

Правила объекта собраны в двух соседних секциях карточки: «Правила доступа» — идентификация и время доступа; «Условия доступа» — категории и запреты. У каждой секции свои кнопки «Сбросить» и «Сохранить».

Идентификация и ограничения:

- «Режим идентификации» — «Только карта», «Карта + PIN», «Карта + подтверждение», «Карта + PIN + подтверждение». Режимы с PIN требуют установленный «Пин код подтверждения» у персоны (глава 12). Режимы с подтверждением реализуют двойной контроль для персон с признаком «Требует подтверждения» (раздел 12.3): после карты такой персоны система 15 секунд ждёт предъявления карты подтверждающего — сотрудника с признаком «Может подтверждать» и собственным действующим доступом к этому объекту. Остальные персоны проходят режимную точку как обычную: «Карта + подтверждение» — по карте, «Карта + PIN + подтверждение» — по карте и PIN. Подтверждение действует одинаково на входе и на выходе. PIN на режимной точке вводит только подтверждающий — по правилам стороны: на выходе персональный PIN не запрашивается, поэтому там подтверждающий предъявляет только карту;
- «Доступ под принуждением» — поведение при вводе PIN под принуждением (кода, отличающегося от обычного PIN последней цифрой, увеличенной на единицу): «Разрешен» — проход открывается внешне неотличимо от обычного, «Запрещен» — в доступе отказывается; в обоих случаях событие помечается как проход под принуждением и поднимает тревогу критической важности.

Временные профили (для типов с расписанием): недельная сетка доступа по трём профилям — «Нормальное время», «Сокращенное время», «Расширенное время». Какой профиль применяется к конкретному субъекту, определяет его пропуск (поле «Время доступа», глава 12); пропуска «Без ограничения» проходят круглосуточно. Сетка заполняется вручную или из шаблона времени доступа; переключатель «Учитывать производственный календарь» вводит ограничение на доступ в выходные и праздничные дни (нет доступа) из справочника (раздел 11.7). Текущие профили можно сохранить как шаблон.

Категории и запреты (секция «Условия доступа») — назначение объекту готовых правил из каталога (раздел 11.6):

- «Входит в категорию» — участие объекта в периметре АПБ, установка или снятие условия при проходе, списание кратности («Крат: …»);
- «Запрет доступа при наличии» — отказ субъектам с указанным условием (условие-блокировка);
- «Запрет доступа при отсутствии» — отказ субъектам без требуемого условия (допуск, инструктаж).

11.5. Привязка к устройствам

Каждый тип объекта определяет набор **слотов** — функциональных мест для компонент устройств: например, у двери — «Считыватель вход», «Замок», «Кнопка выхода» (обязательные), «Датчик двери», «Кнопка аварийного открывания» (дополнительные); у турникета — считыватели и замки входа и выхода, «Датчик прохода»; у шкафа — «Считыватель», «Замок», «Датчик двери», «Датчик ручки».

Рекомендуемый способ привязки — по **шаблону привязки**: заготовке соответствия «компонент устройства → слот объекта» для типовой схемы подключения (шаблоны настраиваются в системных инструментах «Настройки / Обслуживания», глава 10). В секции «Привязка к устройствам» переключатель «Режим привязки» предлагает шаблоны, подходящие типу объекта: при выборе шаблона привязка по отдельным слотам заменяется назначением устройств группам шаблона (сводка «Назначено: N из M»). Шаблоны применяются и при создании объектов по выбранным устройствам, включая групповое создание (раздел 11.2): подходящий шаблон подставляется автоматически, ручная привязка при этом скрыта.

Режим «Вручную» — альтернатива для нетиповых схем: для каждого слота выбирается компонент устройства с линии. Собранную вручную схему можно сохранить как шаблон («Сохранить текущую привязку как шаблон»); сложные специализированные привязки, по шаблону не редактируются.

Где выполняется привязка. Соответствие «компонент устройства → слот объекта» — одна и та же операция, доступная из нескольких мест; выбирайте то, что ближе к текущей задаче:

- **карточка объекта доступа**, секция «Привязка к устройствам» (этот раздел) — когда отправная точка — объект: настройка новой двери, замена схемы подключения;
- **карточка устройства** в «Настройке / Обслуживании», секция «Привязка к объектам доступа» (глава 10) — когда отправная точка — оборудование: инженер видит компоненты устройства и подключает их к слотам объектов;
- **кнопка «Создать/привязать объект доступа»** в заголовке панели «Оборудование» (иконка объекта доступа, активна при выбранном устройстве) — диалог с режимами «Создать» (новый объект с привязкой по шаблону или вручную) и «Привязать» (существующий объект). Если устройство уже привязано, диалог предлагает **«Отвязать»** — с подтверждением в правой панели; сам объект доступа при отвязке сохраняется, разрывается только связь с устройством. Пока устройство привязано, создание и привязка по нему недоступны;
- **массовые операции панели «Оборудование»**, секция «Создать/привязать объект доступа» (раздел 10.5) — создание и привязка объектов по выбранным в списке устройствам;
- **групповое создание** — кнопка «Создать/привязать объекты доступа группой» в панели «Оборудование» (раздел 11.2): пакетное создание и привязка по списку строк серийных номеров устройств или файлу CSV.

Во всех местах действуют одни и те же шаблоны привязки из системных инструментов «Настройки / Обслуживания» (глава 10), а результат одинаково отражается в состоянии объекта и фиксируется в журнале.

В карточках объекта и устройства привязку можно сохранять по шагам, с неполным набором обязательных слотов: промежуточный результат сохраняется, включая снятие уже сделанной привязки. Массовые операции строже — групповое создание и привязка требуют полного набора обязательных слотов сразу.

Это касается и смены режима, который меняет состав обязательных слотов: например, режима датчиков прохода у шлагбаума или турникета. В карточке объекта такой режим сохраняется сразу, даже если ставшие обязательными компоненты ещё не привязаны, — секция параметров показывает жёлтое предупреждение со списком недостающих привязок, и оно исчезает, когда набор восстановлен. В массовых операциях (пакетное применение шаблонов поведения и времени) та же смена режима по-прежнему отклоняется с ошибкой.

Пока обязательные слоты не привязаны, объект остаётся в состоянии «Не настроено» и не управляет соответствующим оборудованием.

11.6. Каталог правил: условия, периметры АПБ и списание кратности

Секция **«Правила доступа»** панели инструментов — единый каталог правил, назначаемых объектам.

> **Для знакомых с классическими СКУД.** В классических системах антипассбек и подобные ограничения — это флаги в настройках контроллера, привязанные к конкретной плате. Здесь правило — именованная запись в общем каталоге, которая назначается объектам как метка: один периметр может охватывать двери на разных линиях и контроллерах, одно условие — проверяться на любом числе точек, одно правило кратности — действовать на всех входах здания. Правило создаётся один раз, а объекты «входят» в него; вся логика выполняется на сервере, поэтому состав участников меняется без перенастройки оборудования.

Условие — именованный признак субъекта (например, «Инструктаж пройден», «Допуск в серверную»). У условия задаются срок действия в минутах (или без срока), описание и **направленные триггеры** — как условие ведёт себя на объектах, входящих в его категорию:

- «Ставить по» — «проходу/доступу», «входу/началу доступа» или «выходу/концу доступа»: когда субъект совершает указанное движение через объект-«категорию», условие устанавливается;
- «Снимать по» — «не снимать» или один из тех же трёх триггеров: обратный триггер, автоматически снимающий условие.

Подписи триггеров двойные: для проходных объектов действует первая часть («проходу», «входу», «выходу»), для сессионных — шкафов — вторая: вместо прохода у шкафа сессия доступа, поэтому «вход» для него — начало доступа, «выход» — окончание доступа, а «проход» срабатывает на обеих границах сессии. На проходных объектах «по входу» и «по выходу» срабатывают только на считывателях с заданным направлением; «по проходу» — на любом подтверждённом проходе. Если на одном событии совпали установка и снятие, условие устанавливается. Срок действия продолжает работать как страховка: условие истечёт само, даже если выход не был зафиксирован. Пара триггеров позволяет строить правила присутствия: например, условие «Находится в цехе» ставится по входу через проходную цеха, снимается по выходу, а двери опасной зоны требуют его наличия.

Условие можно:

- устанавливать и снимать автоматически при проходе через объект-«категорию» (триггеры выше);

- требовать («Запрет доступа при отсутствии») или запрещать («Запрет доступа при наличии») на других объектах;
- устанавливать и снимать вручную в карточке персоны (глава 12).

Периметр АПБ — зона с запретом повторного прохода: объекты-участники задают входы и выходы, система отслеживает присутствие субъектов внутри. Параметры периметра:

- «Режим нарушения»: «Жёсткий (запрет)» — повторный вход или выход без входа запрещаются; «Мягкий (только журнал)» — проход разрешается, нарушение фиксируется;
- «Задержка повторного входа, сек» - возможность запросить повторный проход в течении короткого времени, если например открыл дверь но не пошел и закрыл;
- «Запрет выхода по внутренней карте» — выход из периметра только по обычным картам (защита от передачи внутренних карт);
- «Автосброс, мин» — автоматическая очистка присутствия по истечении заданного времени.

Списание кратности — правило, превращающее подтверждённый проход через объект в списание одного прохода из кратности пропуска (лимита «N из M», глава 12). У правила задаются название, «Льготное окно, мин» и описание; на объекте оно отображается меткой «Крат: ‹название›» в блоке «Входит в категорию». Правило применимо только к типам объектов с подтверждаемым проходом (двери обоих типов, турникет, шлагбаум).

Льготное окно задаёт, когда именно списывается проход после входа. Полная логика:

- **вход** через объект с правилом начинает визит: система ждёт выхода в течение льготного окна, списания в этот момент нет;
- **выход в пределах окна** списывает один проход — визит оплачен при выходе;
- **окно истекло раньше выхода** — проход списывается автоматически по истечении окна, даже если субъект ещё внутри или вышел незафиксированно;
- **выход без зафиксированного входа** ничего не списывает;
- при льготном окне «0» каждый вход списывается почти сразу;
- один вход списывает не более одного прохода: повторные сигналы и гонка «выход одновременно с истечением окна» двойного списания не дают.

Кратность проверяется при каждом решении о доступе **на вход**: пропуск с исчерпанной кратностью доступа на вход не получает. **Выход разрешён всегда**, даже при исчерпанной кратности, и квоту не проверяет — иначе после списания по окну было бы не выйти. Каждое списание фиксируется в журнале отдельным событием с моментом («При выходе» / «По истечении льготного окна») и остатком проходов.

Пропуска без конечного счётчика (безлимитные) правило не затрагивает: вход по ним не ограничивается и списаний не создаёт. Проверка на входе использует доступный остаток — записанный остаток за вычетом списаний, которые уже произошли, но ещё не перенесены в счётчик, — поэтому и списание, и пополнение кратности (глава 12) действуют на решение о доступе немедленно.

Маршрут — именованный набор проходных объектов доступа, через которые пропуск получает доступ, как будто ему выдан тег на все точки маршрута, но без классов «вход/выход» и без привязки к направлению считывателя. Маршрут назначается на пропуск (глава 12); на объекте отображается меткой «Марш: ‹название›» в блоке «Входит в категорию». Каталог маршрутов — раздел 11.10.

Учёт присутствия (УРВ) — наблюдательный механизм рабочего времени: фиксирует интервалы «время в зоне» или «время сессии» для персон, явно включённых в зону. На решение о доступе **не влияет**. Бейдж «Уч: ‹название›» ставится на проходные объекты и шкафы; членство персоны задаётся в карточке персоны (глава 12). Закрытие интервала пишет событие в журнал (домен «Учёт присутствия», глава 13). Каталог и монитор — раздел 11.11.

11.7. Производственный календарь

Секция «Производственный календарь» панели инструментов — справочник типов дней по годам: «Рабочий», «Выходной», «Праздник», «Сокращенный». Календарь года загружается из открытых внешних источников при наличии интернета (провайдеры isDayOff и xmlCalendar публикуют принятый в России производственный календарь) и правится вручную. Когда сеть недоступна, год заполняет провайдер «Сгенерировать»: суббота и воскресенье становятся выходными, праздников нет — праздничные и перенесённые дни администратор отмечает вручную. Объекты с включённым учётом календаря применяют его в правилах доступа (раздел 11.4): для выходных и праздничных дней доступ не разрешается.

11.8. Панель «Текущий доступ»

Оперативная картина в трёх вкладках (обновляется автоматически, статус соединения показан в заголовке):

- **«Присутствие»** — кто сейчас внутри каждого периметра АПБ: персона, время входа, объект входа. Кнопки «Сбросить присутствие» (по персоне) и «Сбросить все» (по периметру) выполняют операторский сброс АПБ — например, после эвакуации или сбоя учёта;
- **«Активные условия»** — у кого какие условия действуют и до какого времени; условие можно снять;
- **«Активные сессии»** — открытые сессии доступа объектов: объект, тип сессии («Сервис шкафа», «Открыто оператором», «Заблокировано»), персона, длительность. Кнопка «Сбросить сессию» принудительно завершает сессию — например, если инженер ушёл, не закрыв шкаф штатно.

Сбросы фиксируются в журнале с оператором-инициатором.

11.9. Панель «События»

Панель показывает события доступа и аудит объектов: решения «Разрешено» / «Запрещено» с причиной, эпизоды сессий, нарушения, а также изменения настроек объектов с перечнем изменений «было/стало». Причина решения показывается в строке события и в карточке, например: «Разрешено по пропуску», «Разрешено с подтверждением», «Доступ запрещён: нет прав на этот объект», «Неверный PIN-код», «Запрет повторного прохода: повторный вход», «Доступ запрещён: вне разрешённого расписания», «Доступ запрещён: нерабочий день по производственному календарю». Проникновение без права в открытую дверь (раздел 4.3) фиксируется тревогой «Проход без разрешения».

Переключатель «Выбранные» сужает ленту до выбранного объекта — его события доступа и история изменений в одной ленте. Приёмы работы с лентой — в главе 8.

11.10. Каталог «Маршруты»

Секция **«Маршруты»** панели инструментов — каталог именованных маршрутов. Маршрут назначается:

- на пропуск — в диалоге выдачи и в карточке пропуска (список маршрутов пропуска);
- на объект доступа — меткой «Марш: ‹название›» в блоке «Входит в категорию» (раздел 11.6); допустимо только на проходных типах (двери обоих типов, турникет, шлагбаум).

В каталоге задаются название и описание. Маршрут можно назначить или снять массовой операцией «Установка маршрута» на выбранных объектах. Удаление записи из каталога не снимает метки с объектов и пропусков — они останутся, но ссылка на каталог будет потеряна.

11.11. Каталог «Учёт присутствия»

Секция **«Учёт присутствия»** панели инструментов — каталог бейджей учёта рабочего времени.

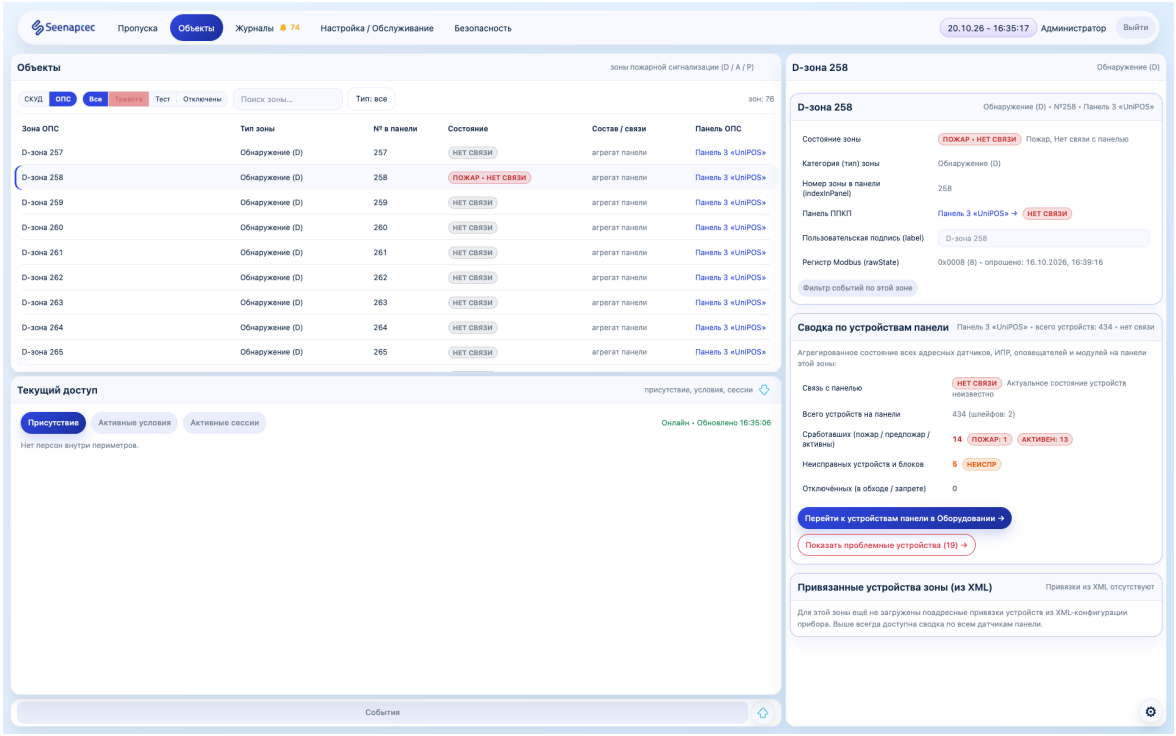
Каталог. Для каждой зоны задаются название, описание и «Таймаут закрытия, сек» — через это время «зависший» интервал закрывается автоматически и помечается в журнале как недостоверный (`0` = не закрывать по таймауту). Зона назначается:

- на объект — меткой «Уч: ‹название›» (проходные объекты и шкафы);
- на персону — секция «Учёт присутствия» в карточке персоны (глава 12): интервалы пишутся **только** для персон с явным членством в зоне.

Учёт присутствия не заменяет периметр АПБ (раздел 11.8): АПБ может запрещать доступ, УРВ — только наблюдает время.

11.12. Объекты ОПС (пожарные зоны D, A, P)

При переключении пилюли **`СКУД | ОПС`** в верхней строке в положение **`ОПС`** рабочая область «Объекты доступа» (в шапке отображается как **«Объекты»**) переходит в режим мониторинга и оперативного управления пожарными зонами ОПС. Зоны создаются автоматически при опросе состава подключённых панелей UniPOS IFS7000 и обогащаются пользовательскими именами и привязками датчиков при загрузке проектного файла `.xml` (раздел 10.9).



Левая панель списка зон и фильтрация

В левой панели отображается сводный список всех пожарных зон подключённых панелей с колонками `Зона`, `Тип`, `Панель` и `Состояние`. Над списком расположены элементы быстрого отбора:

- **быстрый фильтр состояний `Все | Тревога | Тест | Отключены`** — сегментированный переключатель для мгновенного отбора зон по оперативному режиму. При наличии в системе хотя бы одной зоны в состоянии пожара, предтревоги или активного пуска кнопка **«Тревога»** пульсирует красным цветом и показывает счётчик тревожных зон;
- **поиск и мультиселект типа зоны** — строка текстового поиска по названию/номеру зоны и выпадающий фильтр **`Тип: Обнаружение (D) | Оповещение (A) | Автоматика (P)`**, позволяющий оставить в списке один или несколько типов зон.

Если панель UniPOS теряет связь с сервером по Modbus TCP, все её зоны в списке отображают достоверный статус **«НЕТ СВЯЗИ»**.

Типы зон и фазы состояния в UniPOS

Платформа поддерживает все три типа логических зон панелей UniPOS серии IFS7000 и различает их аппаратные фазы состояния:

1. **Зона обнаружения (`D`, Detection)** — объединяет автоматические пожарные извещатели (дымовые, тепловые, комбинированные, газовые) и ручные извещатели (`ИПР`) защищаемого помещения:
   - **`Норма`** — дежурный режим контроля;
   - **`Предтревога`** — предварительный сигнал срабатывания (этап верификации или одиночный датчик до формирования общего пожара);
   - **`Пожар`** — подтверждённая пожарная тревога в зоне с явным указанием источника срабатывания: **от ручного извещателя** (`ИПР`) или **от автоматического датчика**;
   - **`Неисправность`** — отказ, обрыв или потеря связи с извещателем зоны;
   - **`Тест`** — зона переведена оператором в режим сервисной проверки извещателей;
   - **`Отключена / Обход`** — зона временно выведена из формирования тревог.
2. **Зона оповещения (`A`, Alarm / Notification)** — управляет контурами звукового, речевого и светового оповещения и разделяет три фазы работы прибора UniPOS по битовой маске регистра состояния:

- **Предупреждение (Пожар 1)** (warning, бит 0x0040) — первая фаза тревоги (локальное предупреждение персонала до общего пуска эвакуации);
- **Задержка пуска** (delayed, бит 0x0010) — идёт отсчёт программируемой задержки перед включением оповещателей Второй фазы;
- **Срабатывание / Оповещение активно (Пожар 2)** (active, бит 0x0008) — активный пуск сирен и табло оповещения в зоне. Дополнительно для зоны A отслеживаются состояния Норма, Неисправность и Отключена / Обход.

