

Ай Ти Ви групп

Руководство по настройке и работе с модулем интеграции
«Securiton»

Версия 1.1

Москва 2012



Содержание

СОДЕРЖАНИЕ	2
1 СПИСОК ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ	4
2 ВВЕДЕНИЕ	5
2.1 Назначение документа	5
2.2 Структура и функциональные возможности СКУД ПК «Интеллект»	5
2.3 Назначение модулей интеграции оборудования СКУД ПК «Интеллект»	5
2.4 Общие сведения о модуле интеграции «Securiton»	6
3 НАСТРОЙКА МОДУЛЯ ИНТЕГРАЦИИ «SECURITON»	7
3.1 Порядок настройки модуля интеграции «Securiton»	7
3.2 Настройка подключения СКУД «Securiton»	7
3.3 Построение дерева объектов СКУД «Securiton»	8
3.4 Настройка объектов СКУД «Securiton»	9
3.4.1 Настройка периферийного контроллера Securiton	9
3.4.2 Настройка выхода	10
3.4.3 Настройка типа датчиков Securiton	12
3.4.4 Настройка датчика	14
3.4.5 Настройка дверной зоны Securiton	16
3.4.6 Настройка двери	17
3.4.7 Настройка списка датчиков Securiton	21
3.4.8 Настройка списка дверных зон	22
3.5 Пересылка конфигурации в Site-контроллер Securiton	23
3.6 Настройка динамической пересылки данных СПР	24
3.7 Удаление неактуальных пользователей	24
3.8 Удаление неактуального оборудования	25
3.9 Переподключение к Site-контроллеру	26
4 РАБОТА С МОДУЛЕМ ИНТЕГРАЦИИ «SECURITON»	27
4.1 Общие сведения о работе с модулем интеграции «Securiton»	27
4.2 Управление выходом	27

4.3	Управление датчиком	27
4.4	Управление дверью Securiton	28

1 Список используемых терминов

Доступ – перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

Система контроля и управления доступом (СКУД) – программно-аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.

Контроль двойного прохода – контроль последовательности прохода (защита от повторного использования идентификатора для прохода в одном направлении).

Зональный контроль двойного прохода – контроль последовательности прохода, при котором пользователь должен сначала зарегистрироваться в **зоне выхода**, чтобы иметь возможность войти в **зону входа**, т.е. пройти определенный путь.

2 Введение

2.1 Назначение документа

Документ *Руководство по настройке и работе с модулем Securiton* является справочно-информационным пособием и предназначен для специалистов по настройке модуля *Securiton*. Данный модуль входит в состав системы контроля и управления доступом (СКУД), реализованной на основе программного комплекса *Интеллект*.

В данном Руководстве представлены следующие материалы:

1. общие сведения о модуле *СКУД Securiton*;
2. настройка модуля *СКУД Securiton*;
3. работа с модулем *СКУД Securiton*.

2.2 Структура и функциональные возможности СКУД ПК «Интеллект»

Система контроля и управления доступом (СКУД) ПК *Интеллект* может иметь следующую модульную структуру:

1. модули интеграции оборудования СКУД;
2. модуль *Фотоидентификация*;
3. модуль *Служба пропускного режима*;
4. модуль *Учет рабочего времени*.

При использовании СКУД ПК *Интеллект* доступны следующие функциональные возможности (в зависимости от установленных функциональных модулей):

1. возможность совмещения контроля доступа с другими подсистемами безопасности в одних и тех же центрах управления распределенной системы;
2. возможность запрограммировать реакции СКУД на события, в том числе происходящие в других подсистемах безопасности;
3. высокий уровень автоматизации механизма управления правами доступа;
4. возможность объединять пользователей в группы;
5. контроль состояния системы и ее работоспособности.

2.3 Назначение модулей интеграции оборудования СКУД ПК «Интеллект»

Модули интеграции оборудования СКУД выполняют следующие функции:

1. настройка взаимодействия ПК *Интеллект* и оборудования СКУД;

Примечание. Роль оборудования играет СКУД стороннего производителя.

2. обработка информации, поступающей от считывателей, электромеханических замков, и прочих средств контроля доступа;
3. управление исполнительными устройствами доступа – средствами блокировки и отпирания ворот и пр.

2.4 Общие сведения о модуле интеграции «Securiton»

Модуль *Securiton* является компонентом СКУД, реализованной на базе ПК *Интеллект*, и предназначен для выполнения следующих функций:

1. конфигурирование *СКУД Securiton* (производитель SECURITON AG);
2. обеспечение взаимодействия *СКУД Securiton* с ПК *Интеллект* (мониторинг, управление).

Примечание. Подробные сведения о СКУД Securiton приведены в официальной справочной документации по данной системе.

Перед настройкой модуля *Securiton* необходимо выполнить следующие действия:

1. установить аппаратные средства *СКУД Securiton* на охраняемый объект (см. справочную документацию по *СКУД Securiton*);
2. подключить *СКУД Securiton* к Серверу *Интеллект* (см. справочную документацию по *СКУД Securiton*).

3 Настройка модуля интеграции «Securiton»

3.1 Порядок настройки модуля интеграции «Securiton»

Настройка модуля *Securiton* производится в следующей последовательности:

1. Настроить подключение *СКУД Securiton*.
2. Построить дерево объектов *СКУД Securiton*.
3. Настроить объекты *СКУД Securiton*.
4. Переслать конфигурацию в Site-контроллеры *Securiton*.

3.2 Настройка подключения СКУД «Securiton»

В программном комплексе *Интеллект* настройка подключения *СКУД Securiton* осуществляется на панели настроек объекта **СКУД «Securiton»**. Данный объект создается на базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.2—1).

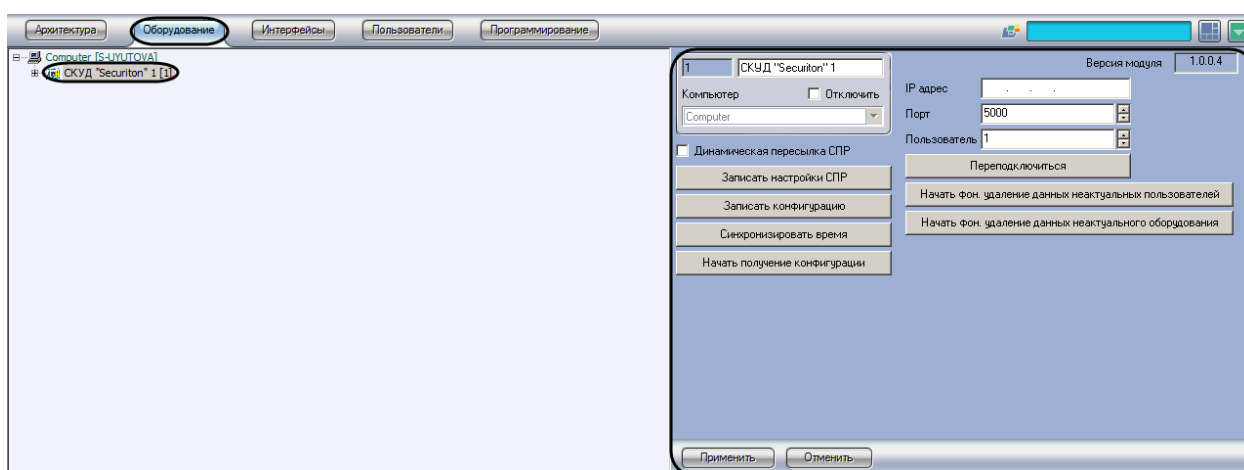


Рис. 3.2—1 Объект СКУД «Securiton»

Настройка подключения *СКУД Securiton* осуществляется в следующей последовательности:

1. Перейти на панель настроек объекта **СКУД «Securiton»** (Рис. 3.2—2).

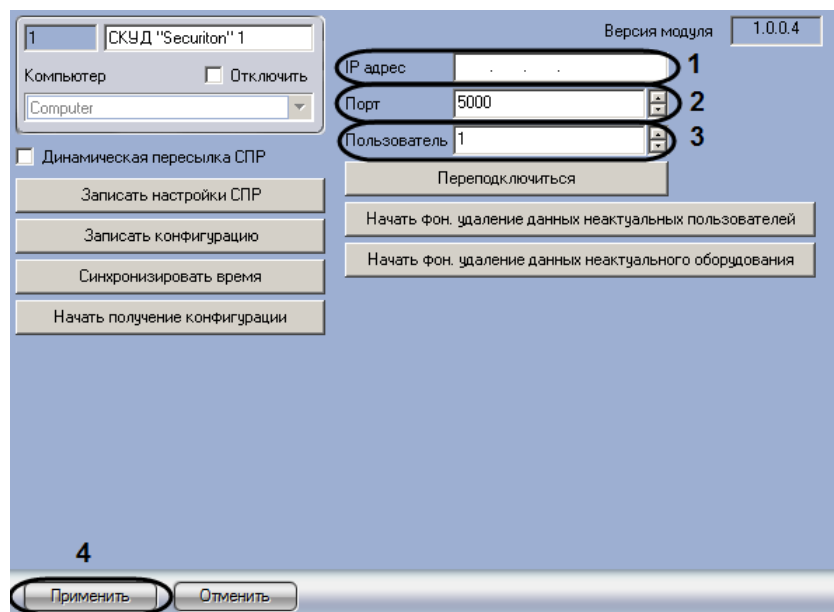


Рис. 3.2—2 Настройка подключения СКУД Securiton

2. Ввести IP адрес контроллера в поле **IP адрес** (см. Рис. 3.2—2, 1).
3. Ввести при помощи кнопок **вверх-вниз** номер порта, используемого для передачи данных контроллеру, в поле **Порт** (см. Рис. 3.2—2, 2).
4. Ввести идентификатор пользователя в поле **Пользователь** (см. Рис. 3.2—2, 3).
5. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.2—2, 4).

Настройка подключения к СКУД Securiton завершена.

