ИТРИУМ®

Программное обеспечение интегрированной системы безопасности ITRIUM®

Драйвер Bioscrypt

Руководство пользователя

Санкт-Петербург
2020

Содержание

1 Назначение Драйвера Bioscrypt

«Драйвер Bioscrypt» является частью ПО ITRIUM® и предназначен для интеграции считывателей биометрической информации в систему безопасности. Драйвер работает со считывателями следующих моделей: V-Flex, V-Prox, V-Pass, V-Smart компании BIOSCRYPT.

Использование «Драйвера Bioscrypt» предоставляет следующие возможности:

- Организация пропускного режима на основе считывателей биометрической информации (отпечатка пальца).
- Организация единой базы данных биометрических параметров пользователей в системе безопасности.
- Возможность ввода отпечатка пальца с выделенного считывателя в Бюро пропусков, сохранение его в базе данных ПО ITRIUM® (MSSQL, Oracle) и рассылка информации остальным считывателям, объединенным по интерфейсу RS-485.
- Возможность интегрировать считыватели биометрической информации с любыми контроллерами доступа, которые имеют интерфейс Wiegand (Рубеж-07, Рубеж-08, AAN-100, панели Parsec, Northern Computers и т.д.).
- Возможность работы в нескольких режимах – палец, несколько пальцев, карта + палец.

«Драйвер Bioscrypt» позволяет использовать следующие считыватели:

- **V-Prox** – считыватель объединяет в себе сканер отпечатков пальцев и считыватель HID - PROX-карты.
- **V-Flex** – отличием от предыдущей модели является отсутствие встроенного PROX-считывателя. V-Prox и V-Flex позволяют использовать любой внешний считыватель с Wiegand-интерфейсом.
- **V-Pass** – работает только как сканер отпечатка пальцев. Исключает возможность объединять идентификацию по сканеру со считывателем PROX-карт.
- **V-Smart** – также объединяет в себе дактилоскопический сканер отпечатка пальца и считыватель бесконтактной Smart-карты. Особенность данного считывателя в том, что шаблон отпечатка хранится в памяти Smart-карты.

2 Порядок подключения считывателей

Для того чтобы подключить считыватель в ПО ITRIUM®, выполните следующие шаги:

- Подключите считыватель Bioscrypt для ввода биометрии к компьютеру и к контроллеру доступа.
- Настройте и запустите Драйвер Bioscrypt.

- Настройте форму для ввода биометрии в «Программе оформления пропусков».
- Назначьте в «Программе оформления пропусков» считыватель Bioscrypt для ввода биометрии.
- Настройте уровень доступа Bioscrypt для считывателя Bioscrypt.

После настройки **Драйвера Bioscrypt** и настройки формы **Бюро пропусков** можно приступать к вводу отпечатка пальца и выдаче готовых пропусков.

3 Подключение считывателей Bioscrypt

Считыватели Bioscrypt подключаются к компьютеру тремя способами:

- Через порт RS-232 DB15.
- Через порт RS-485 DB15, последовательно можно подключить 31 считыватель. Для этого необходимо использовать преобразователь интерфейса RS-232 в интерфейс RS-485.
- Через порт RS-232 RJ11.

Кроме того, считыватель Bioscrypt может подключаться к контроллеру доступа посредством Wiegand-интерфейса. При таком подключении считыватель Bioscrypt будет работать как обычный считыватель, выдавая в контроллер доступа номер карты. В этом случае решение о разрешении или о запрете доступа будет производиться самим контроллером доступа. Для детального подключения считывателя Bioscrypt к контроллеру см. документацию по Bioscrypt.

4 Настройка и запуск драйвера

После подключения считывателя Bioscrypt к компьютеру необходимо добавить его в конфигурацию программы «Администратор системы» программного обеспечения ITRIUM®. Для этого необходимо:

1. В программе «Администратор системы», в дереве конфигурации кликнуть правой кнопкой мыши на название компьютера, на котором установлено ПО ITRIUM®, в контекстном меню выбрать пункт **Создать новый элемент**. В высветившемся окне **Добавить к "Компьютер"** из списка необходимо выбрать элемент **Драйвер Bioscrypt** и нажать кнопку **Принять**.
2. На элементе **Драйвер Bioscrypt** кликнуть правой кнопкой мыши, в контекстном меню выбрать пункт **Создать новый элемент**. В высветившемся окне **Последовательный порт Bioscrypt** необходимо нажать кнопку **Принять**.
3. В меню **Показать** выбрать пункт **Частные свойства**. В частных свойствах **Последовательный порт Bioscrypt** необходимо указать номер порта и скорость передачи данных.