3. **Зона автоматики (P, Automation / Protection)** — управляет исполнительными контурами противопожарной автоматики (дымоудалением, огнезадерживающими клапанами, вентиляцией, установками пожаротушения и модулями FPE):
   - **Задержка пуска** (delayed, бит 0x0010) — идёт предымпульсная задержка перед пуском исполнительных механизмов автоматики;
   - **Срабатывание зоны автоматики** (active, бит 0x0008) — выполнен пуск противопожарной автоматики в зоне;
   - **Норма**, **Неисправность** и **Отключена / Обход** — штатный дежурный режим, неисправность цепей пуска или обход зоны.

Карточка зоны ОПС и команды оператора

При выборе зоны в правой области открывается её карточка:

- **Сводка состояния и свойства** — номер и редактируемое название зоны, тип (Зона обнаружения (D), Зона оповещения (A) или Зона автоматики (P)), принадлежность к панели ОПС, текущая фаза состояния, источник тревоги и детальные флаги прибора.
- **Команды оперативного управления** (доступны при наличии прав на управление в подсистеме ОПС):
  - для **зоны обнаружения (D)**: **«Взять на контроль»** (возврат в дежурный режим из теста или обхода), **«Режим теста»** (перевод зоны в режим проверки извещателей) и **«Отключить (обход)»** (временное отключение зоны);
  - для **зоны оповещения (A)** и **зоны автоматики (P)**: **«Взять на контроль»**, **«Пуск»** (дистанционная активация оповещения или контура автоматики), **«Останов / Сброс»** (останов пуска и сброс срабатывания зоны) и **«Отключить (обход)»**.
- **Привязанные устройства («Состав зоны»)** — таблица всех адресных извещателей, модулей и выходов БИО, входящих в выбранную зону (заполняется при импорте XML-конфигурации прибора или привязке объектов), с отображением их адресов, типов, текущих состояний и переходом в карточку устройства в рабочей области «Настройка / Обслуживание».

Глава 12. Пропуска

Рабочая область «Пропуска» — рабочее место бюро пропусков: персоны, идентификаторы и выдача пропусков. Левые панели области — «Пропуска», «События», «Идентификаторы»; на панели инструментов — «Шаблоны доступов», «Шаблоны идентификаторов», «Дополнительные поля персонала», «Авто-очистка».

12.1. Ключевой принцип: пропуск — документ

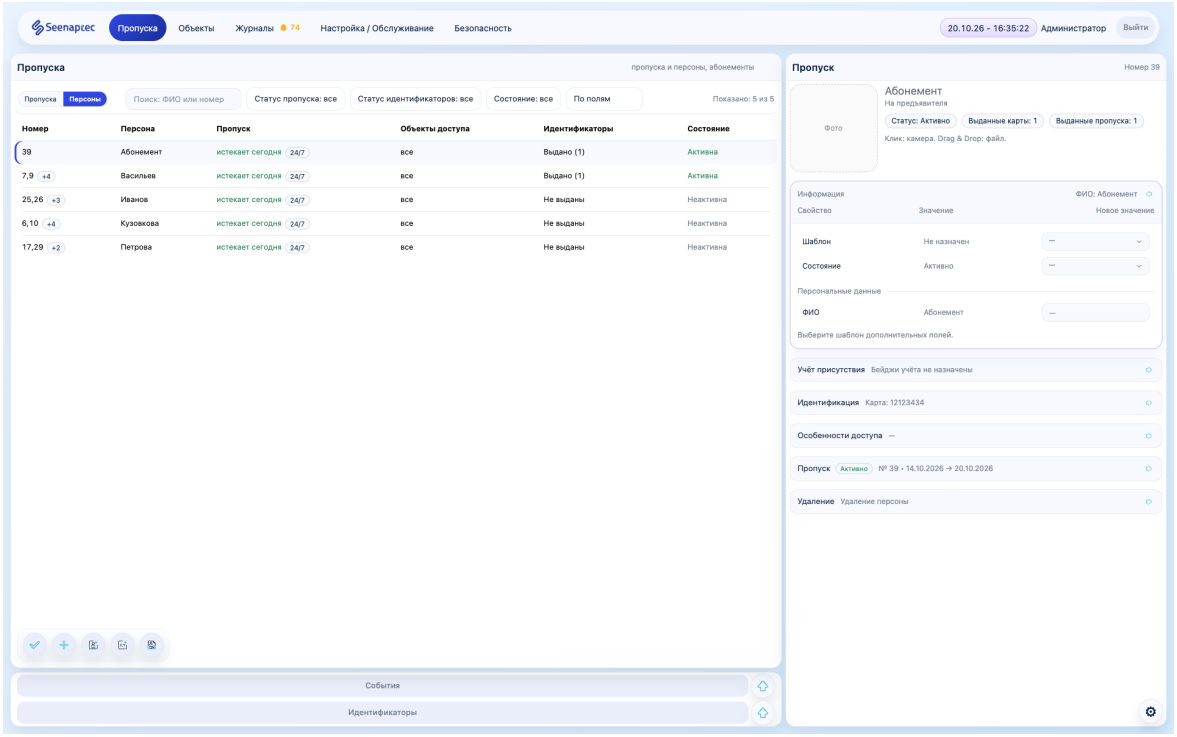
> **Для знакомых с классическими СКУД.** В классической системе доступ описывается «уровнем доступа», присвоенным карте: карта и есть право. Здесь право — это **пропуск**: самостоятельный документ, который отвечает на все вопросы о доступе разом — *кому* (персона), *чем* (привязанные идентификаторы), *куда* (объекты доступа и теги), *когда* (срок и время доступа) и *сколько раз* (кратность). Карта — лишь один из идентификаторов, привязанных к пропуску; у персоны может быть несколько пропусков с разными правами и сроками одновременно. Роль «типовых уровней доступа» играют **шаблоны доступов** (раздел 12.5) — заготовки пропусков, а предварительное согласование оформляется **заявкой** (раздел 12.4) — документом, резервирующим номер до фактической выдачи.

Пропуск в системе устроен как документ строгой отчётности:

- **номер** присваивается сервером и никогда не переиспользуется;
- после выдачи изменению подлежат только: продление срока (дата окончания — только позже), пополнение кратности, привязка и отвязка идентификаторов, сопровождающий и состояние (приостановка и возврат в действие);

- персона, дата начала, время доступа, набор объектов и тегов выданного пропуска **не меняются** — если доступ нужен другой, выдаётся новый пропуск;
- каждое действие с пропуском фиксируется в журнале аудита.

12.2. Панель «Пропуска»



Панель «Пропуска» предназначена для просмотра персон и пропусков, поиска записей, создания персон, выдачи пропусков и выполнения массовых операций.

Режимы отображения

Переключатель **«По персонам»** изменяет состав списка:

- переключатель «Пропуска» активен — каждая строка соответствует отдельному пропуску;
- переключатель «Персоны» активен — каждая строка соответствует персоне, включая персон без пропусков.

При переключении между режимами «Пропуска» и «Персоны» выбранная персона сохраняется; в режиме «Пропуска» для неё автоматически выделяется актуальный пропуск.

В списке отображаются колонки:

- **«Номер»**;
- **«Персона»**;
- **«Пропуск»**;
- **«Объекты доступа»**;
- **«Идентификаторы»**;
- **«Состояние»**.

В колонке **«Пропуск»** отображается краткая информация о сроке и состоянии пропуска, например:

- «действует до … · ещё N дн»;
- «закончился N дней назад»;
- «приостановлен»;
- «бессрочно»;
- «заявка»;
- «не выдан».

Значок **«24/7»** обозначает пропуск без ограничений по времени доступа. Чтобы просмотреть точные даты действия и профиль времени доступа, наведите указатель на ячейку.

В колонке **«Состояние»** отображается текущее состояние персоны: «Активна», «Неактивна», «Заблокирована» или «В черном списке».

Отображение нескольких пропусков

В активном режиме **«Персоны»** колонка **«Номер»** содержит номера первых двух пропусков персоны. Если пропусков больше, рядом отображается значок **«+N»**. Наведите на него указатель мыши, чтобы просмотреть остальные номера.

Срок действия и объекты доступа в строке персоны отображаются по одному пропуску, выбранному по следующим правилам:

1. Если есть действующие пропуска, то отображается пропуск с ближайшей датой окончания.
2. Если действующих пропусков нет, но есть пропуска, срок которых ещё не начался, то отображается ближайший по дате начала пропуск.
3. Если все пропуска истекли, отображается пропуск с наиболее поздней датой окончания.

При одинаковом приоритете действующий пропуск отображается раньше приостановленного. Бессрочный пропуск учитывается после пропусков с установленной датой окончания.

Заявка отображается как основной документ персоны только при отсутствии выданных пропусков. Полный список пропусков доступен в карточке персоны, в секциях «Пропуск» и «Доп. пропуск».

Поиск и фильтрация

Для отбора записей доступны:

- текстовый поиск по номеру, ФИО и названию;
- фильтр по сроку: «Актуальные», «Просрочено», «Не наступило»;
- фильтр по ближайшей дате: «Сегодня», «Завтра», «На этой неделе»;
- фильтр по объекту доступа;
- фильтр по времени доступа;
- фильтр по статусу пропуска: «Активно», «Приостановлено», «Ожидает», «Истекло», «Заявка».

Чтобы применить фильтр со списком значений, откройте список, выберите одно значение и нажмите кнопку подтверждения.

В режиме **«По персонам»** дополнительно доступны:

- фильтр по статусу выдачи: «Выдано (N)», «Изъято», «Не выдавалось»;
- кнопка **«По полям»** для поиска по дополнительным полям персон.

Поиск по дополнительным полям поддерживает до трёх условий. Набор условий можно сохранить в дальнейшем как шаблон поиска.

Создание персон и пропусков

В нижней части панели первой расположена кнопка включения режима множественного выбора, за ней — кнопки создания записей:

1. **«Новый пропуск»** — создаёт пропуск или заявку. Если в списке выбрана персона либо её пропуск, данные персоны подставляются автоматически.
2. **«Новая персона»** — открывает диалог создания персоны (с возможностью сразу перейти к выдаче пропуска кнопкой **«Создать и выдать пропуск»**).
3. **«Выдать пропуск выделенной персоне»** — открывает окно выдачи пропуска для выбранной в списке персоны. Кнопка недоступна, если персона не выбрана или находится в чёрном списке.

Полный перечень пропусков персоны всегда виден в её карточке (секции «Пропуск» и «Доп. пропуск», раздел 12.4).

Доступность кнопок, колонок и секций зависит от полномочий оператора системы. Если действие оператору запрещено, кнопка блокируется с пояснением причины; если у оператора есть право чтения персон без права чтения пропусков, интерфейс работает в режиме картотеки персон без колонок и секций пропусков и идентификаторов. Для операторов

с полномочием ограниченной выдачи процедура оформления пропуска строится на основе разрешённых шаблонов доступа (раздел 12.5).

Массовые операции и удаление

Чтобы выбрать несколько записей, включите режим множественного выбора. Доступные действия появятся в панели массовых операций.

В режиме «По персонам» панель массовых операций содержит секции **«Выдача пропусков»**, **«Установка зоны учёта»** и **«Удаление»**. В секции «Выдача пропусков» выберите шаблон доступа (раздел 12.5), проверьте его состав (период, время доступа, кратность, теги и объекты доступа) и нажмите «Применить» — выбранным персонам выдаются новые действующие пропуска по шаблону, а ход выполнения отображается в колонке «Состояние» каждой строки.

Удаление выполняется:

- для одной записи — из карточки персоны или пропуска;
- для нескольких записей — через панель массовых операций.

Перед удалением система запрашивает подтверждение и показывает перечень затрагиваемых записей.

12.3. Персона

> **Для знакомых с классическими СКУД.** Классическая «карточка сотрудника» — фиксированный набор граф, одинаковый для всех: табельный номер, отдел, должность. Здесь у персоны фиксированы только базовые атрибуты (ФИО, фотография, состояние), а остальной состав карточки определяется **шаблоном полей персонала** (раздел 12.8): организация сама описывает нужные поля — их названия, категории и типы значений (строка, целое, логическое, перечисление с собственным списком вариантов), признаки обязательности и уникальности — и собирает из них шаблоны под разные категории людей. Сотруднику — табельный номер и отдел, посетителю — документ и принимающая сторона, подрядчику — организация и срок договора; смена шаблона не теряет заполненные вне его поля.

Персона создаётся в двухколоночном диалоге «Новая персона»: слева указываются фотография, «ФИО / название», тип («Персона» — конкретный человек, «На предъявителя» — обезличенный носитель) и состояние; справа выбирается «Шаблон» полей персонала (раздел 12.8) и заполняются дополнительные поля выбранного шаблона (обязательные поля отмечены звёздочкой). Кнопка **«Создать»** сохраняет карточку персоны и значения полей шаблона; кнопка **«Создать и выдать пропуск»** сохраняет персону и сразу открывает для неё диалог выдачи пропуска (раздел 12.4). При выборе состояния «В черном списке» или отсутствии у оператора права выдачи пропусков кнопка «Создать и выдать пропуск» блокируется.

Фотография. Поле фотографии (в диалоге создания и в карточке персоны) заполняется двумя способами: щелчок открывает съёмку камерой компьютера, а файл с изображением можно просто перетащить на поле. Снимок автоматически ужимается до 640×480 точек; если прямой доступ к камере недоступен, диалог предлагает выбрать файл с устройства. Наведение указателя на фотографию — в карточке персоны, в карточке идентификатора или при выборе персоны в диалоге выдачи — плавно увеличивает её (до трёх раз или до границ окна); увеличенная копия исчезает, как только указатель уходит с миниатюры.

Карточка персоны (общая с пропуском) состоит из секций:

- **«Информация»** — состояние («Активна», «Приостановлена», «В черном списке»), персональные данные и **дополнительные поля** по назначенному шаблону полей: организационные данные, контакты, служебные данные и другие категории. Состав полей настраивается в секции «Дополнительные поля персонала» панели инструментов (раздел 12.8).
- **«Идентификация»** — карты персоны: добавление, изъятие, перевыпуск (раздел 12.6).
- **«Особенности доступа»** — параметры, влияющие на решения о доступе:
  - подтверждение на режимных точках (двойной контроль): «Требует подтверждения» — персона проходит режимную точку «Карта + подтверждение» (глава 11) только после предъявления карты подтверждающего; «Может подтверждать» — персона вправе подтверждать проход других, в том числе сопровождать гостей (раздел 12.4). Признаки взаимоисключающие: персона либо сама нуждается в подтверждении, либо подтверждает других — сохранение карточки с обоими признаками отклоняется с ошибкой;
  - «Пин код подтверждения» — PIN из 4–12 цифр для объектов с режимом «карта + PIN»; показывается только признак «PIN установлен», сам код прочитать нельзя;

  - условия персоны — именованные признаки (допуски, инструктажи), которые проверяются правилами объектов доступа (глава 11);
  - **«Учёт присутствия»** — зоны рабочего времени, в которых персона участвует в учёте интервалов (раздел 11.11): интервалы пишутся только при явном членстве; на доступ это не влияет.
- **«Пропуск»** — выбранный пропуск персоны (раздел 12.4); прочие её пропуска показаны свёрнутыми секциями «Доп. пропуск». В заголовке каждой секции пропуска — цветной индикатор состояния («Активно», «Приостановлено», «Ожидает», «Истекло», «Заявка»), в свёрнутом виде — сводка «№ N • период».
- **«Удаление»** — свёрнутая секция в конце карточки: удаление персоны изымает её пропуска и отвязывает идентификаторы, история в журнале сохраняется. Кнопка удаления подтверждается в правой зоне. Групповое удаление персон выполняется в режиме выбора через панель массовых операций.

Состояние «В черном списке» блокирует персону: выдача пропусков ей недоступна.

12.4. Выдача пропуска и заявки

Кнопки «Новый пропуск» и «Выдать пропуск выделенной персоне» открывают общий диалог выдачи. В верхней части — переключатель типа документа: **«Пропуск» | «Заявка»**.

Пропуск оформляется сразу: слева — персона (существующая или созданная тут же) и карта; справа — секция «Доступ»: даты начала и окончания, время доступа («Без ограничения», «Нормальное», «Сокращенное», «Расширенное» — профили длительности, глава 11), кратность (лимит проходов), сопровождающий (гостевой доступ), теги, маршруты и объекты доступа (для двусторонних объектов доступ можно ограничить конкретным направлением или стороной: «Вход» / «Выход», а у двустороннего серверного шкафа — «Передняя» / «Задняя»). Даты согласуются автоматически: если дату начала установить позже даты окончания, окончание подтягивается к новому началу (бессрочное окончание при этом не затрагивается).

При открытии диалога кнопкой **«Выдать пропуск выделенной персоне»** (или после нажатия **«Создать и выдать пропуск»** в диалоге создания персоны) персона в левой колонке зафиксирована для чтения: фотография, «ФИО / название» и тип не редактируются, чтобы исключить случайную перезапись карточки человека при оформлении пропуска. Под заголовком «Идентификация» выводится название назначенного шаблона персоны (либо её тип), а раскрываемая «Сводка» показывает шаблон и заполненные дополнительные поля персоны.

Сопровождающий (гостевой доступ). Поле «Сопровождающий (гостевой доступ)» назначает пропуску сотрудника, отвечающего за посетителя. На точке, где у гостя нет собственного доступа, сценарий такой: гость предъявляет карту первым — система открывает окно ожидания 15 секунд; сопровождающий предъявляет свою карту на том же считывателе — доступ разрешается. Подтверждение засчитывается, только если в момент предъявления у сопровождающего есть признак «Может подтверждать» и собственный действующий доступ к этому объекту. Спонсируется только отсутствие права: отказы по другим причинам (просроченный пропуск, запрет повторного прохода, условия, исчерпанная кратность) сопровождающий не перекрывает. Там, где у гостя собственный доступ есть, он проходит сам, без сопровождающего.

Теги, маршруты и классы доступа. Тег даёт пропуску доступ ко всем объектам с совпадающей меткой (глава 11). **Маршрут** — именованный набор проходных объектов: пропуск получает доступ ко всем точкам маршрута без классов «вход/выход» (раздел 11.10); в диалоге выдачи маршруты выбираются в секции «Доступ» рядом с тегами и объектами. Если среди объектов тега есть типы с направлениями, под выбранными тегами появляется блок «Класс доступа по тегу (по умолчанию — все направления)»: для группы «Турникеты» кнопками «Вход» / «Выход» доступ по тегу сужается до одного направления — например, разовый пропуск «только на выход». Помните о правиле приоритета: объект, добавленный в пропуск явно (в списке «Объекты доступа»), подчиняется только явному указанию — ограничения тегов на него не действуют.

Персона и карта в диалоге. Пока поле персоны пусто, чтение карты подставляет её владельца автоматически. Если персона уже выбрана или введена, выбор карты, принадлежащей другой персоне, означает **изъятие**: у поля карты появляется отметка «Будет изъята у …», а при сохранении карта отвязывается от прежнего владельца и выдаётся персоне текущего пропуска (персона в диалоге при этом не меняется). Смена персоны или карты не сбрасывает выбранный шаблон и состав секции «Доступ». Если карта жёстко закреплена за конкретным пропуском прежнего владельца, сохранение завершится ошибкой — сначала уберите карту из того пропуска.

Вместо ручного заполнения можно выбрать «Шаблон доступа» — он заполнит период, время, кратность и набор доступа (раздел 12.5). Первые шаблоны показаны в верхней строке диалога кнопками быстрого выбора — столько, сколько

помещается по ширине; остальные собраны в раскрывающийся список «ещё…». Правило периода шаблона превращается в конкретные даты в момент выбора, после чего все поля можно править вручную (кроме режима ограниченной выдачи, где состав доступа задаётся строго шаблоном).