3.3 Построение дерева объектов СКУД «Securiton»

Построение дерева объектов СКУД Securiton может быть произведено одним из следующих способов:

1. Вручную. В данном случае объекты, соответствующие устройствам СКУД Securiton создаются и настраиваются вручную.
2. Автоматически. В данном случае считывание конфигурации устройств СКУД Securiton и создание соответствующих им объектов в дереве оборудования ПК *Интеллект* осуществляется автоматически. Также при считывании конфигурации считываются настройки оборудования СКУД Securiton.

Автоматическое построение дерева объектов осуществляется в следующем порядке:

1. Перейти на панель настроек объекта **СКУД "Securiton"** (Рис. 3.3—1).

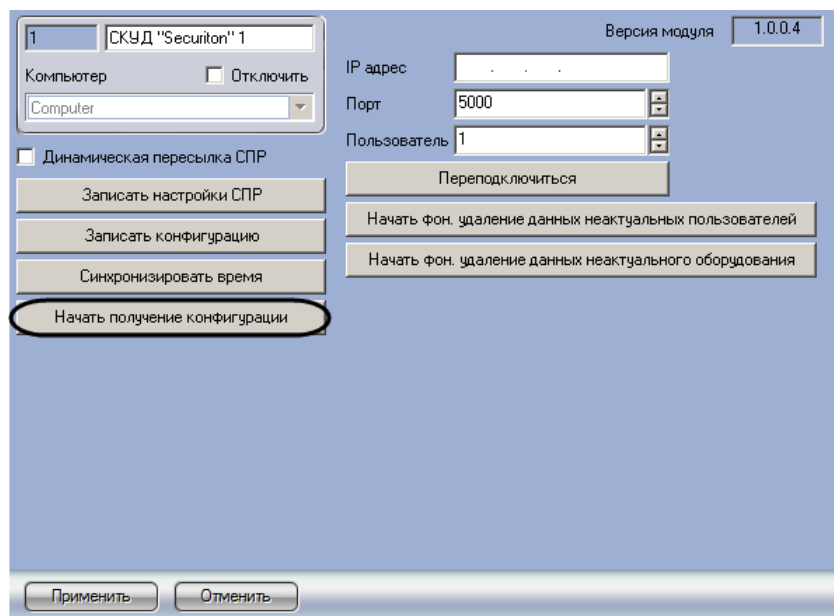


Рис. 3.3—1 Получение конфигурации

2. Нажать на кнопку **Начать получение конфигурации** (см. Рис. 3.3—1).
3. Дождаться завершения считывания конфигурации контроллера.

В результате выполнения указанных действий в дереве оборудования ПК *Интеллект* будут созданы объекты, соответствующие устройствам конфигурации, записанной в память контроллера *СКУД Securiton*.

Автоматическое построение дерева объектов завершено.

3.4 Настройка объектов СКУД «Securiton»

При настройке объектов *СКУД Securiton* следует следить за уникальностью значения в поле **Номер элемента в памяти** среди элементов одного типа: датчиков, выходов, дверей и т.д.

3.4.1 Настройка периферийного контроллера Securiton

В программном комплексе *Интеллект* настройка периферийного контроллера Securiton осуществляется на панели настроек объекта **Перифер. контроллер Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—1).

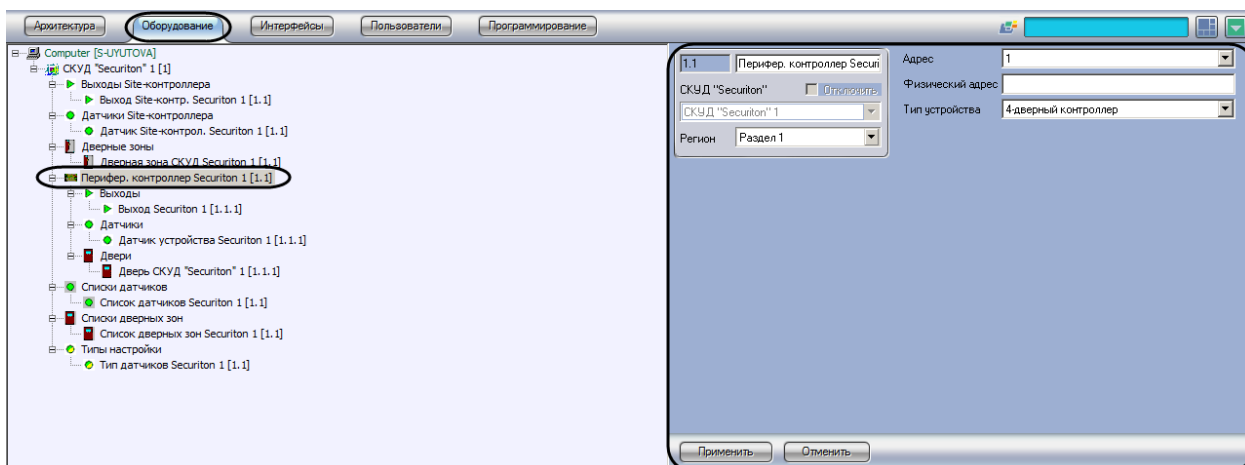


Рис. 3.4—1 Объект Периф. контроллер Securiton

Настройка периферийного контроллера осуществляется в следующей последовательности:

1. Перейти на панель настроек объекта **Перифер. контроллер Securiton** (Рис. 3.4—2).

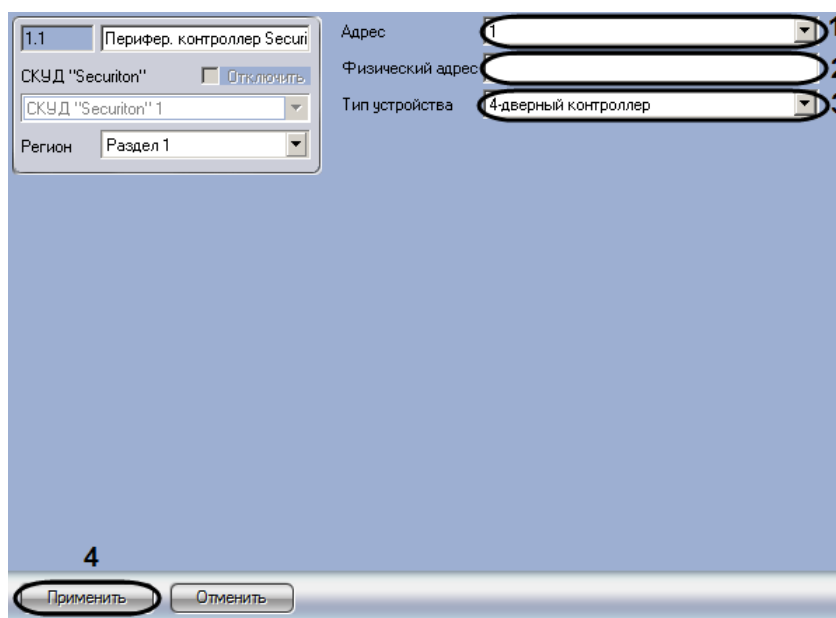


Рис. 3.4—2 Настройка периферийного контроллера

2. Из раскрывающегося списка **Адрес** выбрать уникальный номер контроллера (см. Рис. 3.4—2, 1).
3. В поле **Физический адрес** ввести физический адрес контроллера (см. Рис. 3.4—2, 2).
4. Из раскрывающегося списка **Тип устройства** выбрать тип подключенного периферийного контроллера (см. Рис. 3.4—2, 3).
5. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—2, 4).

Настройка периферийного контроллера Securiton завершена.

3.4.2 Настройка выхода

В программном комплексе *Интеллект* настройка выходов Site-контроллера и периферийного контроллера осуществляется идентично.

Настройка выхода Site-контроллера осуществляется на панели настроек объекта **Выход Site-контр. Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—3).

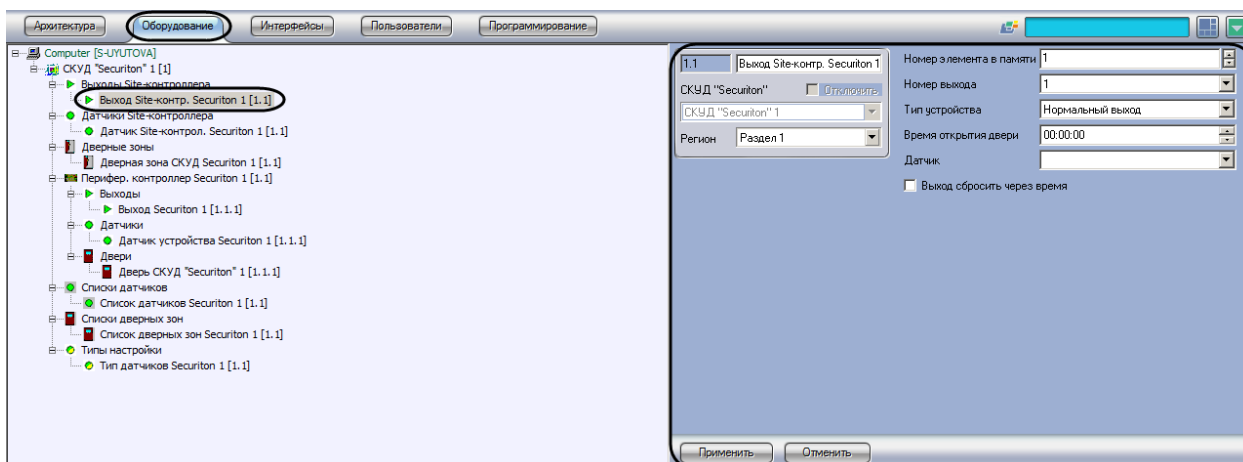


Рис. 3.4—3 Объект Выход Site-контр. Securiton

Настройка выхода периферийного контроллера осуществляется на панели настроек объекта **Выход Securiton**. Данный объект создается на базе объекта **Периферийн. контроллер Securiton** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—4).