У считывателей **V-Prox**, **V-Flex**, **V-Pass** выставляется скорость:

- 9600 – при подключении по интерфейсу RS-485 DB15 и RS-232 DB15,
- 57 600 – при подключении по интерфейсу RS-232 RJ11.

У считывателя **V-Smart** выставляется скорость 57 600. Допускается установка следующих скоростей:

- 57 600,
- 56 000,
- 38 400,
- 19 200,
- 9 600.

Другие свойства последовательного порта изменять не рекомендуется.

4. На элементе **Последовательный порт Bioscrypt** кликнуть правой кнопкой мыши, в контекстном меню выбрать пункт **Создать новый элемент**. В открывшемся окне **Свойства "Считыватель Bioscrypt"** нажмите на кнопку **Принять**.

5 Частные свойства считывателей

Элемент **Считыватель Bioscrypt** имеет четыре вкладки частных свойств:

- Инициализация Bioscrypt,
- Свойства Wiegand,
- Свойства биометрии,
- Свойства верификации.

5.1 Инициализация Bioscrypt

Вкладка **Инициализация Bioscrypt** представлена на рисунке 1.

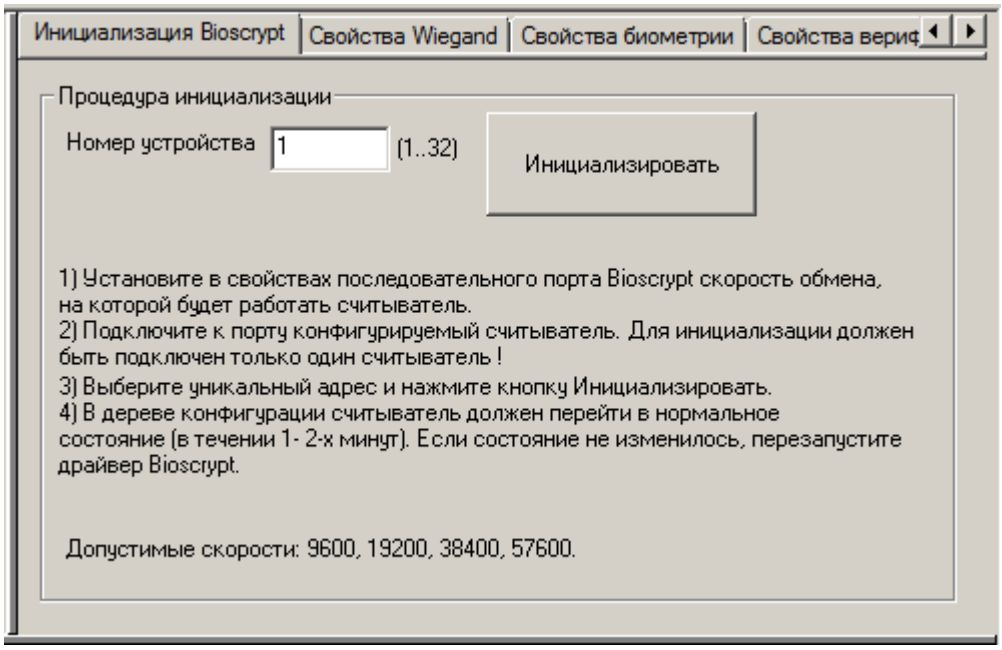

Рисунок 1 — Вкладка **Инициализация Bioscrypt**

Здесь устанавливается номер устройства (считывателя) и скорость обмена данными с компьютером. Эта закладка предназначена для инициализации устройств. Инициализация проходит только при непосредственном подключении к компьютеру. Через сеть (по интерфейсу RS-485) это сделать невозможно. Для подключения считывателя необходимо произвести следующие действия:

1. Подключить один считыватель к порту.
2. Выбрать уникальный адрес (номер устройства).
3. Нажать кнопку **Инициализировать**.
4. В конфигурации системы элемент **Считыватель** должен перейти в нормальное состояние (зеленый цвет иконки).