Заявка резервирует номер пропуска и данные, но не даёт доступа: указываются только период и обязательный комментарий; объекты и время доступа назначаются при выпуске. Заявка видна в списке со статусом «Заявка»; в её карточке доступны действия:

- **«Выпустить пропуск»** — открывает диалог «Выпуск пропуска по заявке № N»: назначаются объекты и время доступа, заявка становится действующим пропуском;
- **«Отклонить»** — заявка удаляется; действие фиксируется в журнале.

Типовой сценарий: стойка регистрации или внешняя система создаёт заявку, бюро пропусков выпускает пропуск.

Карточка выданного пропуска (секция «Пропуск»): состояние показано цветным индикатором в заголовке секции; поля — номер, период (продлевается только дата окончания, в том числе до бессрочного), кратность («N из M» — пополняется только вверх), привязка «По идентификаторам» (ограничение действия пропуска конкретной картой персоны; значение «- Нет -» снимает привязку, чтобы пропуск действовал по любому активному идентификатору персоны), сопровождающий. Время доступа, теги и объекты показываются только для чтения — по принципу документа (раздел 12.1).

Строка «Номер» — ссылка «Пропуск № N»: в основной секции «Пропуск» она показывает строку пропуска в режиме «По пропускам»; в секции «Доп. пропуск» — выбирает этот пропуск, делая его секцию основной. Редактирование полей документа (даты, кратность, идентификаторы, сопровождающий) доступно только в основной секции; секции «Доп. пропуск» показывают пропуск для чтения и предлагают приостановку, удаление и переход.

Приостановка и возврат в действие выполняются кнопкой **«Приостановить» / «Возобновить»** в нижнем ряду действий секции (рядом с «Удалить пропуск»); обе операции требуют полного уровня прав по пропускам и применяются сразу, без сохранения карточки. Для ещё не начавшегося пропуска («Ожидает») приостановка недоступна; у заявки вместо неё — «Отклонить».

Изъятие пропуска — его удаление: красная кнопка «Удалить пропуск» внизу секции пропуска (есть и в «Пропуск», и в «Доп. пропуск»); подтверждение называет конкретный документ — «Пропуск № N будет удалён (изъят)». Требуется полный уровень прав по пропускам. История пропуска сохраняется в журнале, номер не переиспользуется. У заявки вместо удаления — кнопка «Отклонить». Групповое удаление пропусков выполняется в режиме выбора через панель массовых операций.

12.5. Шаблоны доступов и ограниченная выдача

Секция **«Шаблоны доступов»** панели инструментов — заготовки пропусков. Шаблон хранит:

- «Правило периода» — «На сегодня», «На завтра», «На неделю», «До даты»: правило превращается в конкретные даты в момент выдачи;
- «Время доступа» и «Кратность»;
- объекты доступа и теги;
- флаг **«Ограниченная выдача»** — разрешение использовать шаблон операторам уровня «выдача по шаблону».

Ограниченная выдача — режим для стоек регистрации и приёма посетителей: оператор с уровнем «выдача по шаблону» (глава 14) может выдавать пропуска **только** по шаблонам с этим флагом. В диалоге выдачи такой оператор выбирает шаблон из разрешённых, персону и существующую карту; состав доступа показан только для чтения и отклоняться от шаблона нельзя. Установка и снятие флага требуют полного уровня прав на шаблоны — набор «того, что доступно на стойке», контролирует офицер безопасности.

12.6. Панель «Идентификаторы»

Панель «Идентификаторы» предназначена для учёта карт доступа независимо от выданных пропусков. Идентификатор используется для распознавания системой персоны, а права доступа определяются связанным пропуском.

В списке отображаются:

- **«Код»**;
- **«Действует с»**;

- **«Действует по»**;
- **«ФИО»**;
- **«Состояние»**.

Возможные состояния идентификатора:

- **«Активно»** — идентификатор выдан персоне и может использоваться;
- **«Неактивно»** — идентификатор создан, но не выдан персоне;
- **«Приостановлено»** — использование временно запрещено;
- **«Утеряно»** — идентификатор отмечен как утраченный и отвязан от персоны;
- **«Изъят»** — идентификатор выведен из обращения;
- **«Ожидает»** — срок действия ещё не начался;
- **«Истекло»** — срок действия завершён.

Вид идентификатора показывается в списке пометкой, доступна фильтрация по виду. Вид **«Аварийная»** — карта аварийного открывания: такая карта открывает объект при потере устройством связи с сервером, если на объекте включено аварийное открывание по картам (раздел 11.3); на один объект действует не более трёх аварийных карт. Пометка «Аварийная» выделяется красным.

Создание идентификатора

Идентификатор можно создать двумя способами.

Из панели «Идентификаторы»

1. Нажмите кнопку **«+»**.
2. В диалоге «Добавить идентификатор» укажите:

- **«Шаблон»**;
- **«Код»**;
- **«Вид»**: «Обычная», «Внутренняя», «Контрольная» или «Аварийная»;
- дату начала и срок действия.

3. Сохраните запись.

Созданный идентификатор получает состояние «Неактивно» и не связывается с персоной. Такой способ используется для предварительного формирования запаса карт в бюро пропусков.

Чтобы позднее выдать идентификатор новой персоне, откройте его карточку и нажмите **«Выдать текущей»** либо выберите его при оформлении пропуска.

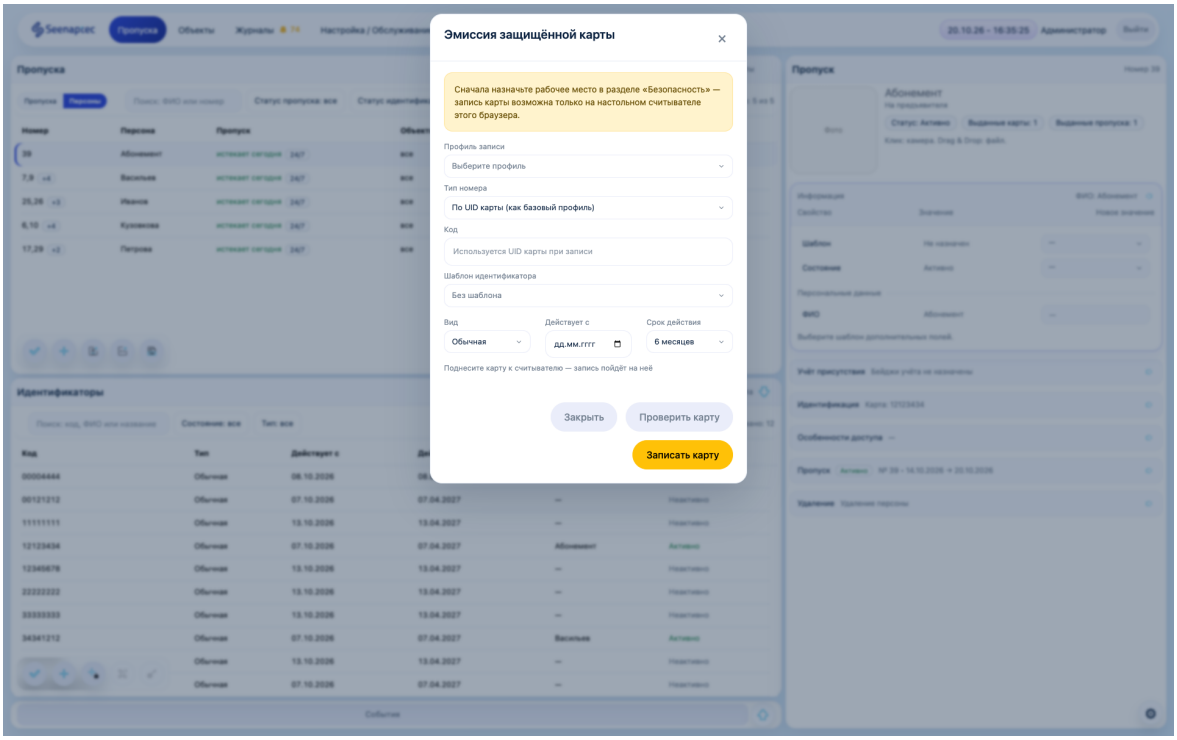
Из карточки персоны

1. Откройте карточку персоны.
2. В секции «Идентификация» нажмите кнопку **«+»**.
3. В блоке «Новый идентификатор» укажите шаблон, код, вид, дату начала и срок действия.
4. Нажмите кнопку **«Сохранить»**.

Идентификатор создаётся и сразу связывается с выбранной персоной. Кнопка **«Сбросить»** закрывает блок без сохранения.

Эмиссия защищённой карты

Эмиссия — запись кода в защищённую зону карты на настольном считывателе с одновременным созданием идентификатора в системе. Выполняется на АРМ считывателя (раздел 14.8) по профилю карт из библиотеки (раздел 14.9); требуется полный уровень прав на пропуска.



1. В панели «Идентификаторы» нажмите кнопку **«Эмиссия защищённой карты»**.
2. Выберите **«Профиль записи»** — профиль технологии MIFARE или DESFire из библиотеки.
3. Выберите **«Тип номера»** — источник кода идентификатора. Во всех режимах код записывается в защищённую зону карты; режимы различаются источником кода:
   - **«По UID карты (как базовый профиль)»** — код совпадает с UID карты;
   - **«Вручную»** — код задаёт оператор;
   - **«Привязка к UID»** — код вычисляется из UID карты функцией SHA-256, не совпадает с UID и читается только считывателями с secure-профилем.
4. Задайте параметры идентификатора — шаблон, вид, дату начала и срок действия, как в диалоге «Добавить идентификатор».
5. Поднесите карту к настольному считывателю и нажмите **«Записать карту»**. Держите карту на считывателе до завершения — ход операции показывается лентой сообщений диалога.

Кнопка **«Проверить карту»** выполняет пробу состояния карты без записи — для любого профиля (MIFARE и DESFire): диалог показывает уровень и состояние карты и подсказывает, возможна ли запись выбранным профилем. Если карта не готова к записи (заводская MIFARE Plus, DESFire без приложения профиля, повреждённая структура DESFire), диалог предлагает перейти к инициализации карты — подготовка карты выполняется там.

Эмиссия требует: АРМ на связи, браузеру назначено рабочее место АРМ (раздел 14.8), ключи профиля заведены в хранилище секретов (раздел 14.5) — иначе диалог сообщит, что ключи не найдены.

Действия с идентификатором

В карточке идентификатора доступны следующие действия:

- **«Забрать»** — отвязать идентификатор от персоны;
- **«Выдать текущей»** — связать идентификатор с персоной, выбранной в панели «Пропуска»;
- **«Заблокировать»** — запретить использование идентификатора;
- **«Разблокировать»** — восстановить возможность использования;
- **«Перевыпустить»** — заменить идентификатор новым с сохранением необходимых связей;
- **«Удалить идентификатор»** — удалить запись после подтверждения операции.

Доступность действий зависит от текущего состояния идентификатора и полномочий оператора.

Перевыпуск идентификатора

Операция **«Перевыпустить»** используется для замены карты без изменения пропусков персоны.

1. Откройте карточку идентификатора или карточку персоны.
2. В секции «Идентификация» нажмите кнопку **«Перевыпустить»**.
3. Укажите новый код вручную или считайте его контрольным считывателем.
4. Проверьте отметку **«Будет отвязан»** у прежнего кода идентификатора.
5. Нажмите кнопку **«Сохранить»**.

Во время перевыпуска идентификатора остальные поля секции недоступны.

После сохранения:

- прежний идентификатор получает состояние «Изъят» и отвязывается от персоны;
- создаётся идентификатор с новым кодом;
- сохраняются вид идентификатора и его связи с персоной и пропусками;
- в журнале регистрируются связанные события изъятия и выдачи.

Новый идентификатор получает такой же срок действия, какой был установлен для прежнего, но дата начала отсчитывается от даты перевыпуска. Бессрочный идентификатор остаётся бессрочным.

Перевыпуск карты

Перевыпуск карты записывает дубликат существующего кода идентификатора на новую защищённую карту — картотека при этом не меняется (в отличие от перевыпуска идентификатора, который заводит идентификатор с новым кодом). Кнопка **«Перевыпуск карты»** в панели «Идентификаторы» активна при открытой карточке идентификатора и требует полного уровня прав на пропуска.

1. Откройте карточку идентификатора и нажмите **«Перевыпуск карты»**.
2. Выберите **«Профиль записи»** — целевой профиль новой карты.
3. Поднесите карту к настольному считывателю. Кнопка **«Проверить карту»** выполняет пробу без записи: диалог покажет состояние карты и подскажет, возможна ли запись выбранным профилем.
4. Нажмите **«Записать карту»**. Держите карту на считывателе до завершения.

В типовом сценарии (карта уже подготовлена под целевой профиль) ключи карты не меняются: если целевой ключ не подошёл, запись отклоняется, карта остаётся нетронутой.

Сценарий **со сменой ключей** доступен при праве «Инициализация карт» (раздел 14.2): в диалоге появляется поле **«Исходный профиль карты»**. Выберите профиль текущих ключей карты — для новой транспортной карты MIFARE это транспортный профиль из библиотеки. Если целевой ключ не подошёл, агент проверит исходный, сменит ключи сектора на целевые и выполнит запись; итог «записано со сменой ключей» виден в ленте диалога и в журнале.

Особые случаи:

- карта MIFARE Plus в заводском состоянии (SL0) и карта DESFire без приложения профиля не записываются — сначала выполните инициализацию карты, диалог предложит переход;
- для карт DESFire смена ключей приложения выполняется только через инициализацию — поле исходного профиля для них не предлагается;
- чужая карта (не открылась ни целевым, ни исходным ключом) не изменяется.

Инициализация карты

Инициализация переводит карту с текущих (транспортных, заводских или чужих) ключей на ключи профиля из библиотеки — без создания идентификатора. Это подготовка новых карт к эмиссии и перевод уже выпущенных карт на новые ключи (re-key). Для карт DESFire инициализация создаёт на карте приложение профиля (идентификатор приложения, файл кода, ключи) — только после этого возможна запись кодов на карту. При инициализации область данных профиля обнуляется: если на карте был записан код, он стирается. Повторная инициализация карты, уже находящейся на ключах профиля (исходный и целевой профили совпадают), — штатный способ обнулить данные на карте без смены ключей. Кнопка **«Инициализация»** в панели «Идентификаторы» требует права «Инициализация карт» (раздел 14.2) и назначенного рабочего места АРМ (раздел 14.8).

1. Нажмите **«Инициализация»**.

2. Выберите **«Исходный профиль (текущие ключи карты)»** — для новой карты MIFARE это транспортный профиль из библиотеки (раздел 14.9); транспортные профили помечены в списке и идут первыми. Для целевого профиля DESFire поле называется **«Исходный профиль (re-key приложения — необязателен)»**: укажите его, только если карта уже несёт приложение на ключах другого профиля (смена ключей приложения); идентификаторы приложения обоих профилей обязаны совпадать.
3. Выберите **«Целевой профиль (новые ключи сектора)»** — профиль MIFARE или DESFire (профили DESFire помечены в списке; для них поле называется «Целевой профиль (приложение и ключи DESFire)»).
4. Для целевого профиля MIFARE Plus выберите **«Целевой уровень Plus»**: «SL3 (AES) — целевой режим, без Classic-совместимости» либо «SL1 — режим Classic, доход в SL3 возможен позже». Персонализация требует admin-ключей Plus в профиле (раздел 14.9).
5. Поднесите карту; при необходимости выполните пробу состояния кнопкой **«Проверить карту»**. Если проба показывает незавершённое приложение DESFire (след обрыва прошлой инициализации), постановка потребует явного подтверждения доигрывания отметкой в диалоге.
6. Подтвердите отметкой понимание риска и нажмите **«Инициализировать»**. Держите карту на считывателе до завершения.

Для целевого профиля DESFire в диалоге доступна кнопка **«Отформатировать карту»** — полный сброс карты к заводскому состоянию с подтверждением (стираются все приложения и ключи, действие необратимо). Форматирование возможно, только если мастер-ключ карты заводской; после форматирования выполните инициализацию.

> **Внимание.** Инициализация и переходы уровней Plus необратимы: перешивка меняет ключи сектора, переход в SL3 навсегда снимает совместимость с MIFARE Classic, а уровень Plus можно только повышать. Если карта уйдёт со считывателя в момент записи, сектор останется на неизвестных ключах — восстановление вне системы невозможно.

Ограничения жизненного цикла

- Код существующего идентификатора изменить нельзя. Для замены кода используйте операцию **«Перевыпустить»**.
- Регистр букв в коде не важен: при сохранении код приводится к нижнему регистру, при предъявлении карты регистр не учитывается.
- Состояние **«Изъят»** необратимо. Такой идентификатор нельзя повторно активировать, выдать или перевыпустить.
- Код изъятого идентификатора остаётся занятым, а связанная с ним история сохраняется.
- Идентификатор в состоянии **«Утеряно»** автоматически отвязывается от персоны. Выдать его повторно можно только после изменения состояния.
- Состояния **«Утеряно»** и **«Изъят»** имеют разное назначение: первое устанавливается при утрате карты, второе — при её перевыпуске.

Шаблоны идентификаторов

Шаблоны настраиваются в секции «Шаблоны идентификаторов» панели инструментов. Шаблон определяет вид идентификатора и правило расчёта срока действия:

- «Бессрочно»;
- «На 3 месяца»;
- «На 6 месяцев»;
- «На год»;
- «До даты».

Для периодов срок отсчитывается от даты создания идентификатора. В варианте «До даты» используется установленная в шаблоне дата окончания.

12.7. Панель «События»

Панель показывает аудит персон, идентификаторов и пропусков вместе с событиями доступа: видно и «кто изменил пропуск», и «как он сработал на точке». Переключатель «Выбранные» сужает ленту до выбранной записи — пропуска, персоны или открытого идентификатора: её аудит и её проходы в одной ленте. Приёмы работы с лентой описаны в главе 8.

12.8. Дополнительные поля персонала

Секция «Дополнительные поля персонала» панели инструментов настраивает состав карточки персоны:

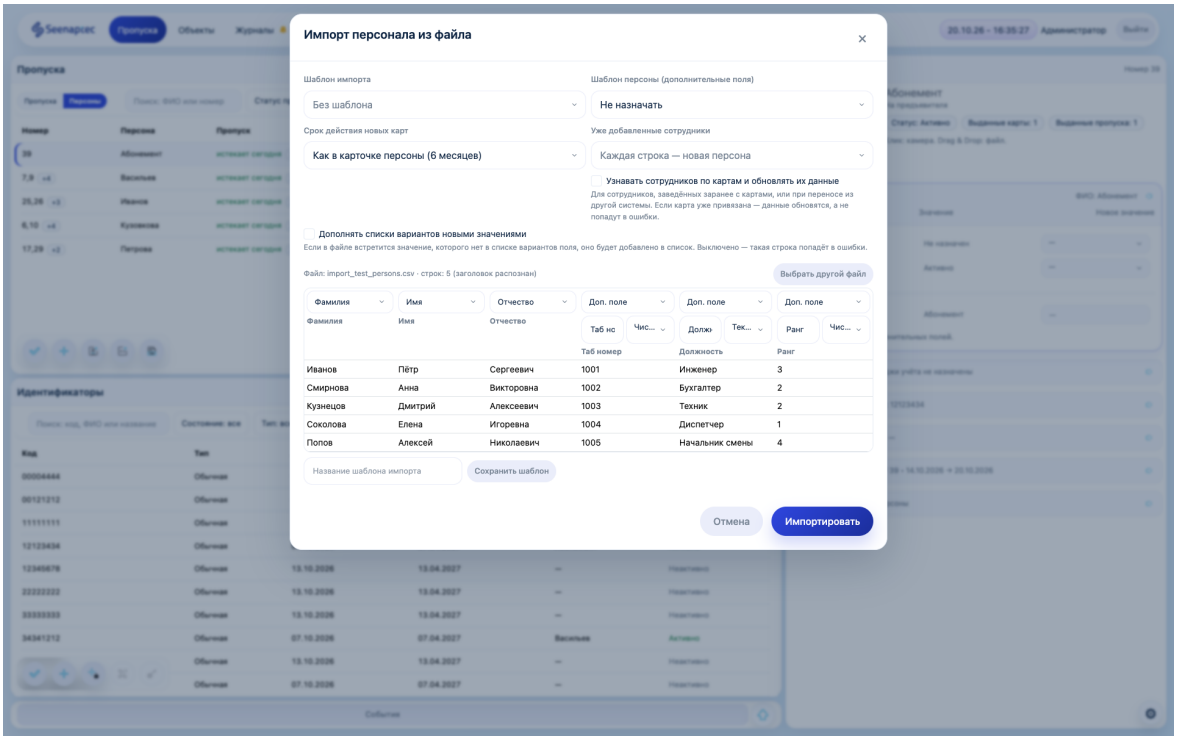
- **«Типы дополнительных полей»** — определения полей: название, категория («Персональные данные», «Организационные данные», «Контакты», «Служебные данные», «Статус», «Прочее»), тип значения («Строка», «Целое», «Логическое», «Перечисление»), признаки «обязательное» и «уникальное»;
- **«Шаблоны полей персонала»** — упорядоченные наборы полей; шаблон назначается персоне в карточке. Поля, заполненные вне текущего шаблона, сохраняются и показываются отдельным блоком.