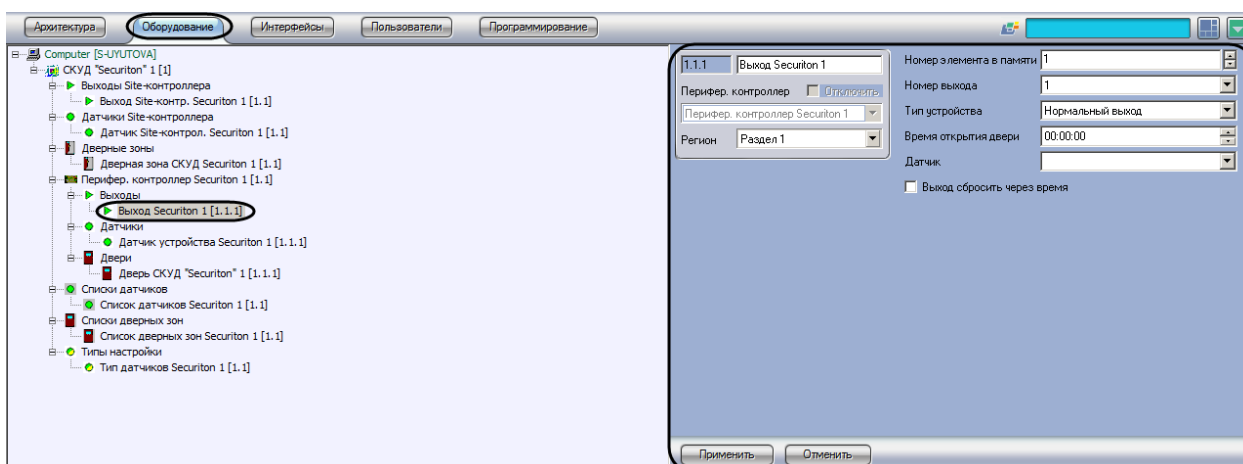


Рис. 3.4—4 Объект Выход Securiton

Настройка выхода осуществляется в следующем порядке:

1. Перейти на панель настроек объекта, соответствующего требуемому выходу (Рис. 3.4—5).

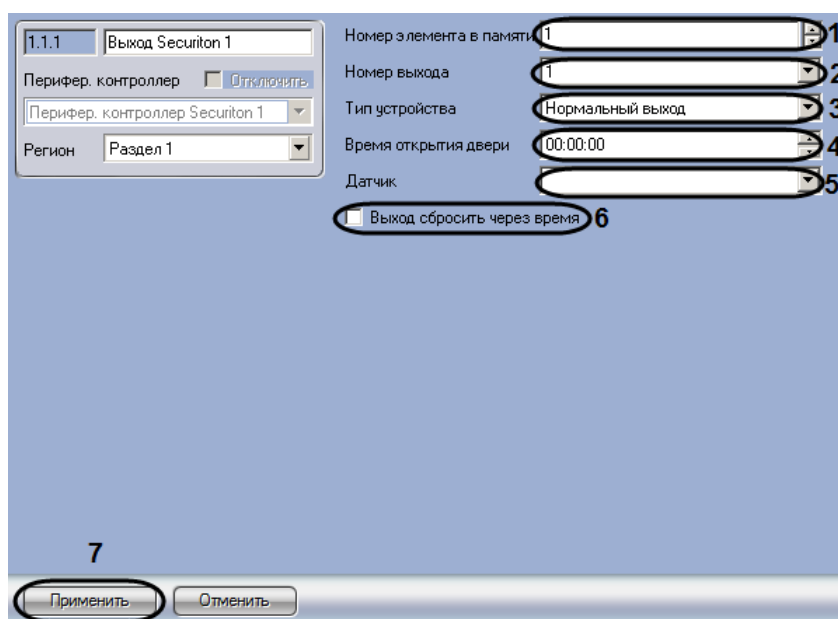


Рис. 3.4—5 Настройка выхода

2. Ввести в поле **Номер элемента в памяти** с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер выхода (см. Рис. 3.4—5, 1).
3. Из раскрывающегося списка **Номер выхода** выбрать номер выхода в устройстве (см. Рис. 3.4—5, 2).
4. Из раскрывающегося списка **Тип устройства** выбрать режим использования выхода (см. Рис. 3.4—5, 3).
5. В поле **Время открытия двери** ввести с помощью кнопок **вверх-вниз** и с помощью маски период времени в формате ЧЧ:ММ:СС, в течение которого выход будет оставаться активным (см. Рис. 3.4—5, 4). Данная настройка используется при активированном флажке **Выход сбросить через время** (см. шаг 7).
6. Из раскрывающегося списка **Датчик** выбрать датчик или список датчиков, который должен быть активирован при активации выхода (см. Рис. 3.4—5, 5).
7. В случае, если требуется сбрасывать выход через время, заданное параметром **Время открытия двери**, необходимо установить флажок **Выход сбросить через время** (см. Рис. 3.4—5, 6).
8. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—5, 7).

Настройка выхода завершена.

3.4.3 Настройка типа датчиков Securiton

Тип датчика задает виды сигналов, присылаемых датчиком при тревоге, задает тип физического подключения, время задержек на вход и выход и другие параметры.

В программном комплексе *Интеллект* настройка типа датчика осуществляется на панели настроек объекта **Тип датчиков Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—6).

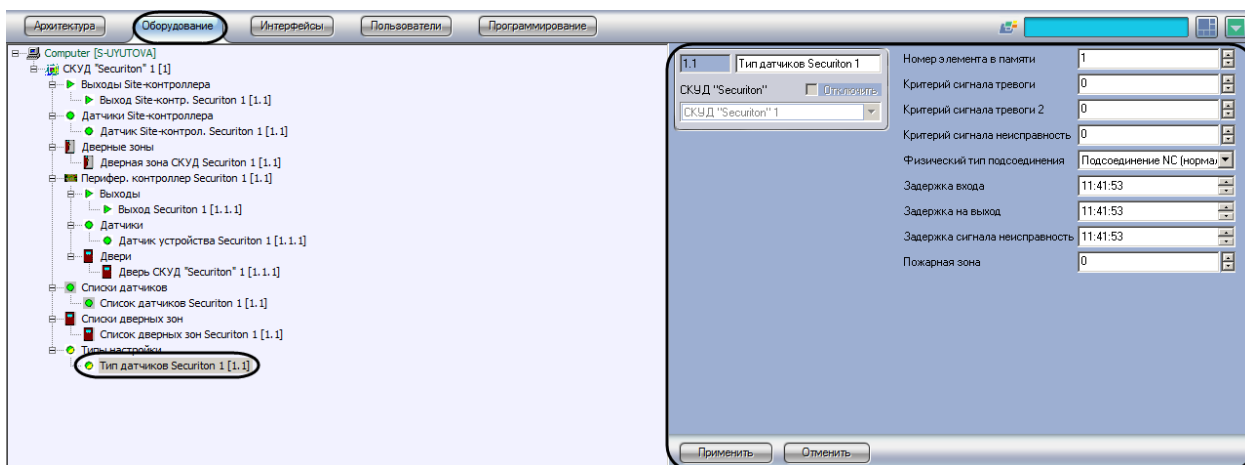


Рис. 3.4—6 Объект Тип датчика Securiton

Настройка типа датчиков производится в следующем порядке:

1. Перейти на панель настроек объект **Тип датчиков Securiton** (Рис. 3.4—7).

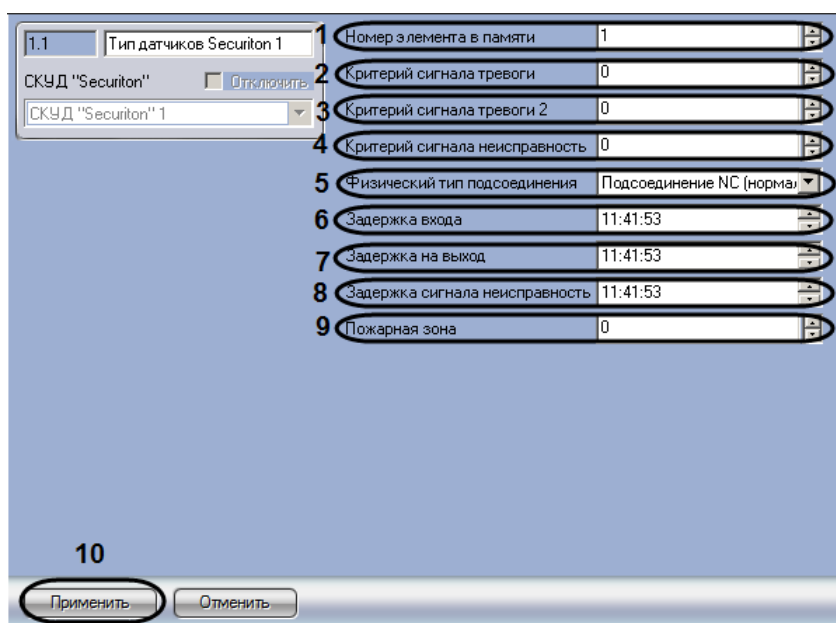


Рис. 3.4—7 Настройка типа датчиков Securiton

2. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер типа датчиков (см. Рис. 3.4—7, 1).
3. Ввести в поле **Критерий сигнала тревоги** с помощью кнопок **вверх-вниз** номер сообщения, посылаемого датчиком при активации шлейфа (см. Рис. 3.4—7, 2).
4. Ввести в поле **Критерий сигнала тревоги 2** с помощью кнопок **вверх-вниз** номер сообщения, посылаемого датчиком при активации второго датчика на шлейфе (см. Рис. 3.4—7, 3). Данная настройка используется при выбранном физическом типе подключения **Подсоединение 3 по 10k**.
5. Ввести в поле **Критерий сигнала неисправности** с помощью кнопок **вверх-вниз** номер сообщения, посылаемого датчиком при неисправности шлейфа (см. Рис. 3.4—7, 4). Данная настройка используется при типах подключения **Подсоединение 3 по 10k** и **Подсоединение 2 по 10k**.

6. Из раскрывающегося списка **Физический тип подсоединения** выбрать тип подключения датчиков (см. Рис. 3.4—7, 5, Таб. 3.4—1).