Внимание: при подключении нескольких считывателей необходимо учесть, что, после добавления элемента **Считыватель** к последовательному порту, его сначала инициализируют, а только затем подключают следующий считыватель.

5.2 Свойства Wiegand

Свойства Wiegand иллюстрирует вкладка на рисунке 2.

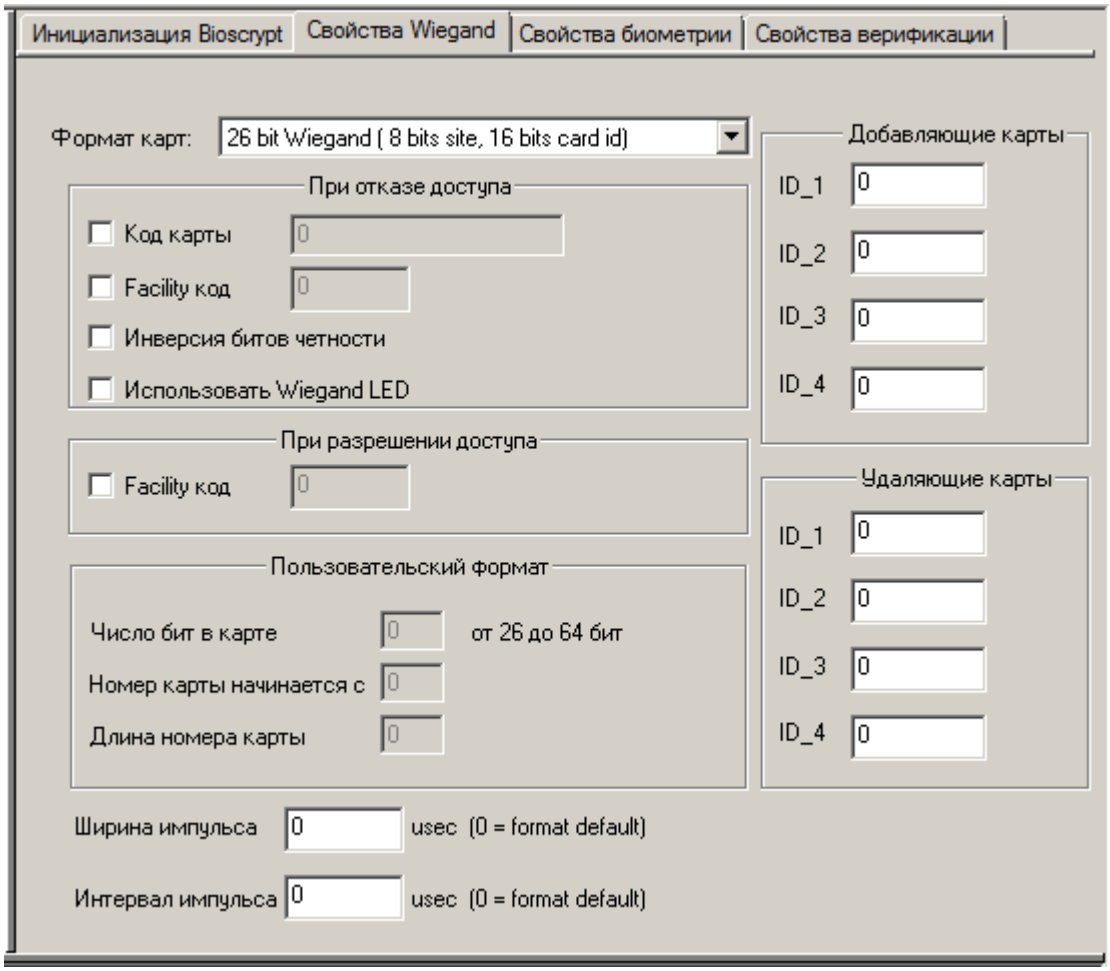

Рисунок 2 — Вкладка **Свойства Wiegand**

Данная вкладка используется для установки Wiegand-интерфейса.