По дополнительным полям работает поиск «По полям» в списке персон (раздел 12.2).

> **Для знакомых с классическими СКУД.** Дополнительные поля — это не «свободные графы примечаний», а типизированный справочник уровня системы: поле «Отдел» одно на всю систему, а не своя строка в каждой карточке. Тип «Перечисление» со списком вариантов защищает данные от разнобоя («ИТ», «IT», «ит.») и делает поля пригодными для точного поиска «По полям» и для опознания персон при импорте (раздел 12.9). Признак «уникальное» превращает поле в ключ — например, табельный номер, по которому персонал синхронизируется с кадровой системой.

12.9. Импорт персонала из файла

Кнопка «Импорт персонала из файла» в панели «Пропуска» открывает мастер загрузки списка людей из файла CSV — способ завести или обновить персонал массово: при вводе системы в эксплуатацию, при регулярной синхронизации с кадровой выгрузкой, при переносе из другой системы. Импорт создаёт и обновляет персон, их дополнительные поля и карты; пропуска импорт не выдаёт — они оформляются штатной выдачей (в том числе массовой, по шаблону).



Привязка колонок. Мастер показывает файл таблицей предпросмотра; над каждой колонкой выбирается её роль: «Не импортировать», «ФИО целиком», «Фамилия», «Имя», «Отчество», «Карты», «Доп. поле». Для колонки «Доп. поле» указываются название поля и тип значения; для перечислений список вариантов собирается из данных файла. Типовые роли мастер предлагает сам по заголовкам колонок; несколько строк одной персоны (например, по строке на карту) объединяются автоматически.

Настройки. Помимо ролей колонок задаются:

- «Шаблон персоны (дополнительные поля)» — какой шаблон полей назначить создаваемым персонам;

- «Срок действия новых карт» — шаблон идентификатора для карт из файла («Как в карточке персоны (6 месяцев)» по умолчанию);
- «Уже добавленные сотрудники» — ключ дообновления: «Каждая строка — новая персона» либо «Узнавать по полю „…“ и обновлять» — внешний идентификатор (уникальное доп. поле, например табельный номер), по которому найденные персоны обновляются, а не дублируются: у них обновляются ФИО и поля, добавляются недостающие карты;
- «Узнавать сотрудников по картам и обновлять их данные» — дополнительный ключ для людей, заведённых заранее с картами, или при переносе из другой системы: если карта из файла уже привязана к сотруднику, строка обновит его данные;
- «Дополнять списки вариантов новыми значениями» — разрешение расширять перечисления значениями из файла (иначе строка с неизвестным значением попадёт в ошибки).

Результат импорта. Каждая строка файла обрабатывается независимо. Ошибка в одной строке — например, занятый код карты, конфликт уникального поля или недопустимое значение перечисления — не останавливает импорт остальных данных. После завершения мастер отображает сводку с количеством созданных, обновлённых, пропущенных и ошибочных записей, а также пояснение для каждой строки с ошибкой. В журнале импорт регистрируется одним сводным событием с показателями исходного количесва вводимых данных и их финальных значений при импорте.

Шаблоны импорта. Собранную раскладку — роли колонок, режим ФИО, ключ дообновления, шаблоны и флаги — можно сохранить как именованный **шаблон импорта** и при следующей выгрузке применить одним выбором в поле «Шаблон импорта». Шаблоны общие для всех операторов; регулярная ежемесячная синхронизация с кадровой системой сводится к «выбрать файл → выбрать шаблон → применить».

Права: импорт требует права создания персон; колонки «Карты» — права выдачи идентификаторов; режимы дообновления — полного уровня прав на персоны; создание и расширение полей — прав на шаблоны. Недоступные режимы мастер блокирует с пояснением.

12.10. Авто-очистка

Секция «Авто-очистка» панели инструментов — автоматический жизненный цикл данных:

- «Удалять просроченные пропуска» + «Хранить после окончания (дни)» — просроченные пропуска (включая заявки) удаляются после срока хранения;
- «Удалять персон без пропусков» + «Срок неактивности персон (дни)» — персоны, у которых давно нет действующих пропусков, удаляются вместе с идентификаторами.

Персоны в чёрном списке авто-очисткой не удаляются. Каждое автоматическое удаление фиксируется в журнале отдельными событиями; история удалённых записей остаётся читаемой (глава 13).

Глава 13. Журналы

Рабочая область «Журналы» — рабочее место аудитора и оператора безопасности: исторический анализ событий, расследования, тревоги, архивация и контроль целостности журнала. Для живого наблюдения за своей зоной в каждой рабочей области есть панель «События» (глава 8); «Журналы» — рабочая область для работы с полной историей.

13.1. Устройство журнала

Журнал — единая лента событий всей системы, устроенная по принципу «только добавление»: сохранённые записи не изменяются и не удаляются (кроме штатной архивации, раздел 13.6). Каждое событие классифицировано по трём осям:

- **категория** — «Доступ» (решения и эпизоды доступа), «Аудит» (изменения данных и настроек операторами и сервисами), «Техсостояние» (состояние оборудования и сервисов), а также фильтр категории **«ОПС»** (события пожарных панелей, зон, шлейфов и извещателей) и «Тревоги»;
- **домен** — «Персонал и пропуска», «Объекты доступа», «Оборудование», «ОПС», «Безопасность», «Учёт присутствия»;
- **важность** — «Справочно», «Внимание», «Предупреждение», «Критично».

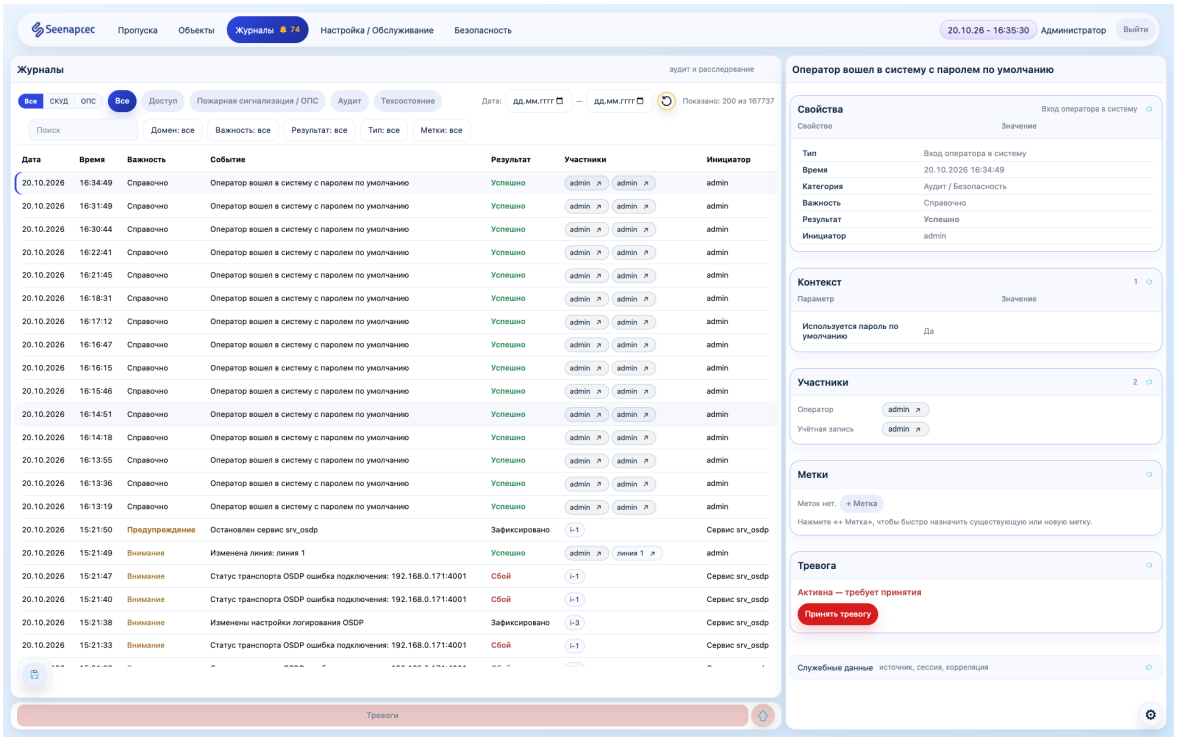
Каждая изменяющая операция в системе обязана оставить событие аудита — это правило продукта. У событий аудита сохраняется перечень изменений «было/стало»; у событий доступа — участники и причина решения.

События, произошедшие на устройстве при потере связи с сервером — например, срабатывания аварийного открывания (раздел 11.3), — не теряются: устройство хранит собственный офлайн-журнал, и после восстановления связи система импортирует эти события в общую ленту с их фактическим временем и с защитой от дублей.

Единственный изменяемый слой поверх записей — операторские **метки** (раздел 13.3); их добавление и снятие само фиксируется в журнале. Метки предназначены для удобного поиска маркированных событий.

Ссылки на удалённые объекты. Именование персон сохраняются на момент события, а числовые идентификаторы (системные ID) сущностей никогда не переиспользуются — поэтому история остаётся достоверной и читаемой после любых удалений в системе. Значок удалённого участника показывается в интерфейсе приглушённым основным цветом, с пометкой «(удалён)» в подсказке; переход к объекту недоступен, но фильтрация истории по нему работает.

13.2. Панель «Журналы»: поиск по истории



Верхняя строка панели — переключатель категорий: «Все» | «Доступ» | «Аудит» | «Техсостояние» (включая фильтр категории **«ОПС»** и «Тревоги»). Кроме того, в верхней шапке приложения при открытых «Журналах» доступна пилюля подсистем **`Все | СКУД | ОПС`**, позволяющая одним нажатием ограничить журнал и панель «Тревоги» событиями только СКУД или только ОПС. Ниже расположены фильтры:

- **период** — поля «Дата: с — по» (включительно); красная кнопка «×» сбрасывает диапазон дат;
- **«Домен»**, **«Важность»**, **«Результат»** («Разрешено», «Запрещено», «Зарегистрировано», «Успешно», «Сбой», «Зафиксировано»), **«Тип»** — множественный выбор; список типов сужается выбранной категорией и доменом;
- **«Поиск»** — подстрока в описании события и подписях участников;
- **«Метка»** — отбор событий с указанной операторской меткой.

Колонки списка: «Дата», «Время», «Важность», «Событие», «Результат», «Участники», «Инициатор». История подгружается по мере прокрутки; счётчик «Показано: N из M» отражает объём выборки.

Объектная история. Щелчок по значку участника добавляет фильтр по объекту — лента сужается до всех событий, где участвовал этот объект (включая удалённые). Активные объектные фильтры показаны строкой «Объектная история:» с кнопкой «Сбросить». Это основной приём расследования: «всё, что происходило с этой дверью / этим пропуском / этим оператором».

Учёт присутствия. События домена «Учёт присутствия» фиксируют закрытие интервала присутствия: персона, зона, длительность, причина закрытия (проход, таймаут, операторский сброс, завершение сессии шкафа). Для выборки задайте домен «Учёт присутствия» и при необходимости тип «Интервал присутствия закрыт».

Переход к участнику и возврат. Помимо фильтра, значок участника — и в списке, и в секции «Участники» карточки события — снабжён стрелкой перехода «Открыть объект»: она открывает саму сущность в её рабочей области — персону, пропуск и идентификатор в «Пропусках», объект доступа или пожарную зону (`D`, `A`, `P`) в «Объектах доступа», устройство, линию, сервер или панель/шлейф/извещатель ОПС в «Настройке / Обслуживании». Щелчок по остальной части значка по-прежнему добавляет фильтр. После перехода в заголовке основной панели открывшейся рабочей области появляется кнопка возврата — она возвращает в «Журналы» к тому же выбранному событию (раздел 8.10). У удалённых участников стрелки нет: переход вёл бы в пустую карточку, но фильтр истории по ним работает.

Работа нижней панели «События» с подсистемой ОПС. В рабочих областях «Настройка / Обслуживание» и «Объекты доступа» нижняя панель «События» автоматически следует за положением переключателя **`СКУД | ОПС`**: в режиме `ОПС` лента показывает события пожарной сигнализации и автоматики, а переключатель **«Выбранные»** отбирает историю конкретной выбранной пожарной зоны (`D`, `A`, `P`), панели UniPOS, шлейфа или адресного устройства ОПС.

Экспорт выборки в CSV

Кнопка «Экспорт» слева внизу панели выгружает в CSV-файл текущую выборку — все события, отобранные фильтрами панели, а не только подгруженные на экране. В режиме просмотра архива (раздел 13.7) кнопка недоступна: выгружается только живая база.

Диалог «Экспорт журнала в CSV» показывает объём выборки и действующий фильтр. Настраиваются колонки и формат:

- **базовые колонки** включаются всегда: «Дата/время», «Тип», «Категория», «Важность», «Результат», «Актор», «Сводка»;
- **участники** — по колонке на тип участника (персона, пропуск, объект доступа, устройство и т. д.); предлагаются только типы, ожидаемые под текущий фильтр, по умолчанию включены все — кнопки «Все» и «Снять» управляют всем списком;
- **контекстные поля** — по колонке на поле, сгруппированы по темам («Доступ», «Аутентификация» и др.); по умолчанию выключены, у события без этого поля ячейка пуста;
- **разделитель** — «Точка с запятой (;)» или «Запятая (,)»;
- **значения** — «Как в журнале» (русские подписи, как в ленте) или «Сырые значения» (коды, как хранятся в базе, — для машинной обработки).

Кнопка «Скачать CSV» выгружает файл `journal-export-ГГГГММДД-ЧЧММСС.csv` в кодировке UTF-8 — кириллица корректно открывается в табличных редакторах. Два ограничения показываются предупреждениями прямо в диалоге:

- фильтр по меткам в выгрузку не попадает — файл содержит события без учёта меток;
- выгружаются не более 50 000 событий; при усечении последняя строка файла — маркер с полным числом событий по фильтру и советом сузить фильтр для полной выгрузки.

Каждая выгрузка фиксируется в журнале событием аудита «Выполнен экспорт событий журнала» со сводкой фильтра и числом выгруженных строк — видно, кто и что выгружал.

13.3. Карточка события

Чтобы открыть карточку события, выберите его строку в журнале. Секции карточки можно сворачивать и разворачивать нажатием на заголовок. Система запоминает набор открытых секций на текущем рабочем месте и применяет его при просмотре других событий.

В зависимости от типа события карточка содержит следующие секции:

- **«Свойства»** — тип события, дата и время, категория, важность, результат и инициатор. В заголовке секции отображается название типа события.
- **«Участники»** — роли и связанные сущности: объект доступа, персона, пропуск, идентификатор, устройство, линия, сервер или оператор. Нажмите значок участника, чтобы отфильтровать журнал по этой сущности, либо стрелку на значке, чтобы открыть её карточку.
- **«Изменения»** — таблица **«Поле / Было / Стало»** с изменёнными значениями. Отображается для событий аудита.
- **«Связи»** — добавленные и удалённые связи между сущностями, например изменения состава объектов доступа в пропуске.

- **«Контекст»** — дополнительные параметры события: режим идентификации, направление прохода, причина принятого решения и другие сведения. Компоненты объекта доступа отображаются по назначенным именам, например «Считыватель вход» или «Кнопка выхода».
- **«Метки»** — метки оператора системы, используемые для группировки событий при расследовании. Чтобы добавить метку, введите её в поле **«Новая метка»**. Чтобы удалить метку, нажмите кнопку удаления на её значке. Метки доступны всем операторам, а их добавление и удаление регистрируются в журнале.
- **«Тревога»** — состояние тревожного события. Для активной тревоги отображаются статус **«Активна — требует принятия»** и кнопка **«Принять тревогу»**. После принятия отображаются оператор, дата, время и комментарий.
- **«Служебные данные»** — идентификатор события, сервер, сервис-источник и корреляционные идентификаторы. По умолчанию секция свёрнута.

При просмотре события в другой рабочей области нажмите кнопку **«Открыть в Журналах»**, чтобы открыть это же событие в рабочей области «Журналы» и продолжить расследование.

13.4. Тревоги

Тревога — событие, требующее реакции оператора. К тревогам относятся, например, нарушение доступа, срабатывание датчика вскрытия устройства, нарушение целостности журнала, ошибка получения секрета и доступ под принуждением. Полный перечень определяется реестром событий системы.

Индикатор тревог

Если в системе есть активные непринятые тревоги, на кнопке рабочей области «Журналы» отображается значок колокольчика со счётчиком количества текущих тревог. Появление новой тревоги сопровождается звуковым сигналом.

Нажмите значок колокольчика, чтобы открыть панель «Тревоги» из любой рабочей области.

Панель «Тревоги»

В панели отображаются только активные непринятые тревоги. В заголовке указывается их общее количество, а в списке доступны колонки:

- **«Дата»**;
- **«Время»**;
- **«Важность»**;
- **«Событие»**;
- **«Участники»**.

Выберите строку, чтобы открыть карточку принятия тревоги. Стрелка на значке участника открывает связанную сущность в соответствующей рабочей области.

13.5. Контроль целостности журнала системы

Записи журнала системы объединены в хеш-цепочку. Каждая запись содержит криптографическую свёртку собственных данных и свёртку предыдущей записи. Это позволяет гарантированно обнаружить изменение содержимого, вставку или удаление записей.

Журнал периодически разделяется на “запечатанные” сегменты. Контрольные значения сегментов дополнительно сохраняются в базе конфигурации системы, благодаря чему изменение, вставка, удаление записи и даже перезапись конечной части журнала целиком обнаруживаются проверкой.

Способы проверки

Целостность журнала проверяется:

- автоматически — при запуске сервера системы и во время его работы;
- вручную — в секции **«Целостность журнала»** панели инструментов;
- при открытии файлов архива (раздел 13.6).

В секции **«Целостность журнала»** отображается сводная информация:

- количество событий в журнале;
- количество “запечатанных” сегментов.

Чтобы запустить ручную проверку, нажмите **«Проверить»**. Система проверит “незапечатанную” часть журнала — от последнего “запечатанного” сегмента до последнего зарегистрированного события.

При успешной проверке отображается сообщение:

«Целостность подтверждена: события №A–№B (N шт.)».

При обнаружении нарушения система указывает его тип и первую повреждённую запись.

Возможные нарушения:

- изменение содержимого события;
- разрыв хеш-цепочки вследствие вставки или удаления записи;
- повреждение “запечатанного” сегмента;
- несоответствие контрольных значений сегмента данным, сохранённым в базе конфигурации.

При обнаружении нарушения система:

- создаёт тревогу **«Нарушение целостности журнала»**;
- регистрирует событие о результате проверки;
- продолжает сохранять новые события в журнале.

13.6. Архивация

Архивация переносит старые сегменты журнала в файлы и освобождает живую базу, не разрывая хеш-цепочку. Настраивается в секции **«Архивация»** панели инструментов:

- «Автоархивация» — включение регулярного запуска; «Частота» (дни или месяцы) и «Время старта»;
- «Папка архива» — каталог файлов на сервере;
- «Пароль» — при выборе пароля (секрет из хранилища «Безопасности») файлы шифруются; без пароля («Без шифрования») выгружаются открытыми. Пароль архива можно использовать и для резервной копии — один секрет для обоих механизмов (раздел 10.8).

Кнопка «Архивировать сейчас» запускает выгрузку вручную. Архивируются только запечатанные сегменты; после успешной выгрузки их записи удаляются из живой базы строго по порядку. Сегмент с непринятой тревогой выгружается, но не удаляется, пока тревога не принята. Итог показывается сообщением («экспортировано сегментов X, удалено из базы Y») и фиксируется событиями журнала.

Каждый файл архива содержит открытое оглавление (диапазон событий и контрольные корни) и полные записи сегмента; шифрование не скрывает оглавление, поэтому инвентаризация папки архива возможна без пароля.