Таб. 3.4—1 Типы подсоединения датчиков

Тип подсоединения	Описание
Подсоединение NC (нормально закрыто)	Нормально замкнутый контакт
Подсоединение NO (нормально открыто)	Нормально разомкнутый контакт
Подсоединение 5.6к – норма – к.з. или обрыв - тревога	Оконечный резистор 5.6к, срабатывание происходит при обрыве или при замыкании линии связи.
Подсоединение 2 по 10к	10к-оконечный резистор и 10к-шунтирующий резистор. Линия имеет три состояния: Норма, Тревога и Неисправность (обрыв или КЗ).
Подсоединение 3 по 10к	Аналогично предыдущему. Система может различать, если подключены и сработали два датчика одновременно.
Напряжение сети	Напряжение сети
Напряжение на выходе	Напряжение на выходе
Подсоединение NC Геркон	Нормально замкнутый геркон
Тест аккумулятора	Тест аккумулятора

7. В поле **Задержка входа** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, по истечении которого после активизации датчика будет сформирован сигнал тревоги (см. Рис. 3.4—7, 6).
8. В поле **Задержка на выход** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, в течение которого после постановки на охрану датчика сигналы от него не будут восприниматься как тревога (см. Рис. 3.4—7, 7).
9. В поле **Задержка сигнала неисправность** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, на который допускается неисправность шлейфа датчика (см. Рис. 3.4—7, 8).
10. В поле **Пожарная зона** ввести с помощью кнопок **вверх-вниз** номер пожарной зоны, к которой принадлежит настраиваемый тип датчиков (см. Рис. 3.4—7, 9).
11. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—7, 10).

Настройка типа датчиков завершена.

3.4.4 Настройка датчика

В программном комплексе *Интеллект* настройка датчиков Site-контроллера и периферийного контроллера осуществляется идентично.

Настройка выхода Site-контроллера осуществляется на панели настроек объекта **Датчик Site-контроль. Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—8).

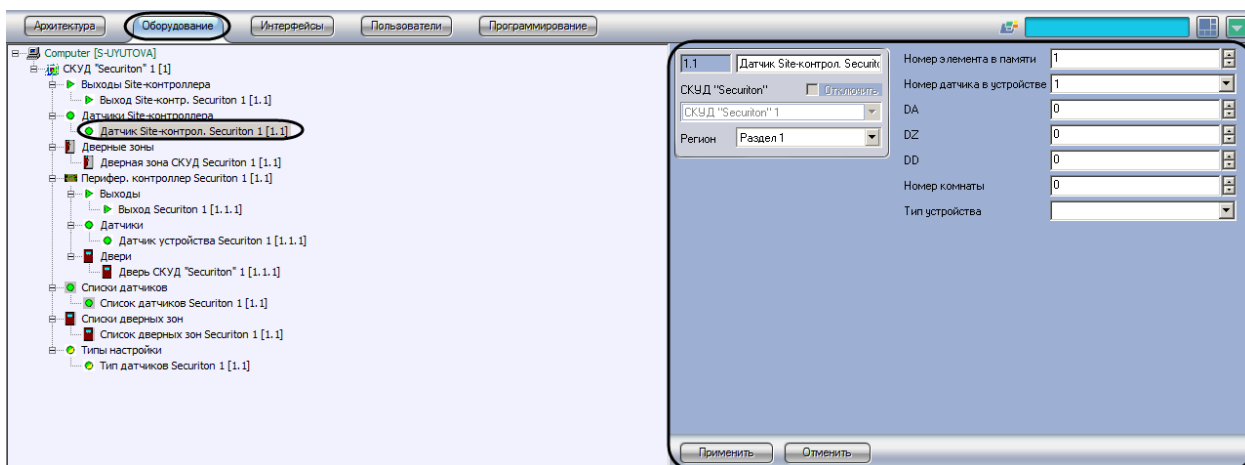


Рис. 3.4—8 Объект Датчик Site-контроль Securiton

Настройка выхода периферийного контроллера осуществляется на панели настроек объекта **Датчик устройства Securiton**. Данный объект создается на базе объекта **Периферийн. контроллер Securiton** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—9Рис. 3.4—4).

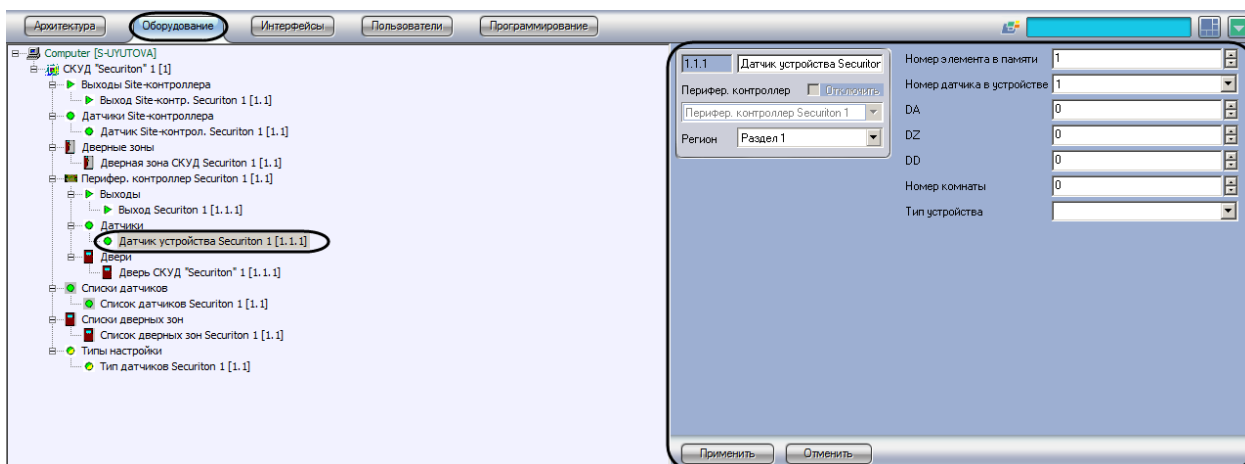


Рис. 3.4—9 Объект Датчик устройства Securiton

Настройка датчика осуществляется следующим образом:

1. Перейти на панель настроек объекта, соответствующего требуемому датчику (Рис. 3.4—10).

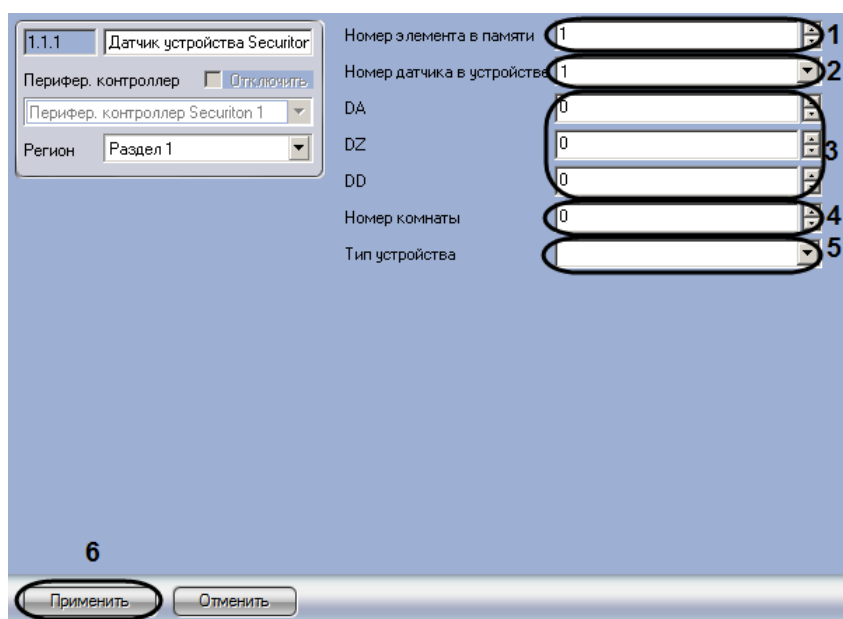


Рис. 3.4—10 Настройка датчика

2. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер датчика (см. Рис. 3.4—10, 1).
3. Из раскрывающегося списка **Номер датчика в устройстве** выбрать номер датчика (см. Рис. 3.4—10, 2). Данное значение не используется в случае, если объект соответствует датчику Securipro.
4. Указать адрес датчика Securipro, представляемый в формате 0x00DADZDD, где DA, DZ, DD – шестнадцатеричные числа (см. Рис. 3.4—10, 3). В поля **DA**, **DZ**, **DD** данные числа необходимо вводить в десятичной системе счисления.
5. В поле **Номер комнаты** ввести с помощью кнопок **вверх-вниз** номер комнаты, в которой расположен датчик (см. Рис. 3.4—10, 4). Данное значение используется для быстрого поиска датчика.
6. Из раскрывающегося списка **Тип устройства** выбрать объект **Тип датчиков Securiton**, соответствующий требуемому типу настройки датчика (см. Рис. 3.4—10, 5).
7. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—10, 6).

Настройка датчика завершена.

3.4.5 Настройка дверной зоны Securiton

В ПК *Интеллект* настройка дверной зоны осуществляется на панели настроек объекта **Дверная зона СКУД Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—11).

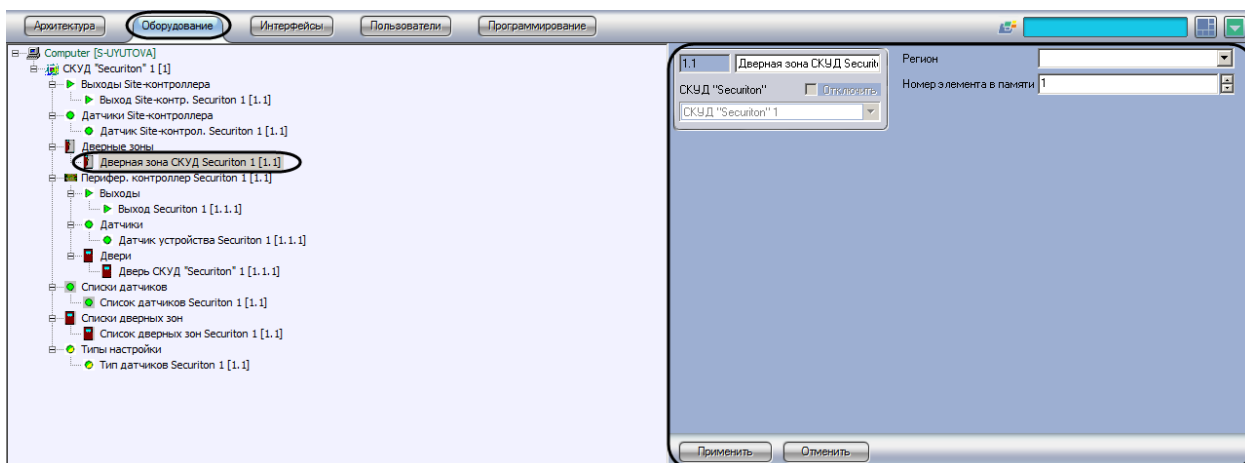


Рис. 3.4—11 Объект Дверная зона СКУД Securiton

Настройка дверной зоны осуществляется следующим образом:

1. Перейти на панель настроек объекта **Дверная зона СКУД Securiton** (Рис. 3.4—12).