13.7. Просмотр архивов

Секция **«Архив»** панели инструментов открывает архивные файлы на чтение:

1. В списке файлов (диапазон дат, число событий, размер, признак шифрования) отметьте один или несколько **смежных** сегментов. Для зашифрованных файлов система подставит пароль из настроек архива, если он задан; иначе появится блок «Пароль архива» — тот же интерфейс, что при восстановлении резервной копии (раздел 10.8). Файл, полученный извне, можно открыть кнопкой «Загрузить файл…».
2. Нажмите «Открыть архив». Система проверит целостность файлов и стыков серии и развернёт временную базу для чтения.

Инструмент переключается в архивный режим: та же лента, фильтры и карточки, сверху — индикатор «АРХИВ» с диапазоном и результатом проверки целостности: целостность подтверждена либо нарушена, с числом нарушений (нарушения не блокируют просмотр). В архивном режиме недоступны тревоги и изменение меток — метки из архива показываются как исторические. Кнопка «Вернуться к живому журналу» закрывает сессию просмотра.

13.8. Отчёты

Секция «Построение отчетов» панели инструментов строит отчёты по данным журнала. В текущей версии поддерживается один вид отчёта — **отчёт по учёту присутствия**: время пребывания персон в зоне выбранного бейджа учёта (раздел 11.11) за период. Источник данных — события «Интервал присутствия закрыт» домена «Учёт присутствия» (раздел 13.2); открытые интервалы в отчёт не попадают.

Определения отчётов

Отчёты хранятся в секции списком именованных определений. Определение задаёт:

- название отчёта;
- бейдж учёта присутствия;
- период: «Сегодня», «Вчера», «Эта неделя», «Прошлая неделя», «Этот месяц», «Прошлый месяц» или произвольный диапазон дат;
- выбранных персон (по умолчанию — все) и фильтр по дополнительным полям персон;
- дополнительные поля персон, включаемые в отчёт отдельными колонками;
- разделитель CSV: «;» или «,».

Определение сохраняется кнопкой «Сохранить»; кнопка «Сохранить и построить» сохраняет определение и сразу строит отчёт.

Построение отчёта

При запуске построения бейдж, период и персону можно переопределить в блоке «Параметры запуска» — сохранённое определение при этом не меняется. Так один и тот же отчёт строится «за прошлый месяц» или «по одной персоне» без правки определения. Периоды рассчитываются по времени сервера в момент построения; неделя начинается с понедельника.

Строка отчёта — итог по паре «дата + персона»:

- «Первый вход» — время первого входа в зону за день;
- «Последний выход» — время последнего выхода по достоверным интервалам;
- «Время в зоне» — сумма длительностей достоверных интервалов за день, а не разница между первым входом и последним выходом: перерывы вне зоны в сумму не входят;
- «Недостоверно» — число интервалов, закрытых по таймауту (раздел 11.11); такие интервалы в сумму времени не входят, колонка пуста, если их нет.

Интервал относится к дате входа и по полуночи не разрезается: ночная смена целиком попадает в день начала.

Файл отчёта

Результат построения — файл CSV в кодировке UTF-8 с BOM (кириллица корректно открывается в табличных редакторах), с разделителем из определения. Хранится только последний построенный файл каждого отчёта: новое построение заменяет предыдущий файл. Если за выбранный период данных нет, предыдущий файл сохраняется. Кнопка «Скачать» выгружает файл; кнопка «Удалить файл» удаляет файл, не удаляя определение.

Создание, изменение и удаление определений, а также каждое построение фиксируются событиями аудита: факт выпуска файла со сведениями о рабочем времени персон виден в журнале независимо от того, кто скачал файл.

Глава 14. Безопасность

Рабочая область «Безопасность» — управление доступом к самой системе: учётные записи операторов, роли и полномочия, активные сессии, хранилище секретов, настройки безопасности и аудит платформы. Здесь же настраивается контур работы с картами: настольные считыватели (АРМ) и библиотека профилей карт. Левые панели области — «Операторы» (с переключателем «Операторы / АРМ»), «События», «Сессии»; на панели инструментов — секции «Роли», «Секреты», «Настройки безопасности», «Профили карт».

14.1. Модель полномочий

Полномочия оператора определяются его ролью (и индивидуальными правами поверх роли, если они заданы). Право — это уровень доступа к области одного из пяти доменов системы:

Домен	Что охватывает
«Оборудование»	Линии, устройства, системные операции обслуживания
«Объекты доступа»	Объекты, правила, текущий доступ
«Персоны и пропуска»	Персоны, идентификаторы, пропуска, шаблоны
«Безопасность»	Операторы, роли, секреты, АРМ считывателей, профили карт, аудит платформы
«Журнал»	Журнал событий, тревоги, целостность, архивы

Уровни кумулятивны — каждый следующий включает предыдущие: «Чтение» → «Добавление» → «Полный». В области пропусков есть промежуточный уровень «Выдача по шаблону» — право выдавать пропуска строго по шаблонам, разрешённым для ограниченной выдачи (глава 12).

В матрице прав области внутри каждого домена разделены на **базовые** (верхний уровень домена: например, «Устройства и линии» в «Оборудовании», «Конфигурация объектов» в «Объектах доступа», «Персоны» и «Пропуска» в «Персонах и пропусках», «Операторы» и «АРМ считывателей» в «Безопасности», «События» в «Журнале») и **зависимые** (вложенные строки ниже базовых). При выборе любого уровня на зависимой области в матрице автоматически включается «Чтение» на базовой области этого домена; снятие всех базовых областей домена («—») автоматически сбрасывает и зависимые области.

Доступ к подсистемам (потолки прав `СКУД` и `ОПС`). Над матрицей доменов в профиле роли и в индивидуальных правах оператора расположен блок **«Доступ к подсистемам»** с двумя областями верхнего уровня:

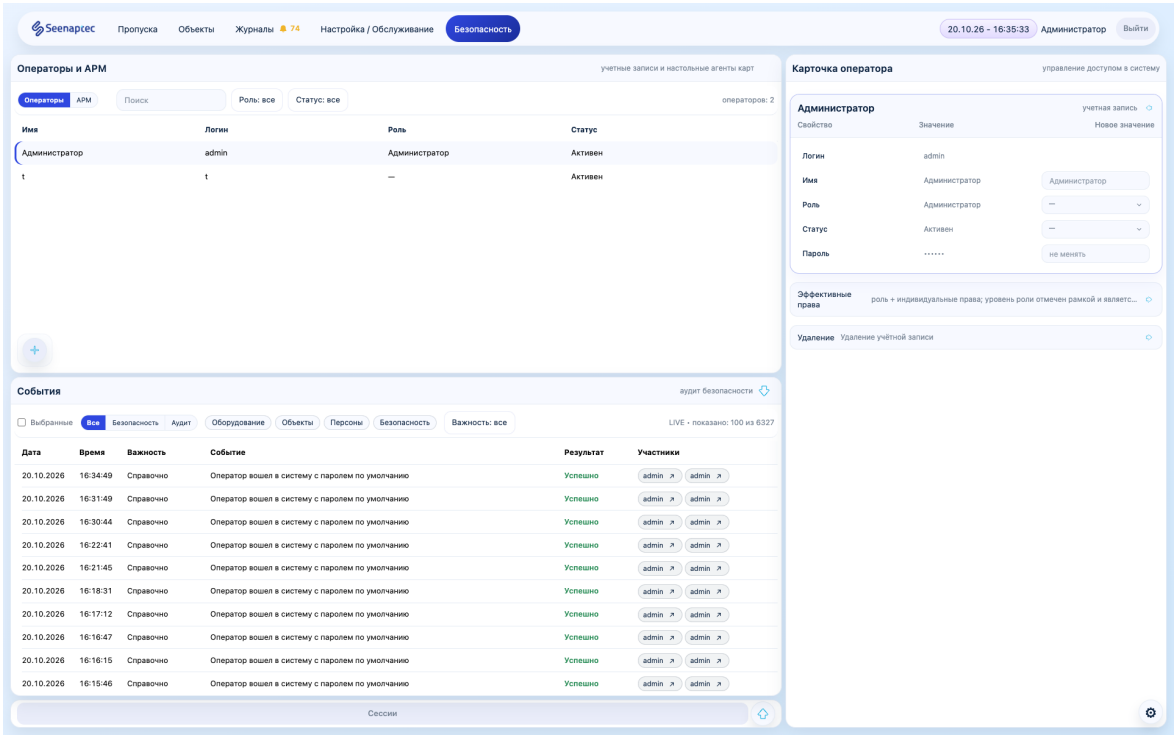
- **«Контроль и управление доступом (СКУД)»** (`domain.skud`);
- **«Охранно-пожарная сигнализация (ОПС)»** (`domain.ops`).

Для каждой подсистемы задаётся потолок полномочий (`Нет` / `Чтение` / `Добавление` / `Полный`), который ограничивает сверху максимальный эффективный уровень прав роли в соответствующей подсистеме (например, если в `domain.ops` выбран уровень «Чтение», оператор сможет просматривать панели и пожарные зоны ОПС, но не сможет отправлять команды пуска, обхода или менять настройки панелей даже при наличии полных прав в доменах «Оборудование» и «Объекты доступа»). Если для одной из подсистем установлен уровень «Нет» (–), эта подсистема полностью скрывается для оператора, а переключатель **`СКУД | ОПС`** в верхней шапке интерфейса автоматически убирается, оставляя рабочее место строго в рамках доступной подсистемы.

Анти-эскалация. Оператор не может выдать другим больше прав, чем имеет сам: при редактировании ролей уровни выше собственных недоступны (подсказка «Выше вашего уровня прав в этой области»), сервер контролирует то же правило. Роль «Администратор» неизменяема и неудаляема; назначать её и изменять учётные записи администраторов может только администратор.

Интерфейс отражает полномочия автоматически: рабочие области, левые панели и секции панели инструментов без права чтения скрыты, а недоступные кнопки действий блокируются с пояснением «Недостаточно прав».

14.2. Панель «Операторы»



Список учётных записей: колонки «Имя», «Логин», «Роль», «Статус» («Активен» / «Отключен»); сверху — поиск и фильтры по роли и статусу (выпадающие списки с флажками, можно выбрать несколько значений; выбор применяется кнопкой подтверждения, как в фильтрах панели «Доступ»). Внизу панели — единственная кнопка «+»; массовых операций у операторов нет. Переключатель «Операторы / АРМ» в заголовке панели переводит её в режим управления настольными считывателями карт (раздел 14.8).

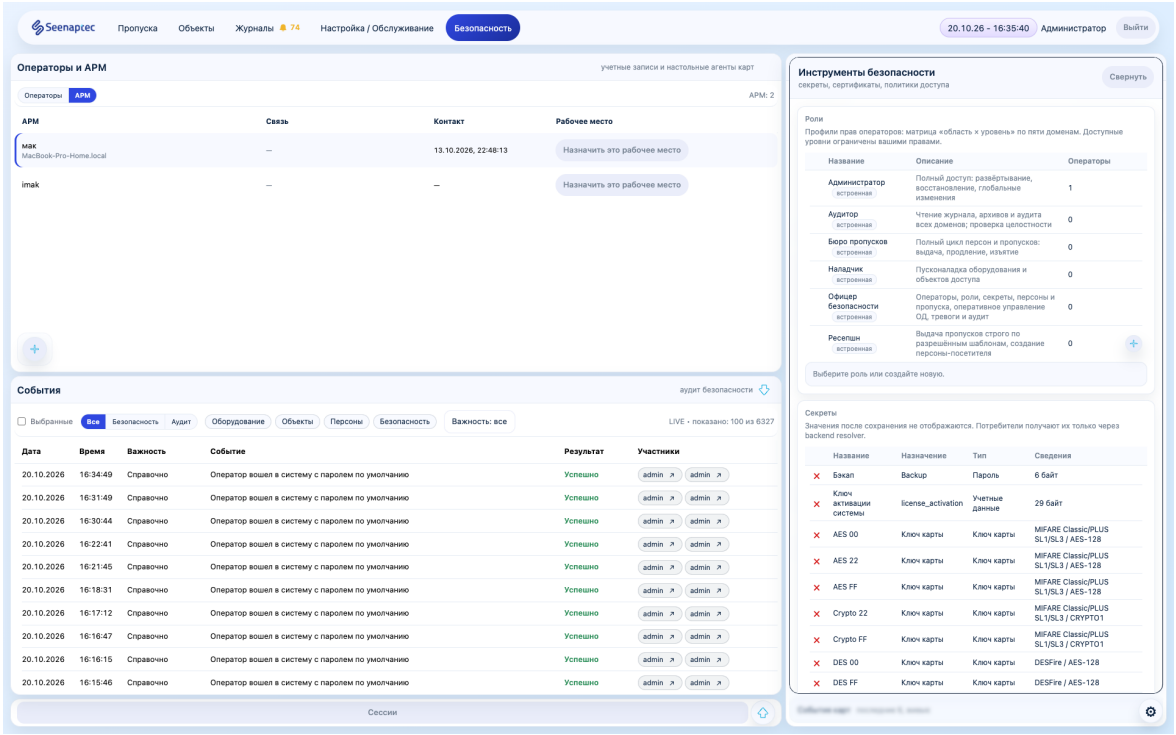
Создание. Кнопка «+» («Добавить оператора») открывает диалог «Новый оператор»: «Логин», «Имя» (по умолчанию совпадает с логином), «Роль» и «Пароль». Требования к паролю определяются настройками безопасности (раздел 14.6).

Карточка оператора. Первая секция — свойства: логин (не изменяется), имя, роль, статус и смена пароля (текущее значение не показывается; пустое поле означает «не менять»). Пароль, установленный оператору другим оператором, считается назначенным: при включённом требовании смены назначенного пароля (раздел 14.6) владелец обязан заменить его при следующем входе. Вторая секция — «Эффективные права»: итоговая матрица полномочий, складывающаяся из роли и индивидуальных прав. Уровень, который даёт роль, отмечен в каждой строке звёздочкой слева от подписи — это унаследованное значение и одновременно минимум: уровни ниже ролевого недоступны для выбора (подсказка «Ниже уровня роли»), индивидуальная настройка может только повышать уровень. Выбор уровня со звёздочкой возвращает область к ролевому значению (снимает индивидуальное повышение); сервер хранит индивидуально только права выше роли, поэтому последующее изменение роли сразу отражается на эффективных правах.

Отключение и удаление. Временное отстранение оператора — статус «Отключен». Удаление выполняется из карточки: свёрнутая секция «Удаление» в её конце поясняет последствия — сессии оператора завершаются, история в журнале сохраняется; кнопка удаления подтверждается в правой зоне. Ограничения: собственную учётную запись удалить нельзя (кнопка заблокирована с пояснением, сервер также отклонит запрос), и нельзя удалить последнего оператора с полными правами на управление операторами — система не позволит остаться без администрирования учётных записей.

Все изменения фиксируются в аудите: создание, изменение, удаление операторов, изменения прав.

14.3. Роли



Секция «Роли» панели инструментов — профили прав: матрица «область × уровень» по пяти доменам.

Предустановленные роли (помечены как «встроенная»):

Роль	Назначение
«Администратор»	Полный доступ: развёртывание, восстановление, глобальные изменения
«Офицер безопасности»	Операторы, роли, секреты, персоны и пропуска, оперативное управление объектами, тревоги и аудит
«Бюро пропусков»	Полный цикл персон и пропусков: выдача, продление, изъятие
«Ресепшн»	Выдача пропусков строго по разрешённым шаблонам, создание персоны-посетителя
«Аудитор»	Чтение журнала, архивов и аудита всех доменов; проверка целостности
«Наладчик»	Пусконаладка оборудования и объектов доступа

Собственные роли создаются кнопкой «Создать роль» (название, описание, потолки «Доступ к подсистемам» для СКУД и ОПС, матрица уровней по пяти доменам) и редактируются по той же схеме; в списке видно число операторов с каждой ролью. Встроенные роли не удаляются; роль, назначенную операторам, удалить нельзя.

14.4. Панель «Сессии»

Живой список активных сессий операторов: «Оператор» (своя сессия помечена «(вы)»), «IP», «Браузер», «Активность»; список обновляется автоматически, счётчик показывает «сессий: N».

Сессия действует по скользящему окну неактивности: каждый запрос оператора продлевает её, при простое дольше установленного времени неактивности (раздел 14.6) сессия истекает, и требуется повторный вход. Администратор может принудительно завершить чужую сессию кнопкой «Завершить сессию» — отзыв фиксируется в аудите событием «Отозвана сессия оператора»; сессии администраторов завершает только администратор.

14.5. Секреты

Секция «Секреты» панели инструментов — защищённое хранилище значений, которые система использует, но никогда не показывает: пароль резервной копии, пароль архива журнала, ключи OSDP Secure Channel, ключи карт, сертификаты HTTPS.

У секрета есть название, назначение (например, «Backup», «OSDP SCBK», «HTTPS/TLS») и тип материала («Пароль», «Симметричный ключ», «Сертификат» и другие). Значение вводится один раз при создании или замене: после сохранения оно шифруется и не отображается ни в одном экране — сменить значение можно, прочитать нельзя. Потребители (резервное копирование, HTTPS, линии OSDP) обращаются к секрету по ссылке.

Создание, изменение и удаление секретов фиксируются в аудите — без значений.

14.6. Настройки безопасности

Секция «Настройки безопасности» панели инструментов — общесистемные параметры входа и сессий:

Параметр	Значение по умолчанию	Описание
«Время неактивности сессии (мин)»	720	Сессия истекает после указанного времени без запросов; активность продлевает её. Допустимо от 1 минуты до 7 суток
«Разрешение пустого пароля»	Нет	Допускает операторов без пароля (для стендов; в эксплуатации не рекомендуется)
«Политика безопасности пароля»	Стандартная	«Нет» — без ограничений.«Стандартная» — от 6 символов.«Строгая» — от 10 символов; нужны буквы и цифры.
«Требовать смену пароля, назначенного администратором»	Нет	Оператор с паролем, который назначил не он сам, обязан задать собственный пароль при следующем входе — до этого работа в системе заблокирована

Политика применяется при создании оператора и смене пароля; на уже установленные пароли изменение политики не влияет. Сохранение настроек фиксируется в аудите событием «Изменены настройки безопасности» со значениями «было/стало».

Требование смены назначенного пароля. Пароль считается «назначенным», если его установил не сам владелец учётной записи: администратор задал или сбросил пароль оператору, либо пароль создан системой (оператор `admin` с паролем по умолчанию `123456` при активации, глава 6). При включённом требовании такой оператор сразу после входа видит экран «Смените пароль» (текущий пароль, новый пароль дважды) и не может работать в системе, пока не задаст собственный пароль; новый пароль проверяется по политике безопасности и **не может совпадать с паролем по умолчанию (**`123456`**)**. Смена пароля отзывает прочие сессии оператора.

Отметка «пароль назначен» ставится всегда, а действует только при включённом требовании — поэтому настройку можно включить и задним числом: все операторы, чьи пароли к этому моменту назначены администратором и ещё не сменены, получат экран смены при ближайшем входе. Включать требование рекомендуется в любой эксплуатации, где пароли выдаются централизованно: оно гарантирует, что рабочие пароли операторов не известны никому, кроме них самих. По умолчанию требование выключено, чтобы не мешать стендам и демонстрациям.

Вход с паролем по умолчанию. Независимо от настроек, каждый вход оператора с паролем `123456` записывается в журнал как **тревожное** событие входа с пометкой об использовании пароля по умолчанию — тревога будет подниматься при каждом таком входе, пока пароль не сменён. Это страховка на случай, когда требование смены выключено, а пароль по умолчанию так и остался в работе.

Смена собственного пароля. Свой пароль оператор меняет на экране «Смените пароль» (при включённом требовании) либо — если есть доступ к рабочей области «Безопасность» — в собственной карточке на панели «Операторы». Пароль, установленный самому себе, «назначенным» не считается и повторной смены не требует.

14.7. Панель «События»: аудит платформы

Панель «События» рабочей области показывает аудит всей системы и технические события платформы. Переключатель категорий — «Все» | «Безопасность» (технические события платформы: запуск и остановка сервисов, проверки целостности) | «Аудит»; в режиме «Аудит» доступны фильтры по доменам — «Оборудование», «ОД» (объекты доступа), «Персоны», «Безопасность».

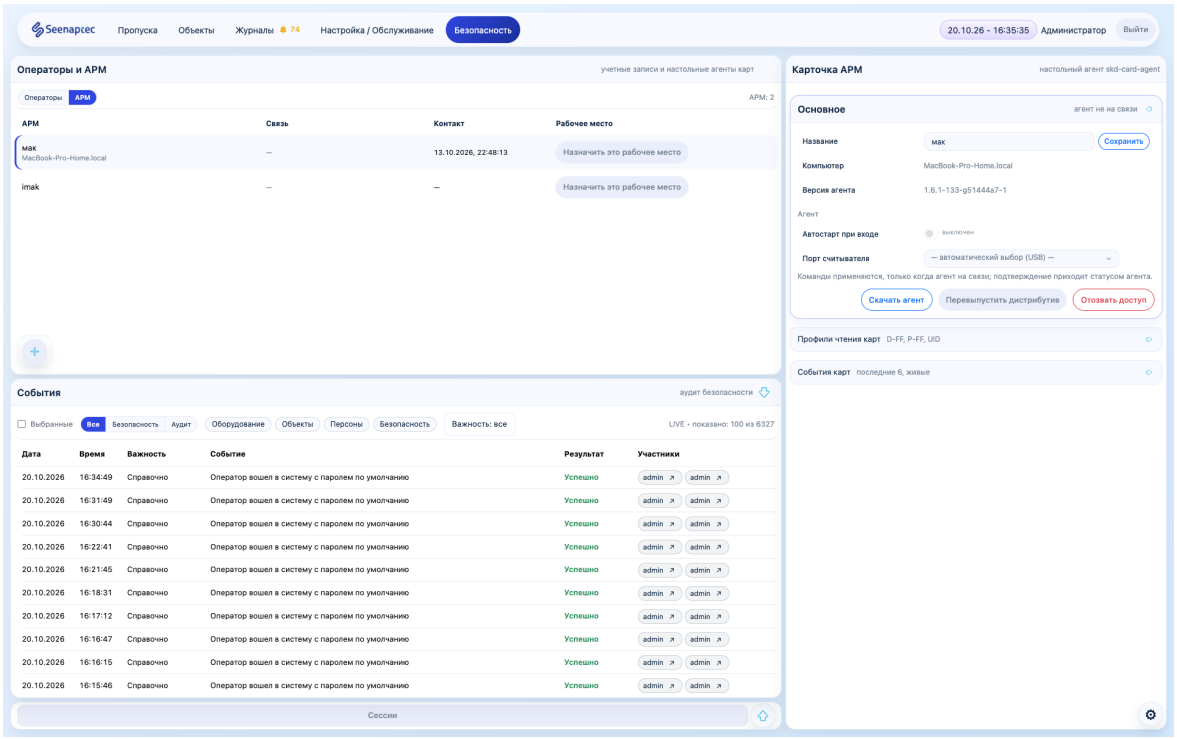
Здесь видны входы операторов, неудачные попытки входа, изменения учётных записей, ролей и прав, отзыв сессий, операции с секретами, изменения настроек безопасности, восстановление из резервных копий, изменения HTTPS.

Вход с паролем по умолчанию помечается как тревога (раздел 14.6). Переключатель «Выбранные» сужает ленту до выбранного оператора — и его действия, и изменения его учётной записи.

История конкретного оператора для расследования доступна и из рабочей области «Журналы» — по значку участника-оператора (глава 13).

14.8. АРМ считывателей

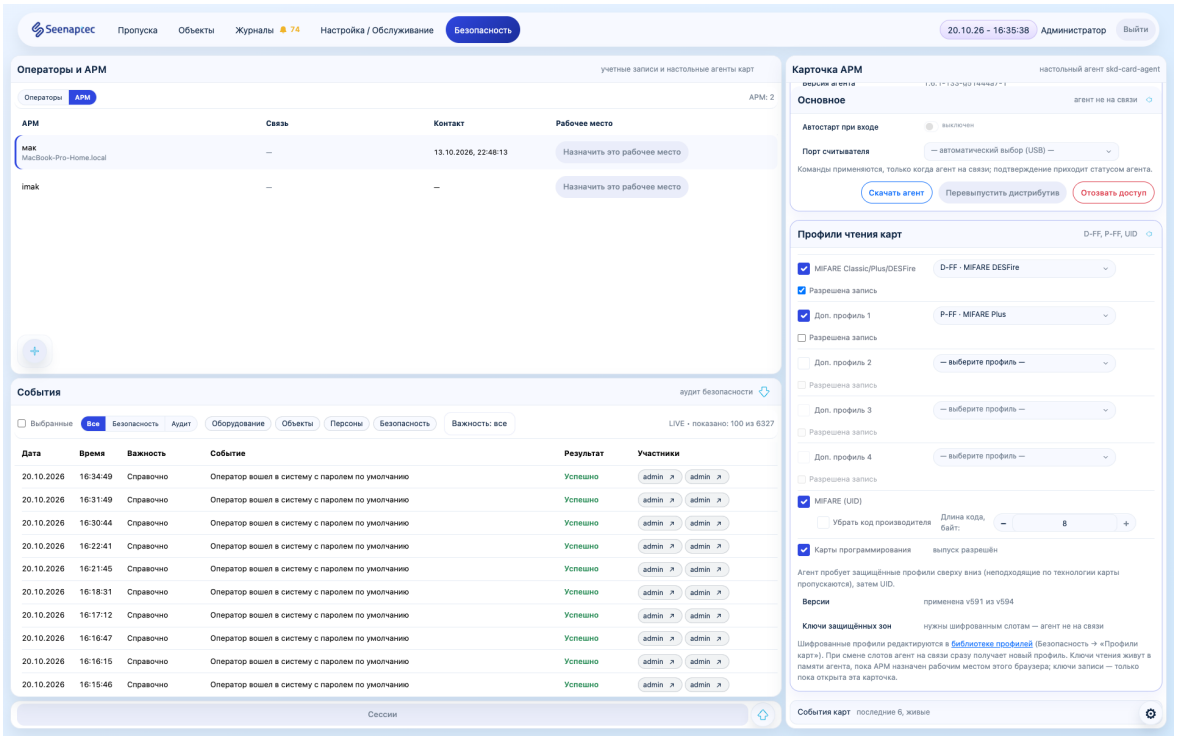
АРМ считывателя — рабочее место с настольным считывателем карт: на компьютере оператора работает программа-агент, которая обслуживает USB-считыватель и выполняет чтение и запись защищённых карт — эмиссию, перевыдачу и инициализацию (раздел 12.6). Управление АРМ ведётся в панели «Операторы», переведённой переключателем в режим «АРМ»; требуется область прав «Безопасность: АРМ считывателей».



Список АРМ: колонки «АРМ» (название и компьютер), «Связь», «Контакт» (время последнего сеанса связи), «Рабочее место». Порядок ввода в эксплуатацию:

1. Создайте АРМ кнопкой **«+»** — задаётся только название.
2. Назначьте АРМ рабочим местом этого браузера — кнопкой «Назначить это рабочее место» в колонке «Рабочее место». Назначение привязывает АРМ к браузеру: занесение карт и диалоги записи в «Пропусках» будут работать с этим считывателем, скачивание дистрибутива разрешено только отсюда. Привязка постоянная: ключ рабочего места хранится в браузере, а запись о привязке — на сервере, поэтому она переживает перезапуск сервера и восстанавливается автоматически, без действий оператора. Привязка относится к браузеру, а не к учётной записи: вход другого оператора на том же рабочем месте перепривязки не требует — оператор с правами на операции с картами работает с тем же считывателем сразу после входа. Назначенный АРМ помечен бейджем «Рабочее место этого браузера»; снять привязку можно кнопкой «Отвязать». Привязка теряется при очистке данных браузера — ключ рабочего места хранится в нём; в этом случае назначьте рабочее место заново. Отметка «Только настольный считыватель» под списком отключает захват карт с настенных считывателей, пока назначено рабочее место, — чужие проходы не попадут в поле ввода.
3. В карточке АРМ нажмите **«Скачать агент»** — система соберёт персональный дистрибутив с кодом доступа. Код ждёт активации один час: установите и запустите агент на компьютере оператора в течение этого срока. Конфигурация дистрибутива несёт отпечаток (пин) TLS-сертификата сервера, поэтому агент доверяет серверу с самоподписанным сертификатом без дополнительной настройки. При перевыпуске или замене сертификата сервера («Доступ по HTTPS», раздел 10.8) скачайте дистрибутив заново и обновите конфигурацию агента: со старым отпечатком агент не подключится и запишет в свой журнал ошибку несовпадения отпечатка сертификата.

Карточка АРМ. Секция «Основное»: название (с кнопкой «Сохранить»), компьютер и версия агента; блок «Агент» — переключатель «Автостарт при входе» (агент прописывает себя в автозагрузку операционной системы) и выбор «Порт считывателя» («— автоматический выбор (USB) —» или конкретный порт из перечисленных агентом; выбранный порт сохраняется в конфигурации агента и переживает перезапуск). Команды применяются, только когда агент на связи; подтверждение приходит статусом агента. Кнопки:



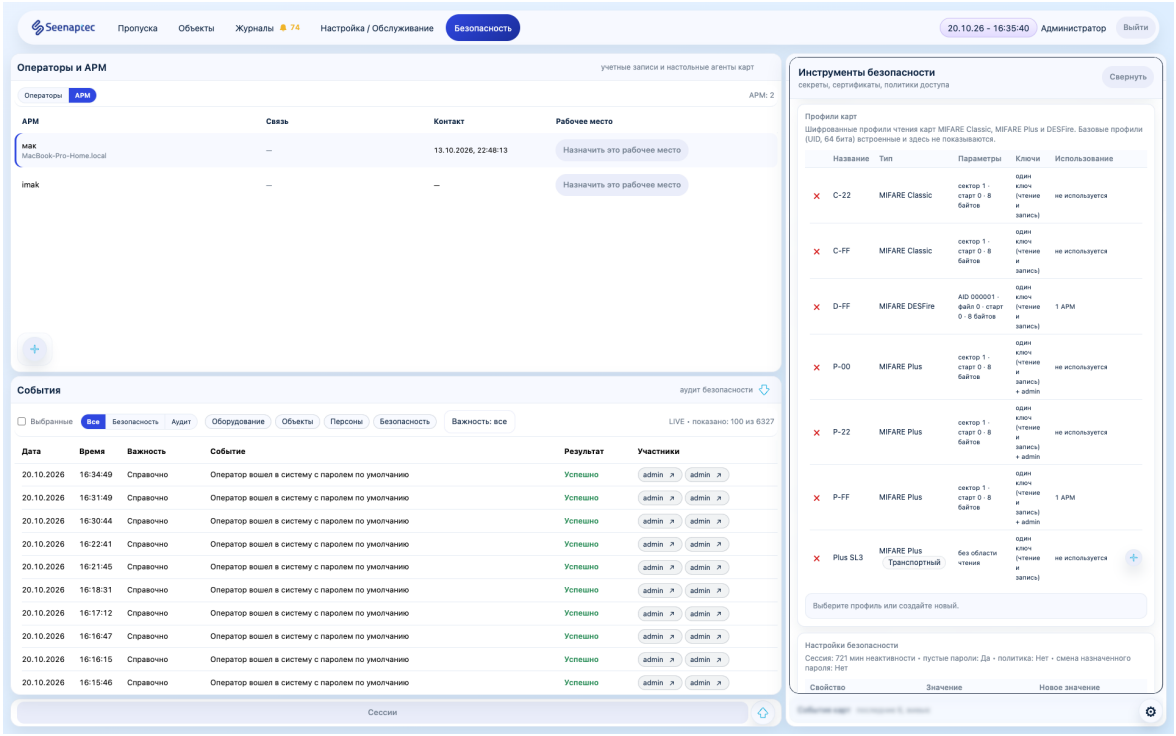
- **«Скачать агент»** — собрать и скачать дистрибутив (создаёт новый код доступа);
- **«Перевыпустить дистрибутив»** — создать новый код доступа: ранее скачанные, но не активированные дистрибутивы перестанут работать, подключённый агент продолжит работу;
- **«Отозвать доступ»** — агент отключится и потеряет доступ к серверу.

Секция «Профили чтения карт» — набор слотов чтения: цепочка защищённых профилей карт из библиотеки (раздел 14.9), которые агент пробует сверху вниз (с флажками «Разрешена запись» для диалогов эмиссии и инициализации), плюс чтение по UID («MIFARE (UID)»). Ниже строки «MIFARE (UID)» расположен переключатель **«Карты программирования»** (`выпуск разрешён` / `выпуск запрещён`) — разрешение выпуска карт программирования и карт входа считывателей на этом АРМ (раздел 10.8); переключение применяется сразу и требует полного уровня прав на АРМ считывателей и на карты программирования, а без разрешения сервер не ставит задания выпуска на этот АРМ. Строка «Версии» показывает применённую агентом версию набора относительно текущей («применена vX из vY»). Ключи защищённых зон передаются агенту из хранилища секретов и живут только в его памяти: ключи чтения — пока АРМ назначен рабочим местом этого браузера, ключи записи — пока открыта карточка АРМ или диалог эмиссии/инициализации.

Секция «События карт» — последние шесть считываний на этом АРМ, обновляются вживую: время, код, привязка к персоне, UID, технология карты.

14.9. Профили карт

Секция «Профили карт» панели инструментов — библиотека шифрованных профилей карт: описаний защищённой зоны карты, по которым считыватели SH-O (раздел 10.4) и АРМ (раздел 14.8) читают и записывают защищённые коды. Базовые профили чтения по UID встроенные и в списке не показываются. Работа с секцией требует области прав «Безопасность: профили карт».



Профиль определяет:

- **название** и **тип карты** — «MIFARE Classic», «MIFARE Plus» или «MIFARE DESFire». Тип задаёт ключевой материал: у Classic оба ключа 6-байтные, у Plus — 16-байтные (AES-128); для карт Plus при инициализации выбирается целевой уровень безопасности (SL1 или SL3);
- **тип профиля** — «Целевой — ключи и область чтения» (полный профиль: чтение и запись карт) или «Транспортный — только ключи» (без области чтения). Транспортный профиль — роль исходного профиля в перевыпуске и инициализации для карт на заводских (транспортных) ключах (раздел 12.6); в селекторах целевого профиля и в слотах чтения он не показывается, в селекторах исходного идёт первым с пометкой «Транспортный». Транспортных профилей DESFire нет: заводская карта DESFire инициализируется без профиля;
- **область чтения** (только у целевого профиля): для MIFARE — номер блока (0–1024); для DESFire — идентификатор приложения «AID» (шесть шестнадцатеричных символов) и «File ID» (0–31);
- **окно кода** (только у целевого профиля): «Стартовый байт» и «Длина кода, байт» (1–8) — где в блоке лежит код карты. Окно обязано умещаться в 16-байтный блок MIFARE; для DESFire — в первые 8 байт файла (ограничение чтения SH-O);
- **ключи**: «Ключ чтения» и «Ключ записи (для эмиссии)» — ссылки на секреты хранилища с назначением «ключ карты» (раздел 14.5); для MIFARE указывается слот («Key A» / «Key B»), для DESFire — номер ключа (0–13). Материал ключей здесь не показывается: секрет выбирается из хранилища или создаётся кнопкой добавления рядом с полем — в том числе генерацией случайного ключа на сервере («Сгенерировать»), при которой материал не проходит через браузер вообще;
- **проверку близости карты** (proximity check) — защиту от ретрансляции для карт, которые её поддерживают; этап проверки — до или после аутентификации.

Для профиля «MIFARE Plus» доступен блок **«Admin-ключи Plus (уровень карты)»** — ключи CardMasterKey, CardConfigurationKey и L3SwitchKey. Они нужны для персонализации карты (перевода с заводского уровня SL0 в SL1 или SL3), перехода SL1→SL3 и смены ключей в SL3 при инициализации карт (раздел 12.6). Ключи задаются все три сразу, материал — 16 байт (AES-128). Без admin-ключей профиль Plus читает и записывает карты, уже находящиеся в SL3, но персонализация и переходы уровней ему недоступны. Переходы уровней Plus необратимы: в SL3 карта навсегда теряет совместимость с Classic.

Создание и правка профиля выполняются кнопкой «+» («Создать профиль карт») в конце списка и кнопкой «Редактировать» в карточке выбранного профиля; черновик сохраняется кнопкой «Сохранить». Изменение профиля не переписывает уже выпущенные карты: карты, записанные по старой редакции профиля, переводятся на новые ключи инициализацией (раздел 12.6).

Удаление выполняется кнопкой «×» в строке профиля. Свободный профиль удаляется сразу. Если профиль используется — в цепочках чтения устройств SH-O и АРМ, в шаблонах настроек оборудования или в наборе карт программирования считывателей, — будет показано предупреждение со списком использований; кнопка **«Снять привязки и удалить»** снимает все перечисленные привязки и удаляет профиль одной операцией. Устройства и АРМ вне связи получают обновлённый набор при следующей записи настроек или подключении; набор карт программирования, лишившийся профиля, потребует перенастройки (раздел 10.8). Уже выпущенные карты удаление профиля не затрагивает.

Глава 15. Типовые сценарии

Пошаговые процедуры повседневных задач. Каждый сценарий завершается проверкой результата; подробности экранов — в главах 10–14. Указана типовая роль исполнителя (глава 14); достаточно любой роли с нужными правами.

15.1. Выдать пропуск посетителю по шаблону

Роль: «Ресепшн» (или выше).

1. Рабочая область «Пропуска» → кнопка «Новая персона»: ФИО посетителя, если нужно — фото → «Создать».
2. Выберите персону в списке → «Выдать пропуск выделенной персоне (по шаблону)».
3. В диалоге выберите «Шаблон доступа» из разрешённых (например, «Гостевой на сегодня») — период, время и объекты заполнятся из шаблона и не редактируются.
4. Добавьте карту посетителя (приложите к настольному считывателю или введите код существующей карты).
5. Нажмите «Выдать по шаблону».

Проверка: в списке — пропуск со статусом «Активно» и сегодняшним сроком; в панели «События» — запись о создании пропуска.

Если нужных шаблонов нет («Нет шаблонов, разрешённых для ограниченной выдачи»), обратитесь к офицеру безопасности: флаг «Ограниченная выдача» на шаблоне (глава 12) устанавливает оператор с полными правами на шаблоны.

15.2. Заявка на пропуск и её выпуск

Роли: заявку создаёт любой оператор с правом выдачи; выпускает «Бюро пропусков».

1. «Пропуска» → «Новый пропуск» → переключатель типа документа: «Заявка».
2. Укажите персону, период и обязательный комментарий (кому и зачем) → «Создать заявку».
3. Позже, при оформлении: найдите заявку (фильтр «Пропуск: Заявка»), откройте её карточку.
4. В секции «Пропуск» нажмите «Выпустить пропуск»; в диалоге «Выпуск пропуска по заявке № N» назначьте объекты, теги и время доступа, добавьте карту → «Выпустить пропуск».

Проверка: статус изменился с «Заявка» на «Активно»; в журнале — события «Создана заявка на пропуск» и «Пропуск выпущен по заявке».

Ненужная заявка отклоняется кнопкой «Отклонить» в карточке — она удаляется с записью в журнале.

15.3. Изъять пропуск, заблокировать персону

Роль: «Бюро пропусков».

Временная приостановка: в карточке пропуска, в нижнем ряду действий секции «Пропуск», нажмите «Приостановить» — операция применяется сразу, сохранять карточку не нужно (требуется полный уровень прав по пропускам). Возврат — той же кнопкой, теперь «Возобновить».

Изъятие пропуска: выберите пропуск в списке → в карточке, внизу секции «Пропуск», нажмите красную кнопку «Удалить пропуск» → подтвердите («Пропуск № N будет удалён (изъят)»). Требуется полный уровень прав по пропускам. Номер пропуска не переиспользуется; история остаётся в журнале.

Блокировка персоны целиком: в карточке персоны (секция «Информация») установите состояние «В черном списке» → «Сохранить». Персоне нельзя выдавать пропуска, действующие пропуска перестают давать доступ.

Проверка: попытка прохода по изъятому или приостановленному пропуску даёт «Доступ запрещён»; в панели «События» — записи об изменениях с перечнем изменений «было/стало».

15.4. Посмотреть, кто открыл дверь

Роль: «Аудитор» или «Офицер безопасности».

1. Рабочая область «Журналы»; категория «Доступ».
2. Задайте период в полях «Дата: с — по».
3. Найдите объект: введите его название в «Поиск» либо откройте любое его событие и щёлкните значок объекта — включится объектная история.
4. В ленте — все решения по объекту; откройте запись: в карточке события видны персона, пропуск, идентификатор и причина решения.

Проверка: строка «Объектная история» со значком объекта активна; в записях есть участники и результат «Разрешено».

Тот же вопрос «на месте» решается быстрее: «Объекты доступа» → выбрать объект → панель «События» → переключатель «Выбранные».