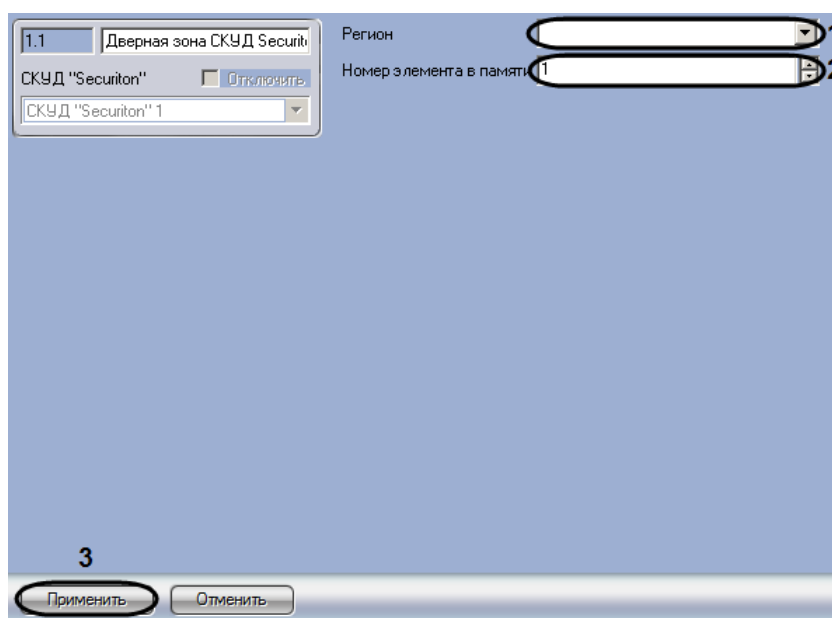


Рис. 3.4—12 Настройка дверной зоны

2. Из раскрывающегося списка **Регион** выбрать объект **Регион**, соответствующий настраиваемой дверной зоне (см. Рис. 3.4—12, 1). В ПК *Интеллект* объекты **Раздел** создаются на вкладке **Программирование** диалогового окна **Настройка системы** на базе объекта **Область**.
3. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер дверной зоны (см. Рис. 3.4—12, 2).
4. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—12, 3).

Настройка дверной зоны завершена.

3.4.6 Настройка двери

В программном комплексе *Интеллект* настройка двери Securiton осуществляется на панели настроек объекта **Дверь СКУД "Securiton"**. Данный объект создается на базе объекта **Перифер**.

контроллер Securiton на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—13).

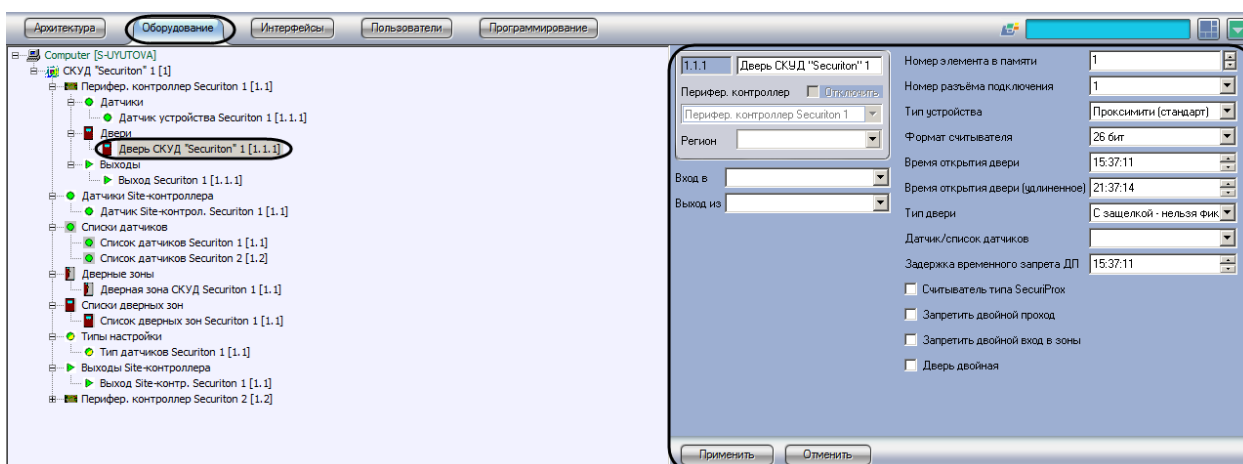


Рис. 3.4—13 Объект Дверь СКУД "Securiton"

Настройка двери Securiton осуществляется в следующем порядке:

1. Перейти на панель настроек объекта **Дверь СКУД "Securiton"** (Рис. 3.4—14).

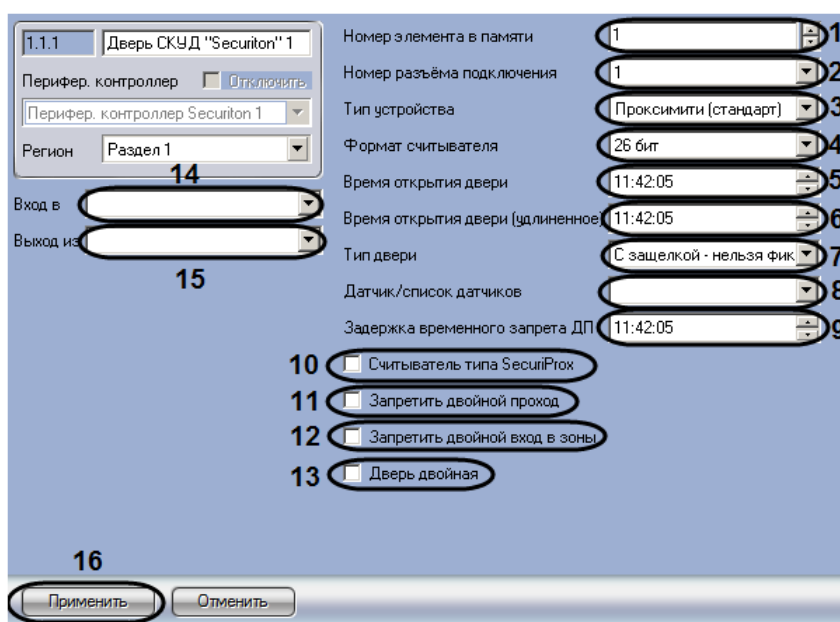


Рис. 3.4—14 Настройка двери Securiton

2. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер двери (см. Рис. 3.4—14, 1).
3. Из раскрывающегося списка **Номер разъема подключения** выбрать номер двери в устройстве (см. Рис. 3.4—14, 2).
4. Из раскрывающегося списка **Тип устройства** выбрать тип подключенного к контроллеру считывателя (см. Рис. 3.4—14, 3, Таб. 3.4—2).

Таб. 3.4—2 Описание типов двери

Тип устройства	Описание
Проксимити (стандарт)	Обычный считыватель проксимити-карт
Прокс. и постановка на охрану	Считыватель проксимити карт с функцией установки на охрану. При

Тип устройства	Описание
	активизации карты происходит открытие двери, и выдача команды постановки на охрану датчика. Номер датчика должен быть прописан в поле Датчик/список датчиков , а так же он должен быть прописан в аналогичном поле описания пользователя.
Прокс. и снятие с охраны	Считыватель проксимити карт с функцией снятия с охраны. При активизации карты происходит открытие двери и выдача команды установку на охрану датчика. Номер датчика должен быть прописан в поле Датчик/список датчиков , а так же в аналогичном поле описания пользователя.
Arming station +простой	Проксимити считыватель с двумя кнопками: Поставить и Снять с охраны. При поднесении карты без нажатия кнопок происходит просто открытие двери. Если же предварительно была нажата кнопка, происходит выдача команды на установку или снятия с охраны. Зона охраны берется как совпадение первой зоны из полномочий пользователя совпавшей с любой зоной из полномочий считывателя.
Arming station тип 1	Считыватель с кодоборником. Может использоваться для авторизации, как при помощи карты, так и непосредственно кодом (для этого надо набрать персональный номер сотрудника по базе и персональный код). После авторизации необходимо ввести короткий номер помещения и нажать 1 для снятия с охраны, 2 для постановки помещения на охрану. Система, проверив уровень доступа (пользователь должен иметь право производить операции с данным объектом, а считыватель должен иметь право управлять этим объектом) выдаст подтверждающий сигнал - отчет об операции.
Arming station тип 2	Аналогично Arming Station + простой за единственным исключением: операция выполняется по всем зонам охраны, которые имеет право ставить (снимать) пользователь и считыватель одновременно.
Arming station тип 3	Для использования совместно с двухдверным контроллером CP02.01. В этом случае Функции встроенного считывателя определяются пользовательским меню, назначенным на пользователя.
Снятие с охраны со счетчиком	Считыватель работает в паре, должен быть подключен на первый или третий разъем контроллера. Система автоматически считает количество входов и выходов. Если заходит первый пользователь, то помещение снимается с охраны.
Постановка на охрану со счетчиком	Считыватель, работающий в паре с предыдущим. Должен быть подключен на второй или четвертый разъем. Если выходит последний пользователь, то происходит автоматическая установка на охрану помещения.
Гостиничный счит. 1	Считыватель с держателем карты. Когда карта кладется в карман считывателя, происходит выдача команды на снятие датчика с охраны, а так же активизация дополнительного выхода (для управления освещением). Когда карта забирается, активизируется задержка на выход (со звуковым сигналом), по истечении которой отключается свет и помещение устанавливается на охрану. Также при вынимании карты из кармана считывателя открывается дверь и активизируется звуковой сигнал.
Гостиничный счит. 2	Аналогично предыдущему, но без звукового сигнала на вход.
Гостиничный счит. 3	Зарезервировано (не используется)
2 карты (подтверждение в теч. 10 сек)	Для авторизации необходимо в течение 10 сек после поднесения первой карты доступа поднести вторую карту.
2 карты (мастер карта в 10 сек)	Для авторизации необходимо в течение 10 сек после первой карты доступа поднести вторую карту, имеющую пометку Мастер .
Код + Карта версия 1	Считыватель с кодоборником. Для авторизации доступа необходимо сначала ввести код, после чего поднести карту доступа к считывателю.
Код + Карта версия 2	Считыватель с кодоборником. Для авторизации доступа необходимо сначала ввести код, после чего поднести карту доступа к считывателю.
Код + Карта версия 3	Считыватель с кодоборником. Для авторизации доступа необходимо сначала ввести код, после чего поднести карту доступа к считывателю.
Код + Карта версия 4	Считыватель с кодоборником. Для авторизации доступа необходимо сначала ввести код, после чего поднести карту доступа к считывателю.