15.5. Принять тревогу

Роль: «Офицер безопасности».

1. Щёлкните по символу колокольчик на кнопке рабочей области «Журналы» в верхней строке (он виден при активных тревогах).
2. В панели «Тревоги» выберите тревогу — справа откроется карточка принятия; изучите событие и участников.
3. Введите комментарий (обязателен) — что установлено и что предпринято.
4. Нажмите «Подтвердить». Для серии однотипных тревог одного участника используйте «Подтвердить для всех (N)».

Проверка: тревога исчезла из панели, счётчик колокольчика уменьшился; в журнале — событие «Тревога принята оператором» с комментарием.

15.6. Подключение пожарной панели UniPOS и импорт конфигурации

Роль: «Наладчик» или «Администратор».

1. Убедитесь, что подсистема ОПС включена («Обзор системы» → панель инструментов → «Подсистемы» → «Охранно-пожарная сигнализация (ОПС)»).
2. Перейдите в «Настройка / Обслуживание» и переключите пилюлю **`СКУД | ОПС`** в верхней строке в положение **`ОПС`**.
3. В нижней части левой панели «Оборудование» нажмите **«+»** («Добавить панель ОПС»), введите название прибора, IPv4-адрес, TCP-порт (по умолчанию `502`), `Modbus Unit ID` (по умолчанию `255`) и номер панели в кластере (`1`–`8`), затем сохраните карточку (раздел 10.9).
4. Дождитесь перехода панели в состояние **«В сети»**: в секции «Канал связи» отобразятся считанные по Modbus `0x2B / 0x0E` модель прибора (`IFS7000`), серийный номер и версия прошивки.
5. В секции «Сервисные операции» карточки панели нажмите **«Опросить состав»** — система автоматически создаст в дереве системные блоки (`БП`, `БИО`, `БРВ`), кольцевые шлейфы, адресные устройства и пожарные зоны (`D`, `A`, `P`).
6. В той же секции нажмите **«Загрузить XML-конфигурацию»** и выберите проектный файл `.xml`, выгруженный из ПО UniPOS, — система перенесёт пользовательские названия зон, шлейфов и датчиков и привяжет извещатели и модули к своим зонам.

Проверка: в дереве панели «Оборудование» (`ОПС`) отображаются блоки, шлейфы и датчики с пользовательскими именами в состоянии «Норма»; в рабочей области «Объекты» (`ОПС`) заполнены зоны обнаружения (`D`), оповещения (`A`) и автоматики (`P`) с таблицами привязанных устройств (раздел 11.12).

15.7. Сбросить присутствие АПБ или сессию шкафа

Роль: «Офицер безопасности».

1. «Объекты доступа» → панель «Текущий доступ».
2. Вкладка «Присутствие»: найдите персону в периметре → «Сбросить присутствие» (или «Сбросить все» для периметра — например, после эвакуации).
3. Вкладка «Активные сессии»: найдите незавершённую сессию (шкаф, который не закрыли штатно) → «Сбросить сессию».

Проверка: запись исчезла из вкладки; в журнале — событие сброса с оператором-инициатором. Персона снова может войти в периметр.

15.8. Заменить неисправное устройство

Роль: «Наладчик».

Привязки к объектам доступа связаны с записью устройства в конфигурации, поэтому удалять запись неисправного устройства не нужно (раздел 10.4).

1. Смонтируйте новое устройство на ту же линию с тем же OSDP-адресом. Если новое устройство отвечает по другому адресу — измените адрес в записи старого устройства: карточка → секция «Подключение» → новый адрес → «Сохранить».
2. Дождитесь, пока сервер зафиксирует ревизию: устройство перейдёт в состояние «Изменено», секция «Модель» покажет поступившие изменения.
3. Примите ревизию («Принять изменения»). Если новое устройство той же модели — привязки к объектам доступа сохраняются, замена завершена. Если модель другая и изменения разрывают привязки — подтвердите кнопкой «Принять и разорвать связи», затем восстановите привязку в карточке объекта доступа (по шаблону привязки или вручную).
4. Если нужно, примените шаблон настроек оборудования и проверьте защищённый канал (новому устройству может потребоваться установка ключа).

Проверка: устройство в состоянии «Настроено», связь «Активно», объект доступа в состоянии «Настроено»; тестовый проход даёт «Доступ разрешён». В режиме «Пусконаладка (LIVE)» видны сигналы нового считывателя.

15.9. Обновить микропрограмму устройства

Роль: «Наладчик».

1. «Настройка / Обслуживание» → панель инструментов → «Микропрограммы устройств»: загрузите файл микропрограммы в каталог («Загрузить новую» или перетаскиванием).
2. Откройте карточку устройства → секция «Обновление микропрограммы»: сравните текущую версию с доступной.
3. Нажмите «Записать в устройство». Следите за этапами: «Подготовка» → «Загрузка образа» → «Проверка контрольной суммы» → «Передача в устройство» → «Активация» → «Проверка версии после записи» → «Завершено».
4. Для парка однотипных устройств используйте массовую операцию «Микропрограмма» (режим выбора устройств).

Проверка: в паспорте устройства («Модель» → «Подробно») — новая версия микропрограммы; в журнале — событие «Результат записи микропрограммы» с успехом.

15.10. Сделать резервную копию и восстановиться

Роль: «Администратор».

Резервная копия:

1. «Настройка / Обслуживание» → панель инструментов → «Бэкап / восстановление».
2. Задайте пароль копии (секрет из хранилища) или включите «Без шифрования», если копия нужна открытой; проверьте папку.
3. Нажмите «Сделать backup сейчас».

Проверка: в журнале — события «Запрошено создание резервной копии» и «Создана резервная копия»; файл появился в папке резервных копий (параметр «Папка backup»). Для регулярных копий включите «Автобэкап» с расписанием.

Восстановление:

1. В той же секции выберите файл копии («Выбрать backup»). Для зашифрованной копии укажите пароль в блоке «Пароль резервной копии» (если пароль уже задан в настройках, поле заполнится автоматически).
2. Нажмите «Восстановить» и подтвердите. Сервисы перезапустятся; панель показывает их состояние до полной готовности.

Проверка: после перезапуска данные соответствуют моменту копии; в журнале — события начала и завершения восстановления.

Восстановить можно только копию своей инсталляции; при переносе на новый сервер восстановление выполняется на чистую систему и завершается повторным вводом ключа активации (раздел 17.6).

15.11. Выборка событий за период

Роль: «Аудитор».

1. «Журналы»: задайте период «Дата: с — по».
2. Сузьте выборку категорией («Доступ» / «Аудит» / «Техсостояние») и фильтрами «Домен», «Результат», «Тип» — например, все отказы доступа за неделю: категория «Доступ», результат «Запрещено».
3. Для выборки по конкретному объекту, персоне или оператору добавьте объектную историю щелчком по значку участника.
4. События, требующие внимания, помечайте меткой (карточка события → «Метки») — затем фильтр «Метка» соберёт их в одну выборку.

Проверка: счётчик «Показано: N из M» отражает объём выборки; выбранные записи открываются с полным контекстом.

15.12. Проверить целостность журнала и архив

Роль: «Аудитор».

Живой журнал:

1. «Журналы» → панель инструментов → «Целостность журнала».
2. Нажмите «Проверить».

Проверка: результат «Целостность подтверждена: события №A–№B (N шт.)». Нарушение — повод для немедленного расследования: детали в событии проверки и тревоге.

Архив:

1. Панель инструментов → «Архив»: отметьте смежные файлы. Для зашифрованных — пароль подставится из настроек архива или введите его в блоке «Пароль архива» → «Открыть архив».
2. Система проверит цепочку и стыки файлов; сверху появится индикатор «АРХИВ» с результатом проверки целостности (подтверждена или нарушена).
3. Просмотрите события теми же фильтрами; по завершении — «Вернуться к живому журналу».

Проверка: индикатор целостности — без нарушений; события архива читаются, метки показаны как исторические.

Глава 16. Возможные неисправности

Глава организована по симптомам. Общий принцип диагностики — сверху вниз по цепочке: служба сервера → веб-интерфейс → линия → устройство → объект доступа → пропуск; на каждом уровне система показывает состояние и события, по которым локализуется отказ.

16.1. Не открывается веб-интерфейс

1. На сервере проверьте службу:

   ```
   sudo systemctl status srv_ctrl.service
   ```

   Если служба не в состоянии `active (running)` — перезапустите её (`sudo systemctl restart srv_ctrl.service`) и посмотрите журнал службы (`journalctl -u srv_ctrl.service`).

2. Проверьте готовность HTTP-сервиса: `curl -i http://localhost:8080/health` — ожидается код 2xx. Если ответа нет, проверьте, не занят ли порт и не изменён ли он в `/etc/skd/seenaptec_acs.yaml`.

3. С другого компьютера — проверьте сетевую доступность сервера и межсетевой экран; в адресе должен быть IP или DNS-имя сервера, а не `localhost`.

4. Проверьте доступность брокера MQTT с сервера. Без брокера страница может открываться, но живые состояния, события и часы сервера в верхней строке обновляться не будут.

16.2. Интерфейс открывается, но данные не обновляются

Признак: списки открываются, но состояния не меняются, событий нет, дата и время сервера в верхней строке не идут.

Причина — нет живого потока данных: недоступен брокер MQTT или разорвано соединение браузера с сервером (поток оперативных событий).

1. Обновите страницу браузера.
2. Проверьте брокер MQTT и его доступность с сервера.
3. Проверьте состояние сервисов: «Настройка / Обслуживание» → панель инструментов → «Управление сервисами» (или запросом `GET /health` проверьте готовность HTTP-сервиса).

16.3. Линия в состоянии «Нет связи», «Возможно обрыв» или «Неактивно»

- **«Неактивно»** — линия не задействована: включите «Задействовать» в карточке линии.
- **«Порт недоступен»** — сервис не может открыть порт: для USB проверьте, что преобразователь подключён и имя порта верно; для TCP — что адрес `host:port` достижим с сервера.
- **«Нет связи»** — порт открыт, но устройства не отвечают: проверьте питание устройств, полярность и целостность шины RS-485, совпадение скорости линии со скоростью устройств.
- **«Возможно обрыв»** — адаптер работает и опрос идёт, но ни одно устройство линии не отвечает дольше минуты: проверьте целостность шины RS-485 (обрыв, замыкание) и питание устройств линии.
- Записи обмена смотрите в панели «Отладка» (журнал работы экземпляра `srv_osdp` линии), историю смен состояния — в панели «События».

16.4. Устройство не отвечает или найдено не полностью

- Устройство в состоянии «Новое» — оно не обслуживается до принятия: откройте карточку и нажмите «Принять».
- Устройство не задействовано («(выкл)») — включите «Задействовать».
- SSB-поиск нашёл не все приборы — запустите поиск повторно: первый проход может быть неполным из-за задержек появления устройств на шине.
- **Конфликт адресов**: два устройства с одним OSDP-адресом на линии дают неустойчивую связь обоих. Разнесите адреса — для AGRG-устройств адреса назначает SSB-поиск, для сторонних смените адрес в карточке («Подключение» → «Сменить») или на самом устройстве.
- Если устройство отвечало и перестало после смены режима шифрования — проверьте состояние Secure Channel в секции «Подключение»; при утере рабочего ключа выполните сброс ключа устройства и повторную установку.

16.5. Доступ не выдан, хотя пропуск активен

Причина отказа всегда записана в событии «Доступ запрещён» — начните с него: «Объекты доступа» → объект → панель «События» (или «Журналы», категория «Доступ»). Типовые причины:

Причина в событии	Что проверить
«Доступ запрещён: идентификатор не найден»	Карта не заведена или изъята; код в панели «Идентификаторы»
«Доступ запрещён: нет прав на этот объект»	Объект (или его тег) не входит в пропуск
«Доступ запрещён: вне разрешённого расписания»	Временной профиль объекта и «Время доступа» пропуска
«Доступ запрещён: нерабочий день по производственному календарю»	Тип дня в календаре и настройка «Учитывать производственный календарь»
«Неверный PIN-код»	Режим идентификации объекта «Карта + PIN» и PIN персоны
«Доступ запрещён: требуется подтверждение»	Режим с подтверждением: персона с признаком «Требует подтверждения» ждёт карты подтверждающего; либо предъявление в открытой двери, которую подтверждающий сессии не покрывает (раздел 4.3)
«Доступ запрещён: подтверждающий не подтвердил вовремя»	Окно ожидания — 15 секунд; повторите предъявление и подтвердите сразу
«Доступ запрещён: карта подтверждающего не имеет прав»	У подтверждающего отозван признак «Может подтверждать» или предъявлена чужая карта
«Доступ запрещён: у подтверждающего нет доступа к объекту»	У подтверждающего нет собственного действующего пропуска на этот объект
«Доступ запрещён: подтверждение вытеснено новым запросом»	На той же точке запросили подтверждение другой персоны; повторите предъявление
«Запрет повторного прохода: …»	Присутствие персоны в периметре АПБ («Текущий доступ» → «Присутствие»; если нужно — сброс)
«Доступ запрещён: действует ограничивающее условие» / «отсутствует требуемое условие»	Условия персоны и правила объекта
«Доступ запрещён: объект заблокирован»	Оператор перевёл объект в режим «Заблокирован» — сбросьте режим в карточке

Также проверьте состояние персоны («Приостановлена» и «В черном списке» блокируют доступ), состояние пропуска («Приостановлен», срок, остаток кратности) и состояние идентификатора («Утеряно», «Истекло»).

16.6. Событие доступа не появляется вовсе

Если при предъявлении карты нет даже события отказа:

1. Проверьте связь линии и устройства (разделы 16.3–16.4).
2. Включите режим «Пусконаладка (LIVE)» в панели «События» «Настройки / Обслуживания» и приложите карту: если сигнала считывания нет — проблема в считывателе или шине; если сигнал есть — переходите к следующему шагу.
3. Проверьте привязку считывателя к объекту доступа (состояние объекта должно быть «Настроено»).
4. Проверьте, что сервис логики доступа запущен («Управление сервисами» → «Сервер доступа»).

16.7. Резервирование не в норме

Итоговое состояние показывают бейдж режима кольца в строке и карточке линии (строка «Кольцо») и индикаторы портов «Основной»/«Резервный»:

- **«Разрыв: опрос по сегментам»** — шина разорвана: устройства каждого сегмента опрашиваются через доступный им порт. Проверьте кабельную трассу между сегментами; после устранения разрыва устройства автоматически вернутся на основной порт;
- **«Работает резервный адаптер»** — основной контур недоступен целиком (отказ преобразователя, потеря TCP-связи): проверьте преобразователь и TCP-доступность основного порта; после восстановления опрос вернётся на основной порт автоматически;
- **«Работает основной адаптер»** — недоступен резервный контур: проверьте преобразователь и TCP-доступность резервного порта; опрос устройств при этом идёт через основной порт, после восстановления кольцо вернётся

в норму автоматически;
- **«Линия недоступна»** — недоступны оба контура: проверяйте оба преобразователя и трассы.

При разрыве и при отказе одного из контуров состояние связи линии и устройств остаётся «Активно» — обмен идёт; отказавший порт виден по погашенным точкам его индикатора (подключение, приём, эхо). «Порт недоступен» линия показывает, только когда недоступны оба порта.

Если режим нормальный, но часть устройств опрашивается через резервный порт (чип «Резервный» у устройства), — это следствие недавнего разрыва: маршрут вернётся на основной порт после выдержки против частых переключений.

История — в панели «События» (события «Кольцо линии разорвано: опрос по сегментам», «Кольцо линии восстановлено», «Потерян адаптер линии», «Адаптер линии восстановлен», «Изменён маршрут опроса устройства»); детали обмена — в панели «Отладка» (журнал единый для обоих портов кольца).

16.8. Тревога «Нарушение целостности журнала»

Тревога означает, что проверка обнаружила расхождение хеш-цепочки журнала: изменение, вставку, удаление записей или перезапись конечной части журнала. Запись новых событий продолжается.

1. Откройте событие проверки — в нём указаны вид нарушения и первая повреждённая запись.
2. Зафиксируйте обстоятельства (доступ к серверу, время) — нарушение целостности означает вмешательство в файлы данных либо их повреждение.
3. Сверьте резервные копии и архивы журнала (их целостность проверяется независимо при открытии).
4. Примите тревогу с комментарием о результатах расследования.

16.9. Забыт пароль администратора

Если доступен другой оператор с полными правами по домену «Безопасность» — смените пароль администратора из его карточки (учётные записи администраторов изменяет только администратор). Если административный доступ утрачен полностью, а восстановление доступа включено — войдите по одноразовому коду поставщика с экрана входа (раздел 17.8). Если восстановление не включалось, самостоятельный сброс невозможен — обратитесь в поддержку производителя.

16.10. Панель ОПС и её устройства в состоянии «НЕТ СВЯЗИ»

Если пожарная панель UniPOS перестаёт отвечать по протоколу Modbus TCP, система переводит в статус **«НЕТ СВЯЗИ»** как саму панель, так и все её системные блоки (`БП`, `БИО`, `БРВ`), кольцевые шлейфы, адресные извещатели/модули и пожарные зоны (`D`, `A`, `P`), чтобы не отображать устаревшую норму при потере канала связи (раздел 10.9).

Порядок диагностики:

1. **Проверьте службу опроса панели.** Откройте «Настройка / Обслуживание» → панель инструментов → «Управление сервисами» и убедитесь, что экземпляр **«Сервер ОПС панели N»** (`srv_ops`) запущен, а в карточке панели в секции «Подключение» включён параметр «Опрос включён».
2. **Проверьте сетевые параметры и однопользовательский режим TCP.** В карточке панели (секция «Подключение») проверьте IPv4-адрес, TCP-порт (по умолчанию `502`), `Modbus Unit ID` (для UniPOS IFS7000 — `255`) и номер панели в кластере (`1`–`8`). Учитывайте, что Ethernet-модуль панели UniPOS обычно принимает только одно одновременное соединение Modbus TCP: если к прибору параллельно подключена сторонняя SCADA-система или конфигуратор, новое соединение может отклоняться или разрываться.
3. **Проверьте живую трассу Modbus-кадров в панели «Отладка».** Выберите панель ОПС в дереве «Оборудование» (режим `ОПС`), откройте нижнюю панель **«Отладка»**, включите переключатель **«MQTT»** и выберите уровень `DEBUG`:
   - строки **`ERR`** при подключении или чтении (`connection refused`, `i/o timeout`, `EOF`) указывают на сетевую недоступность IP-адреса, закрытый порт `502` или перехват TCP-сессии другим клиентом;
   - отправка **`TX fn=0x2B/0x0E`** или **`TX fn=0x03`** без ответных кадров **`RX`** означает отсутствие ответа от прибора по указанному `Unit ID` или таймаут обмена (при высокой загрузке прибора увеличьте «Таймаут ответа, мс»);
   - ответы **`RX EXC`** (например, `Illegal Data Address`) при опросе означают несоответствие номера панели в кластере или карты регистров модели прибора.

4. После восстановления сетевой доступности `srv_ops` автоматически переподключится к панели, перечитает состояния регистров и вернёт панель, шлейфы, устройства и зоны в актуальные рабочие статусы.

Глава 17. Лицензия: активация и жизненный цикл

Глава описывает весь жизненный цикл лицензии: получение ключа у поставщика, активация чистой системы, продление, обновление программного обеспечения, перенос на другой сервер и восстановление из резервной копии. Отдельные разделы посвящены коду для поддержки — отпечатку инсталляции, который привязывает лицензию к оборудованию (раздел 17.7), и восстановлению доступа по одноразовому коду поставщика, если утрачен пароль администратора (раздел 17.8). Процедура активации при установке описана в главе 6 — здесь она дана в контексте всего цикла.

17.1. Как устроено лицензирование

Лицензия в Seenaptec Access Platform (SAP) управляет **только сроком действия**: функциональность всегда полная, отдельно лицензируемых модулей, лимитов на устройства или рабочие места нет. Проверка лицензии выполняется полностью офлайн — системе не нужен доступ в интернет ни при активации, ни в работе.

Ключевой принцип — **мягкое принуждение**: система контроля доступа не имеет права остановить проходы из-за лицензии. Что бы ни происходило с лицензией — истёк срок, не введён новый ключ после обновления, — двери и контроллеры продолжают работать, решения о доступе принимаются, журнал ведётся. Лицензия ограничивает только административный контур: без активации нельзя войти в веб-интерфейс и настраивать систему, а при просрочке интерфейс настойчиво напоминает о продлении.

17.2. Ключ активации и два идентификатора

Ключ активации — строка из шести групп по четыре символа (цифры и латинские буквы A–F):

```
VVMM-SSSS-SSSS-HHHH-HHHH-HHHH
```

Ключ выдаёт поставщик системы; в нём закодированы срок действия лицензии (по последний день указанного месяца включительно), идентификатор инсталляции и защитная подпись. Вводить ключ можно с дефисами или без, строчными или заглавными буквами — форма ввода сама приводит его к каноническому виду. Внутреннее устройство ключа для эксплуатации значения не имеет; важно лишь, что подделать или «подправить» ключ нельзя — изменённый ключ система отклонит.

У инсталляции есть **два разных идентификатора**, которые не следует путать:

Идентификатор	Откуда берётся	Для чего служит
Идентификатор сервера (лицензионный)	Из ключа активации; одинаков во всех ключах, выданных этой инсталляции	Связь «инсталляция ↔ договор с поставщиком»: по нему поставщик выпускает ключи продления, по нему система отличает свой ключ от чужого и свою резервную копию от чужой
Серийный номер сервера	Генерируется системой автоматически при самом первом старте службы	Внутренняя адресация: обмен между сервисами платформы, цепочка журнала, имена файлов архива. В настройке не участвует и вручную не задаётся

Практическое правило: в разговоре с поставщиком фигурирует **идентификатор сервера** (он привязан к вашему договору); **серийный номер сервера** — служебный идентификатор, который может встретиться в именах файлов архива журнала и в диагностике, но никаких действий администратора не требует.

Кроме двух идентификаторов, у инсталляции есть **код для поддержки** — отпечаток по серийным номерам оборудования: он подтверждает привязку лицензии к железу объекта и меняется при замене устройств (раздел 17.7).

17.3. Активация чистой системы

1. Получите ключ активации у поставщика — он выдаётся вместе с поставкой или по запросу по условиям договора.

2. Установите серверную часть (глава 6) и откройте веб-интерфейс. На неактивированной системе показывается экран «Активация системы».
3. Введите ключ и нажмите «Активировать».

При верном ключе система привязывается к лицензии, автоматически создаётся оператор `admin` с паролем по умолчанию `123456`, и показывается экран входа с подсказкой «Система активирована. Вход по умолчанию: admin / 123456 — после входа смените небезопасный пароль». Первый вход и обязательная смена пароля описаны в разделе 6.7; тревожные события при входе с паролем по умолчанию — в главе 14.

До активации службы платформы работают в штатном режиме — активация ничего не «включает» на уровне оборудования, она открывает административный доступ. Настроить объект без активации всё равно невозможно: в интерфейс не войти.

17.4. Просроченная лицензия и продление

Когда срок лицензии истекает, система **продолжает работать полностью**: проходы обслуживаются, события пишутся, операторы работают в интерфейсе. Меняется только поведение интерфейса:

- поверх приложения постоянно виден баннер: «Лицензия просрочена. Срок действия истёк ‹дата›. Система продолжает работать; обратитесь к поставщику за новым ключом активации»;
- периодически показывается модальный диалог «Срок действия лицензии истёк» с полем «Ключ активации». Кнопка «Отмена» закрывает диалог и откладывает напоминание **на 5 минут**, после чего он появляется снова; работе это не мешает, но игнорировать просрочку бесконечно не даст;
- то же предупреждение показывается на экране входа.

Для продления запросите у поставщика новый ключ (он выпускается на тот же идентификатор сервера, но с более поздним месяцем окончания) и введите его в диалоге — либо сразу после получения, не дожидаясь диалога, в том же окне при очередном напоминании. После принятия ключа баннер и диалог исчезают без перезапуска системы.

Если введённый ключ формально верен, но его срок тоже уже в прошлом, система примет его и сообщит: «Ключ принят, но срок действия уже истёк. Обратитесь к поставщику за ключом на текущий месяц».

17.5. Обновление ПО и переходный период 14 дней

Поставщик может менять **поколение ключей активации** — обычно вместе с крупными обновлениями продукта. Если установленное обновление сменило поколение, прежний ключ не становится недействительным мгновенно: действует **переходный период 14 дней**. В интерфейсе на это время появляется предупреждающий баннер: «Обновление сменило поколение ключа. Старый ключ действует ещё N дн. — получите новый ключ у поставщика».

Порядок действий администратора:

1. Увидев баннер, запросите у поставщика ключ нового поколения (идентификатор сервера и срок лицензии не меняются — меняется только поколение).
2. Введите новый ключ — до окончания переходного периода это можно сделать в любой момент; после ввода баннер исчезает.

Если за 14 дней ключ не введён, старый ключ перестаёт приниматься, и при следующем входе система потребует ввести ключ нового поколения (экран активации). На работу дверей и контроллеров истечение переходного периода, как и любая другая лицензионная ситуация, не влияет.

Начало и истечение переходного периода фиксируются в журнале событий; истечение — тревожным событием.

17.6. Перенос, восстановление и повторная активация

Ключ активации хранится на сервере в защищённом локальном хранилище и **не попадает в обычную резервную копию** — копию можно передавать и хранить, не опасаясь утечки ключа. Из этого следуют правила переноса и восстановления. Отдельный случай — копия с включённой настройкой «Включать секреты»: она содержит все секреты системы, включая ключ активации, и всегда зашифрована (раздел 10.8); такую копию храните как пароль.

Восстановление на своей инсталляции (тот же сервер, штатный откат к копии) проходит без лицензионных действий: ключ на месте, идентификатор сервера совпадает.

Перенос на новый сервер: установите серверную часть на новой машине и восстановите резервную копию **на чистую, ещё не активированную систему** — это разрешено. Ключа на новой машине нет, поэтому после восстановления система перейдёт в режим повторной активации: на экране активации появится пояснение «Ключ активации утрачен. Введите ключ этой инсталляции (тот же server id) — учётные записи операторов сохранены». Введите тот же ключ, что использовался раньше (или запросите его у поставщика повторно). Оператор `admin` при повторной активации **не создаётся** — все учётные записи пришли из копии, вход выполняется по прежним паролям. Если копия создана с переносом секретов, ключ активации восстанавливается вместе с остальными секретами — повторная активация не потребуется.

Чужая резервная копия — копия, снятая с другой инсталляции (с другим идентификатором сервера), — **не восстанавливается**: система отклонит восстановление. Это защита от смешения данных двух инсталляций; объединить или «перелить» одну инсталляцию в другую через резервную копию нельзя.

Ключ с чужим идентификатором сервера отклоняется и при активации: форма сообщит «Ключ выпущен для другой инсталляции (другой server id)».

17.7. Код для поддержки (отпечаток инсталляции)

Код для поддержки — короткий код-отпечаток инсталляции, который привязывает лицензию к оборудованию объекта. Код не секретен и не даёт доступа к системе: это опознавательный знак «именно этой» инсталляции. Поддержка сверяет продиктованный код с записанным в карточке клиента и так подтверждает, что обращение относится к инсталляции из договора.

Отпечаток строится по ядру устройств — до пяти устройств, которые приняты в конфигурацию, задействованы, привязаны к объектам доступа и выходят на связь. Состав ядра система выбирает и пополняет сама, вручную изменить его нельзя. Код состоит из групп по четыре символа, разделённых дефисом, — по группе на каждое устройство ядра, например `F5A2-CECD-2026-F0B2`.

Где посмотреть код

1. Щелчком по логотипу системы в левом верхнем углу экрана откройте «Обзор системы».
2. Откройте панель инструментов — кнопка с шестерёнкой у правого нижнего края экрана.
3. Найдите секцию «Поддержка».

Секция показывает три значения:

- **Server ID** — идентификатор сервера из ключа активации (раздел 17.2); если система не активирована, вместо него показан прочерк;
- **Код инсталляции** — сам отпечаток;
- **Серийный номер** — серийный номер сервера (раздел 17.2).

Кнопка «Скопировать всё» копирует все три значения одним блоком — его удобно вставить в письмо или заявку. При обращении в поддержку продиктуйте **Server ID и код инсталляции**: по Server ID поддержка находит карточку вашей инсталляции, по коду подтверждает привязку к оборудованию.

Раскрывающийся блок «Состав отпечатка» показывает устройства ядра: группу кода, линию и адрес устройства, его серийный номер. Пометка «давно не было в сети» означает, что устройство больше двух недель не выходило на связь; если перерыв затянется до месяца, устройство выпадет из отпечатка, и код изменится.

Когда код меняется

Код меняется, когда меняется состав ядра: при замене неисправного устройства новым (раздел 10.4) или когда устройство больше месяца не выходит на связь и выпадает из отпечатка. Дата последнего изменения показана в «Составе отпечатка» — «действует с …». После замены устройства из состава отпечатка сообщите поддержке новый код, иначе сверка при следующем обращении не сойдётся.

Строка «Состояние устройств обновляется после перезапуска» появляется сразу после перезапуска сервера: система ещё не успела опросить устройства и показывает код по сохранённому составу. Это штатная ситуация: код при этом верный, а после первого опроса устройств строка исчезает.

Почему кода может не быть

Отпечаток строится, только когда в эксплуатации минимум два устройства. Пока их меньше, вместо кода показано сообщение «Код появится после ввода в эксплуатацию минимум 2 устройств» — так же выглядит и новая система до первого опроса оборудования. Примите устройства в конфигурацию, задействуйте их и привяжите к объектам доступа (глава 10) — код появится автоматически.

17.8. Восстановление доступа по коду поставщика

Восстановление доступа — запасной вход в систему на случай, когда пароль `admin` утрачен или его учётная запись удалена, а других операторов с полными правами нет. Вход выполняется по одноразовому коду, который выдаёт поставщик после проверки клиента по своему регламенту. На сервере хранится только хэш ожидаемого кода: ни чтение базы данных, ни резервная копия доступа не дают, а сам код поставщик вычисляет по секрету, который в продукт не входит.

Регламент безопасности: держите восстановление выключенным и включайте его на время сессии поддержки. Пока восстановление выключено, вход по коду невозможен в принципе. Включайте его заблаговременно — когда привлекаете поставщика к работам на системе: включение требует живого административного доступа, поэтому после утраты пароля включить восстановление уже нельзя. По завершении работ выключите восстановление.

Включение и выключение

1. Запросите у поставщика **хэш первого кода** — поддержка вычисляет его по идентификатору сервера (раздел 17.2) и записывает в карточку вашей инсталляции.
2. Откройте «Обзор системы» (щелчок по логотипу системы) → панель инструментов → секцию «Восстановление доступа» (между «Поддержкой» и «Порогами внимания»).
3. Вставьте полученный хэш в поле «Хэш первого кода» — это строка из 64 шестнадцатеричных символов (SHA-256); регистр и лишние разделители при вводе не важны — и нажмите «Включить».

Секция показывает состояние — «Включено» (с датой обновления хэша) или «Выключено» — и при включённом восстановлении сам **хэш ожидаемого кода**: сверьте его с записью в карточке инсталляции у поставщика, чтобы убедиться, что стороны синхронны. Тем же полем выполняется замена хэша (кнопка «Заменить хэш») — например, при рассинхронизации цепочки. Кнопка «Выключить» запрашивает подтверждение и отключает восстановление: сохранённый хэш удаляется, и для повторного включения запросите у поставщика новый хэш.

Просмотр секции доступен при уровне «Чтение» в области «Операторы» домена «Безопасность», включение, замена и выключение — при уровне «Полный» (глава 14).

Вход по коду восстановления

1. Обратитесь к поставщику. После проверки по регламенту поддержка выдаст **строку восстановления** вида `КОД.ХЕШ` — одноразовый код и хэш следующего кода одной строкой.
2. На экране входа нажмите «Восстановить доступ» — кнопка показывается, только когда восстановление включено.
3. Введите **ключ активации** инсталляции и **строку восстановления**, нажмите «Восстановить». Требуются оба значения: ключ и строка приходят разными каналами (договорные документы и переписка с поддержкой), поэтому перехват одного сообщения доступа не даёт.
4. При верных данных система сбрасывает пароль `admin` на пароль по умолчанию (удалённую учётную запись `admin` создаёт заново), завершает все прежние сессии `admin` и сразу открывает новую сессию с принудительной сменой пароля — задайте новый пароль, как при первом входе (раздел 6.7).

Код одноразовый: при успешном входе система запоминает хэш следующего кода из выданной строки, и повторить вход с той же строкой нельзя. Следующую строку при необходимости выдаёт поставщик — цепочка кодов «скользит» вперёд, поэтому перехваченная переписка бесполезна.

При неверном ключе форма сообщает «Ключ активации не подходит», при неверной строке — «Неверный код восстановления». Если восстановление успели выключить между загрузкой страницы и попыткой входа, форма сообщит: «Восстановление доступа выключено администратором».

Журнал и защита от подбора

Каждый шаг восстановления фиксируется тревожным событием (раздел 13.4): «Включено восстановление доступа», «Отключено восстановление доступа», «Выполнено восстановление доступа», «Неудачная попытка восстановления доступа», «Восстановление доступа заблокировано анти-брутфорсом». После нескольких неудачных попыток система вводит нарастающую паузу между ними — форма сообщает «Слишком много попыток восстановления» и время ожидания; счётчик неудач хранится на сервере и не сбрасывается перезапуском.

17.9. Типичные ситуации

Потеряли ключ активации. Ключ не секрет одноразового действия — поставщик хранит выданные ключи и по запросу по условиям договора сообщит ключ вашей инсталляции повторно. Пока система работает, потеря записанного ключа ни на что не влияет: он сохранён на сервере. Ключ понадобится заново при переносе или восстановлении на чистую систему (раздел 17.6).

Забыли пароль `admin`, других администраторов нет. Если восстановление доступа включено, запросите у поставщика строку восстановления и войдите кнопкой «Восстановить доступ» на экране входа (раздел 17.8). Если восстановление не включалось, самостоятельного пути нет — обратитесь к поставщику.

Переносим сервер на новое железо. Сделайте свежую резервную копию, установите пакет на новой машине, восстановите копию на чистую систему, введите ключ инсталляции повторно (раздел 17.6). Двери на время переноса управляются в объёме автономных возможностей оборудования; после запуска нового сервера работа продолжается с данными на момент копии.

Срок лицензии истёк в выходные. Ничего экстренного не происходит: проходы работают, журнал ведётся, тревоги принимаются. Операторы будут видеть баннер и периодический диалог продления — «Отмена» откладывает его на 5 минут. В рабочий день запросите и введите новый ключ (раздел 17.4).

Обновили ПО — появился жёлтый баннер про поколение ключа. Это переходный период (раздел 17.5): у вас 14 дней, чтобы получить у поставщика ключ нового поколения и ввести его. Срок и идентификатор сервера при этом не меняются.

Система отклоняет ключ с сообщением про другую инсталляцию. Введён ключ от другого объекта или договора. Сверьте с поставщиком, какой идентификатор сервера закреплён за этой инсталляцией, и получите ключ именно для неё.

Можно ли эксплуатировать систему без активации? Службы работают, но войти в интерфейс и настроить систему нельзя — на чистой системе настраивать и некому, и нечего. Активация — первый шаг ввода в эксплуатацию (глава 6).

Поддержка просит «код для поддержки» — где его взять? Откройте «Обзор системы» (щелчок по логотипу системы) → панель инструментов → секция «Поддержка» и продиктуйте Server ID и код инсталляции (раздел 17.7). Если недавно меняли устройства, код мог измениться — диктуйте текущий из секции.

Глава 18. Интеграция через API

Все функции системы доступны через REST API — тот же интерфейс, которым пользуется веб-приложение. Глава описывает общий порядок интеграции: где взять спецификации, как авторизуется внешняя система и какие права нужны типовым задачам. Отдельные методы API в руководстве не описываются — они документированы в спецификациях OpenAPI.

18.1. Спецификации и Swagger UI

Ресурс	Адрес
Swagger UI — интерактивный просмотр и вызов методов	`http://<адрес-сервера>:8080/api-docs/`
Файлы спецификаций OpenAPI и документация	`http://<адрес-сервера>:8080/docs/`

API разделён на области, каждая со своим префиксом пути:

Область	Префикс	Содержимое
Оборудование	`/api/hw/`	Сервер, линии, устройства, объекты доступа, привязки, состояние сервисов
Данные доступа	`/api/perm/`	Персоны, идентификаторы, пропуска, шаблоны, теги
Журнал	`/api/journal/`	События, тревоги, метки, поток оперативных событий
Аутентификация и безопасность	`/api/auth/`	Вход, операторы, роли, сессии, настройки безопасности

Готовность сервера проверяется запросом `GET /health` (ответ `ok`, авторизация не требуется).

18.2. Авторизация внешней системы

Внешняя система авторизуется так же, как оператор: для неё создаётся отдельная учётная запись оператора с ролью, ограниченной необходимыми правами (глава 14). Порядок работы:

1. Администратор создаёт роль с минимально необходимым набором прав и учётную запись для интеграции.
2. Внешняя система выполняет вход (`POST /api/auth/api/v1/login` с логином и паролем) и получает сессионный cookie `skd_operator_session`.
3. Все дальнейшие запросы выполняются с этим cookie. Сессия продлевается при каждом запросе; при простое дольше установленного времени неактивности (настраивается в «Настройках безопасности», глава 14) сессия истекает, и вход нужно повторить.

Действия интеграционной учётной записи фиксируются в журнале аудита наравне с действиями операторов, а её активные сессии видны на панели «Сессии» рабочей области «Безопасность».

18.3. Модель прав

Права описываются ключом «домен → область → уровень». Доменов пять:

Домен	Что охватывает
`equipment`	Оборудование: сервер, линии, устройства, системные операции
`access`	Объекты доступа, правила, текущий доступ
`iam`	Персоны, идентификаторы, пропуска, шаблоны
`security`	Операторы, роли, секреты, АРМ считывателей, профили карт, аудит платформы
`journal`	Журнал событий, тревоги, целостность, архив

Уровни прав кумулятивны — каждый следующий включает предыдущие:

- `read` — чтение;
- `issue_tpl` — только для области пропусков: выдача строго по шаблонам, помеченным для ограниченной выдачи;
- `add` — создание записей;
- `full` — изменение и удаление.

Базовое правило соответствия HTTP-методов: `GET` требует `read`, `POST` — `add`, `PUT`/`DELETE` — `full`. Точные требования каждого метода перечислены в спецификациях.

18.4. Права для типовых задач интеграции

Задача	Достаточные права
Чтение журнала событий (весь журнал)	`journal.events.read`
Чтение событий одной зоны (например, только доступа)	право чтения домена этой зоны (например, `access.config.read`)
Мониторинг оборудования: состояния линий и устройств	`equipment.devices.read`
Синхронизация персонала: создание персон	`iam.persons.add`
Выдача пропусков по разрешённым шаблонам	`iam.passes.issue_tpl` + `iam.persons.read`
Полное управление пропусками (включая изъятие)	`iam.passes.full`
Чтение текущего доступа (периметры, сессии)	`access.config.read`

Правило проектирования интеграции: выдавайте роль с минимальным достаточным уровнем. Например, системе кадрового учёта, которая заводит сотрудников и выдаёт стандартные пропуска, достаточно `iam.persons.add` и `iam.passes.issue_tpl` — она не сможет менять оборудование, настройки и чужие данные.

18.5. Особенности, которые следует учитывать

- **Команды асинхронны.** Успешный ответ на команду оборудованию означает принятие команды, а не её выполнение; результат подтверждается состоянием или событием журнала (глава 8).
- **Идентификаторы записей не переиспользуются.** Числовые `id` персон, пропусков, идентификаторов и других сущностей присваиваются сервером и после удаления записи никогда не выдаются повторно — их можно безопасно хранить во внешней системе как устойчивые ссылки.
- **Пропуск после выдачи неизменяем в ключевых полях.** Разрешены продление, пополнение кратности, привязка идентификаторов и смена состояния; персона, дата начала и набор объектов выданного пропуска не меняются (глава 12).
- **Живые данные** доступны через поток оперативных событий журнала (Server-Sent Events):

  `GET /api/journal/api/v1/journal/stream/operational`

  Проверка прав по запрошенным зонам — та же, что у истории.

Глава 19. Реквизиты и контакты

Эта редакция руководства ориентирована на рынок Российской Федерации и русскоязычную эксплуатацию.

Наименование	ООО «Синаптек»
ИНН	7717776110
КПП	771601001
ОГРН	1147746137769
Адрес	129343, г. Москва, проезд Серебрякова, д. 8, стр. 1, эт. 2, пом. I, оф. 6
Телефон	+7 (495) 255-27-35
E-mail	kf@seenaptec.com

Инновационный центр «Сколково»