5. Из раскрывающегося списка **Формат считывателя** выбрать тип используемых карт доступа (см. Рис. 3.4—14, 4).

6. В поле **Время открытия двери** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, в течение которого дверь будет оставаться открытой (см. Рис. 3.4—14, 5).
7. В поле **Время открытия двери (удлиненное)** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, в течение которого дверь будет оставаться открытой, если пользователь, открывший ее, имеет статус **С ограниченными возможностями** (см. Рис. 3.4—14, 6).
8. Из раскрывающегося списка **Тип двери** выбрать действие, которое требуется выполнить с дверью при обнаружении пожара (см. Рис. 3.4—14, 7). В случае, если используется дверь с защелкой (выбрано значение **С защелкой – нельзя фиксировать**), команды открыть и зафиксировать будут игнорированы. Дверь будет открыта только на время **Время открытия двери**.
9. Из раскрывающегося списка **Датчик/список датчиков** выбрать датчик или список датчиков для постановки или снятия с охраны при использовании некоторых типов считывателей (см. Рис. 3.4—14, 8, см. шаг 4).
10. В поле **Задержка временного запрета ДП** ввести с помощью кнопок **вверх-вниз** и при помощи маски период времени в формате ЧЧ:ММ:СС, по истечении которого сбрасываются данные для контроля двойного прохода (см. Рис. 3.4—14, 9).
11. В случае, если используется считыватель SecuriProx, установить флажок **Считыватель типа SecuriProx** (см. Рис. 3.4—14, 10).
12. В случае, если требуется активировать режим контроля двойного прохода, необходимо установить флажок **Запретить двойной проход** (см. Рис. 3.4—14, 11). В случае, если режим контроля двойного прохода должен быть отключен, необходимо снять данный флажок.
13. В случае, если требуется включить режим зонального контроля двойного прохода, необходимо установить флажок **Запретить двойной проход в зоны** (см. Рис. 3.4—14, 12). В случае, если режим зонального контроля двойного прохода должен быть отключен, необходимо снять данный флажок.
14. В случае, если к контроллеру подключена двойная дверь, необходимо установить флажок **Двойная дверь** (см. Рис. 3.4—14, 13).
15. Из раскрывающегося списка **Вход в** выбрать объект **Дверная зона СКУД Securiton**, соответствующий территории, расположенной со стороны выхода через данную дверь (см. Рис. 3.4—14, 14).
16. Из раскрывающегося списка **Выход из** выбрать объект **Дверная зона СКУД Securiton**, соответствующий территории, расположенной со стороны входа в данную дверь (см. Рис. 3.4—14, 15).

*Примечание. В случае, если дерево объектов настраивается вручную, объекты **Дверная зона СКУД Securiton** создаются и настраиваются также вручную. В случае, если производится автоматическое построение дерева объектов, дверные зоны назначаются дверям автоматически в соответствии с настройками устройства.*

17. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—14, 16).

Настройка двери *Securiton* завершена.

3.4.7 Настройка списка датчиков Securiton

Списки датчиков используются для выполнения групповых операций, например для одновременной постановки или снятия с охраны нескольких датчиков. В список могут быть включены датчики либо списки датчиков.

В программном комплексе *Интеллект* настройка списка датчиков осуществляется на панели настроек объекта **Список датчиков Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—15).

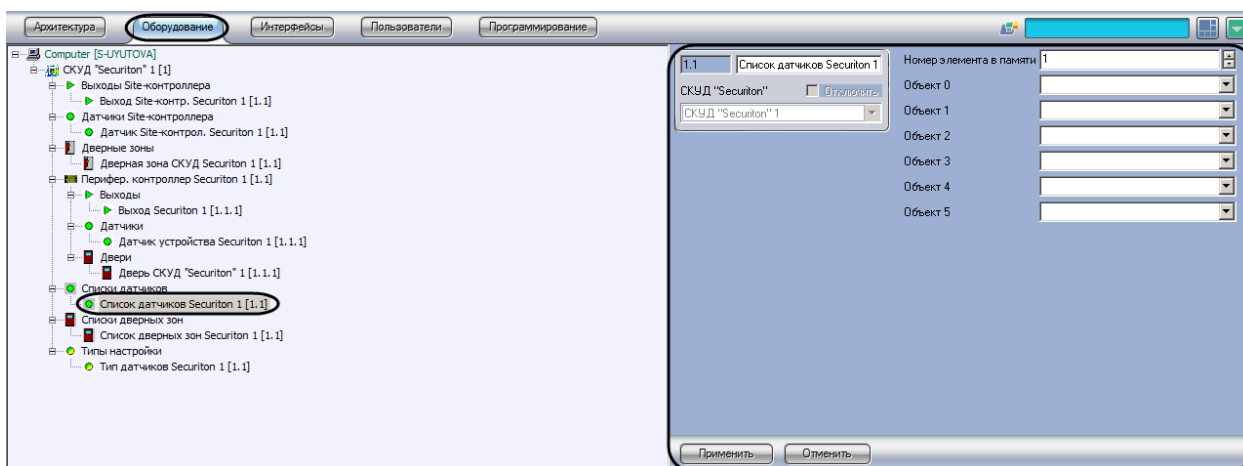


Рис. 3.4—15 Объект Список датчиков Securiton

Настройка списка датчиков производится в следующем порядке:

1. Перейти на панель настроек объекта **Список датчиков Securiton** (Рис. 3.4—16).

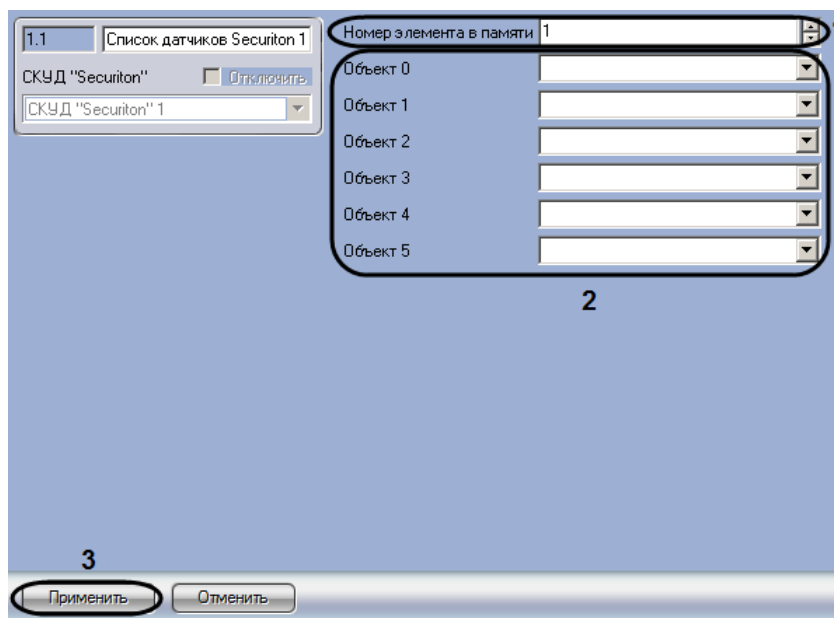


Рис. 3.4—16 Настройка списка датчиков

2. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер списка датчиков (см. Рис. 3.4—16, 1).
3. Из раскрывающихся списков **Объект 0 – Объект 5** выбрать объекты, соответствующие датчикам или спискам датчиков, которые должны быть включены в список (см. Рис. 3.4—16, 2).

4. Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—16, 3).

Настройка списка датчиков завершена.

3.4.8 Настройка списка дверных зон

Списки дверных зон используются для того, чтобы назначать полномочия на доступ к группе зон.

В программном комплексе *Интеллект* настройка списка дверных зон осуществляется на панели настроек объекта **Список дверных зон Securiton**. Данный объект создается на базе объекта **СКУД "Securiton"** на вкладке **Оборудование** диалогового окна **Настройка системы** (Рис. 3.4—17).

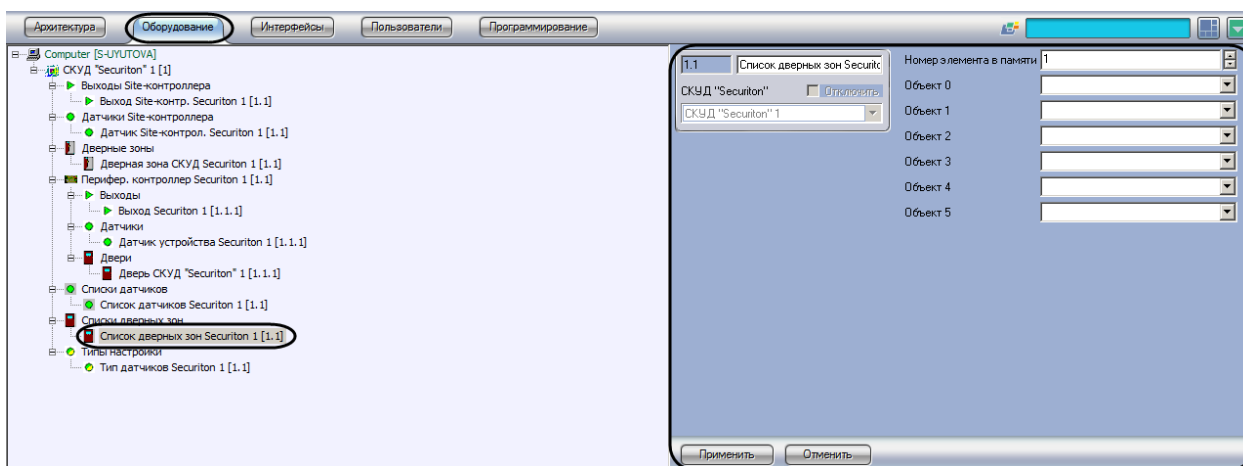


Рис. 3.4—17 Объект Список дверных зон Securiton

Настройка списка дверных зон производится следующим образом:

1. Перейти на панель настроек объекта **Список дверных зон Securiton** (Рис. 3.4—18).

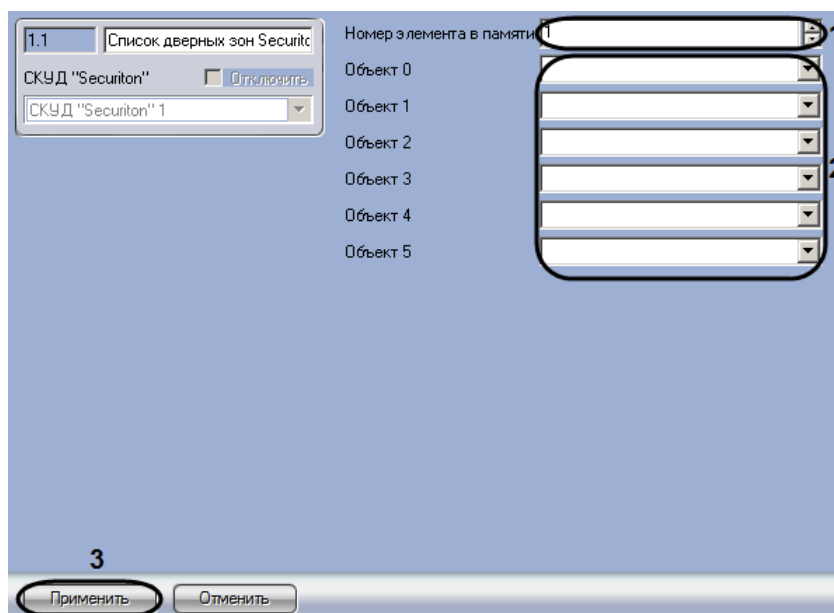


Рис. 3.4—18 Настройка списка дверных зон

2. В поле **Номер элемента в памяти** ввести с помощью кнопок **вверх-вниз** уникальный среди объектов данного типа номер списка дверных зон (см. Рис. 3.4—18, 1).

- Из раскрывающихся списков **Объект 0 – Объект 5** выбрать объекты, соответствующие дверным зонам или спискам дверных зон, которые должны быть включены в список (см. Рис. 3.4—18, 2).
- Для сохранения настроек в ПК *Интеллект* нажать на кнопку **Применить** (см. Рис. 3.4—18, 3).

Настройка списка дверных зон завершена.

3.5 Пересылка конфигурации в Site-контроллер Securiton

Пересылка конфигурации в Site-контроллер Securiton осуществляется следующим образом:

- Перейти на панель настроек объекта **СКУД “Securiton”** (Рис. 3.5—1).

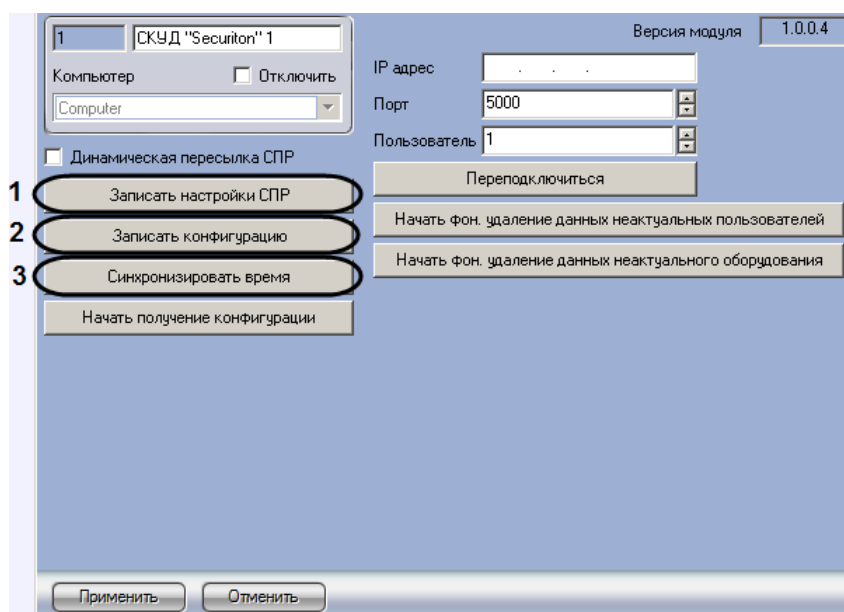


Рис. 3.5—1 Пересылка конфигурации в Site-контроллер Securiton

- Для записи в контроллер конфигурации модуля *Служба пропускного режима* нажать на кнопку **Записать настройки СПР** (см. Рис. 3.5—1, 1). При этом в контроллер будут переданы пользователи, уровни доступа, временные зоны и праздники.

Примечание 1. Для полной перезаписи настроек СПР необходимо выполнять и запись конфигурации СПР, и очистку пользователей (см. раздел Удаление неактуальных пользователей).

Примечание 2. В случае, если после пересылки в контроллер конфигурации СПР некорректно работают праздники или временные зоны, необходимо произвести синхронизацию времени (см. шаг 3).

- Для записи в контроллер конфигурации оборудования нажать на кнопку **Записать конфигурацию** (см. Рис. 3.5—1, 2).

Примечание. При пересылке конфигурации производится запись в контроллер изменений конфигурации, но не производится удаление оборудования. Для полной перезаписи конфигурации оборудования необходимо выполнять и запись конфигурации, и очистку (см. раздел Удаление неактуального оборудования).

4. Для пересылки в контроллер времени Сервера нажать на кнопку **Синхронизировать время** (см. Рис. 3.5—1, 3).

Пересылка конфигурации в Site-контроллер Securiton завершена.

3.6 Настройка динамической пересылки данных СПР

Для включения динамической пересылки данных СПР необходимо выполнить следующие действия:

1. Перейти на панель настроек объекта **СКУД "Securiton"** (Рис. 3.6—1).

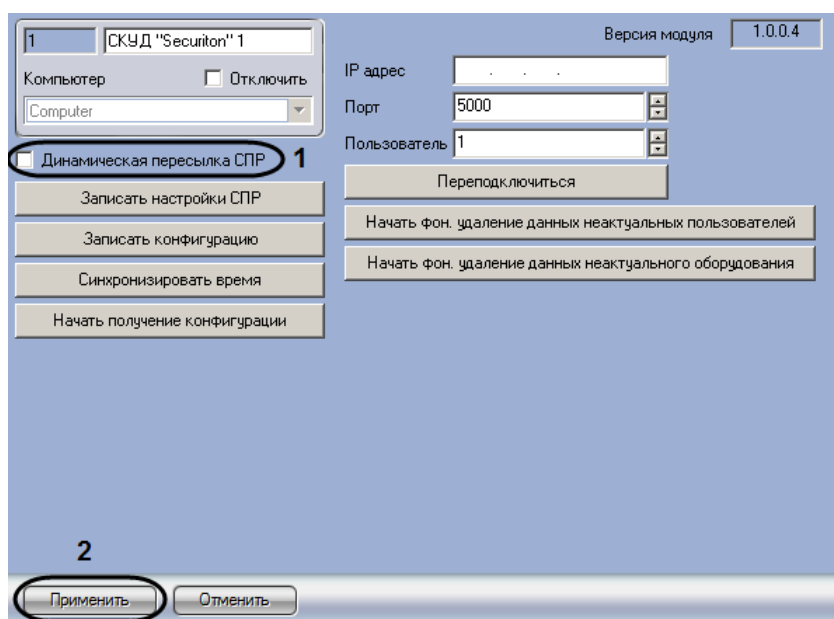


Рис. 3.6—1 Настройка динамической пересылки данных СПР

2. Установить флажок **Динамическая пересылка СПР** (см. Рис. 3.6—1, 1). При изменении конфигурации ПК *Интеллект* посредством модуля *Служба пропускного режима* внесенные изменения будут автоматически пересылаться в контроллер. В случае, если автоматическая пересылка изменений не требуется, необходимо снять данный флажок.
3. Нажать на кнопку **Применить** (см. Рис. 3.6—1, 2).

Включение динамической пересылки данных СПР завершено.

3.7 Удаление неактуальных пользователей

В ПК *Интеллект* имеется возможность удалять из памяти Site-контроллера тех пользователей, которых нет в СПР, при этом проверка их данных (номеров карт и уровней доступа) на корректность не производится.

Примечание. Для полной перезаписи настроек СПР необходимо выполнять и запись СПР, и очистку пользователей.

Для удаления неактуальных пользователей из Site-контроллера необходимо выполнить следующие действия:

1. Перейти на панель настроек объекта **СКУД "Securiton"** (Рис. 3.7—1).

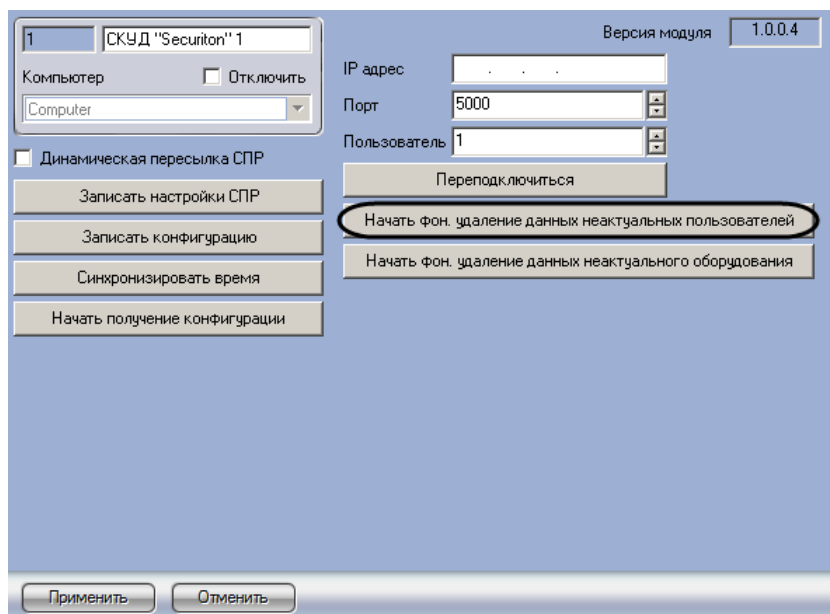


Рис. 3.7—1 Удаление неактуальных пользователей

2. Нажать на кнопку **Начать фон. удаление данных неактуальных пользователей** (Рис. 3.7—1).

Удаление неактуальных пользователей завершено.

3.8 Удаление неактуального оборудования

В ПК *Интеллект* имеется возможность удалять из памяти Site-контроллера **Оборудование**, отсутствующее в дереве объектов ПК *Интеллект*.

Примечание. Для полной перезаписи конфигурации оборудования необходимо выполнять и запись конфигурации, и очистку.

Для удаления неактуального оборудования из Site-контроллера необходимо выполнить следующие действия:

1. Перейти на панель настроек объекта **СКУД "Securiton"** (Рис. 3.7—1).

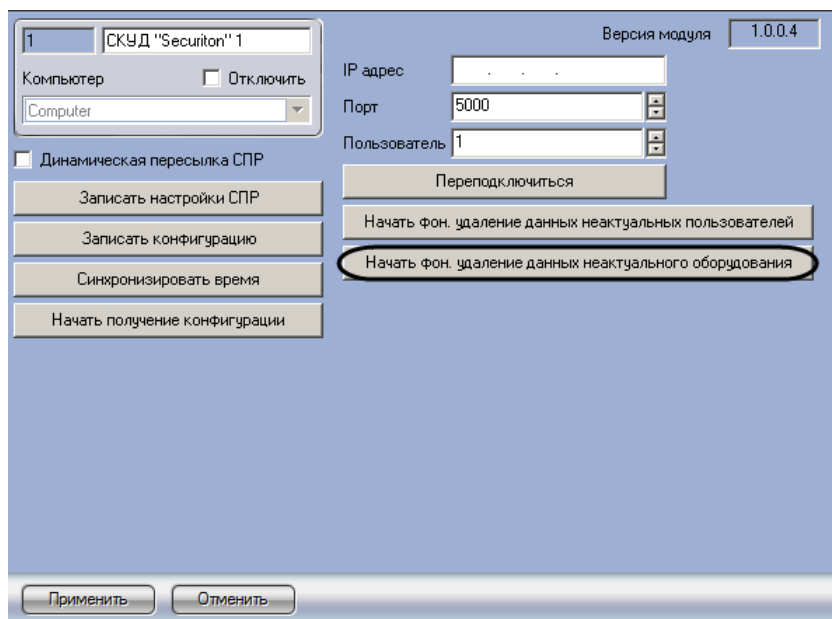


Рис. 3.8—1 Удаление неактуального оборудования

2. Нажать на кнопку **Начать фон. удаление данных неактуального оборудования** (Рис. 3.7—1).

Удаление неактуального оборудования завершено.

3.9 Переподключение к Site-контроллеру

При переподключении соединение с контроллером разрывается и устанавливается заново.

Для переподключения к Site-контроллеру необходимо выполнить следующие действия:

1. Перейти на панель настроек объекта **СКУД "Securiton"** (Рис. 3.9—1).

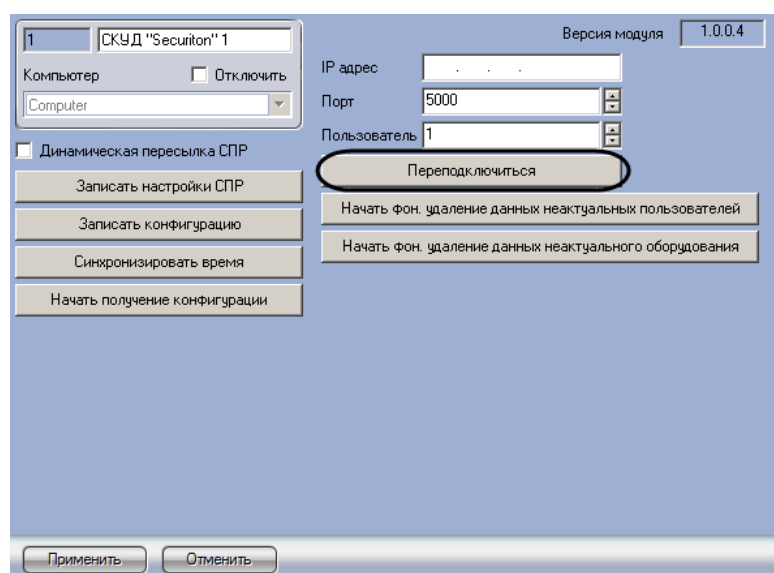


Рис. 3.9—1 Переподключение в Site-контроллеру

2. Нажать на кнопку **Переподключиться** (см. Рис. 3.9—1).

Переподключение к Site-контроллеру завершено.

4 Работа с модулем интеграции «Securiton»

4.1 Общие сведения о работе с модулем интеграции «Securiton»

Для работы с модулем Securiton используются следующие интерфейсные объекты:

1. **Карта;**
2. **Протокол событий.**

Сведения по настройке данных интерфейсных объектов приведены в документе *Программный комплекс Интеллект: Руководство Администратора*.

Работа с интерфейсными объектами подробно описана в документе *Программный комплекс Интеллект: Руководство Оператора*.

4.2 Управление выходом

Управление выходом осуществляется в интерактивном окне **Карта** с использованием функционального меню объектов **Выход Site-контр. Securiton** и **Выход Securiton** (Рис. 4.2—1, Таб. 4.2-1).

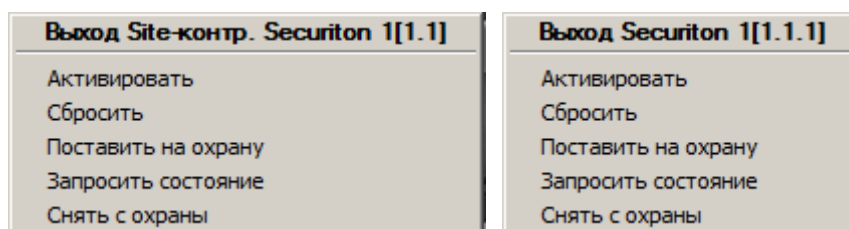


Рис. 4.2—1. Функциональное меню объектов **Выход Site-контр. Securiton** и **Выход Securiton**

Таб. 4.2-1. Описание команд функционального меню объекта **Выход Site-контр. Securiton** и **Выход Securiton**

Команда функционального меню	Выполняемая функция
Активировать	Активировать выход
Сбросить	Сбросить выход
Поставить на охрану	Поставить выход на охрану
Запросить состояние	Запросить состояние выхода
Снять с охраны	Снять выход с охраны

4.3 Управление датчиком

Управление датчиком осуществляется в интерактивном окне **Карта** с использованием функционального меню объектов **Датчик Site-контроль. Securiton** и **Датчик устройства Securiton** (Рис. 4.3—1, Таб. 4.3-1).

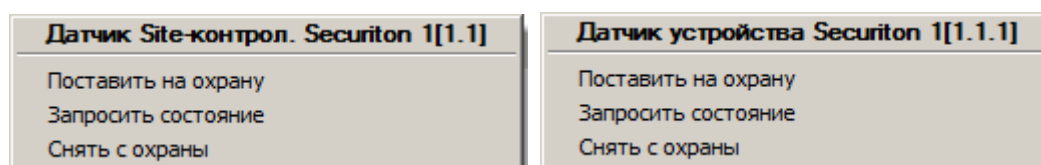


Рис. 4.3—1 Функциональное меню объектов **Датчик Site-контроль. Securiton** и **Датчик устройства Securiton**

Таб. 4.3-1. Описание команд функционального меню объекта **Датчик Site-контроль. Securiton** и **Датчик устройства Securiton**

Команда функционального меню	Выполняемая функция
Поставить на охрану	Поставить датчик на охрану
Запросить состояние	Запросить состояние датчика

Команда функционального меню	Выполняемая функция
Снять с охраны	Снять датчик с охраны

4.4 Управление дверью Securiton

Управление дверью осуществляется в интерактивном окне **Карта** с использованием функционального меню объекта **Дверь СКУД "Securiton"** (Рис. 4.4—1, Таб. 4.4-1).

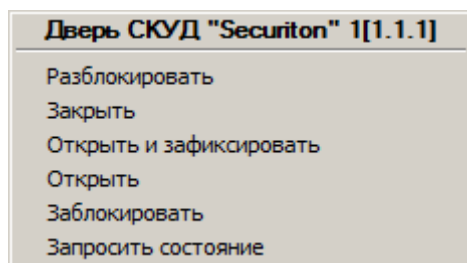


Рис. 4.4—1 Функциональное меню объекта Дверь СКУД "Securiton"

Таб. 4.4-1. Описание команд функционального меню объекта Дверь СКУД "Securiton"

Команда функционального меню	Выполняемая функция
Разблокировать	Разблокировать дверь
Закрыть	Закрыть дверь
Открыть и зафиксировать	Открыть дверь
Открыть	Открыть дверь на время открытия двери
Заблокировать	Заблокировать дверь
Запросить состояние	Запросить состояние двери