1. В пункте **Формат карт** необходимо выбрать один из списка предопределенных форматов карты, если считыватель его использует.

2. Если в списке **Формат карт** выбрать **Определяемый пользователем**, то в поле **Пользовательский формат** станут активными следующие пункты:

   - **Число бит в карте** (может быть от 26 до 64),
   - **Номер карты начинается с** (указывается бит, с которого начинается номер карты),
   - **Длина номера карты** (указывается длина номера карты в битах).

3. При определении пользовательского формата карт необходимо отключить опции **При отказе доступа** и **При разрешении доступа**.

4. В поле **Добавляющие карты** необходимо указать номера карт, с помощью которых можно заносить данные. При поднесении такой карты считыватель переходит в режим добавления: записываются данные отпечатка пальца и данные карты-пропуска.

5. В поле **Удаляющие карты** необходимо указать номера карт, с помощью которых можно удалять данные. При поднесении такой карты считыватель переходит в режим удаления: удаляются данные отпечатка пальца и данные карты-пропуска.

6. В поле **При отказе доступа** необходимо указать: код карты, Facility код, инверсия битов четности и использование Wiegand LED.

7. В поле При разрешении доступа необходимо установить Facility код.

8. Ширина импульса по умолчанию установлена на ноль. Эту величину не рекомендуется менять.

9. Интервал импульса по умолчанию установлен на ноль. Эту величину не рекомендуется менять.

5.3 Свойства биометрии

Представление о биометрических свойствах дает рисунке 3.

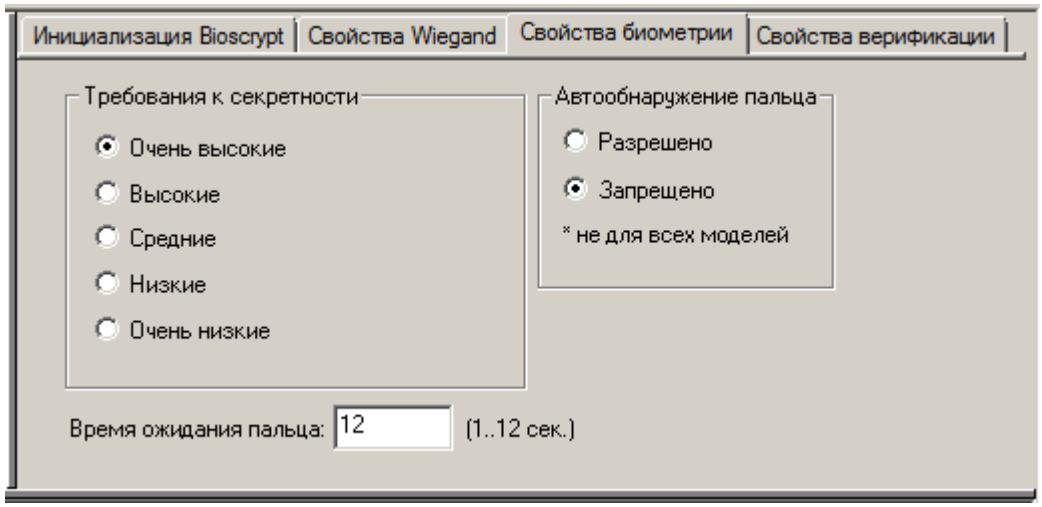

Рисунок 3 — Вкладка Свойства биометрии

На этой вкладке устанавливаются глобальные требования к секретности от **Очень низкие** до **Очень высокие**. Чем выше требования секретности, тем выше вероятность ложного отказа и ниже вероятность ложного пропуска. Данные по уровням секретности приведены в таблице 1.

Требования секретности	Ложный отказ	Ложный пропуск
Очень низкий	1 / 10,000	1 / 100
Низкий	1 / 5000	1 / 200

Требования секретности	Ложный отказ	Ложный пропуск
Средний	1 / 1000	1 / 1000
Высокий	1 / 200	1 / 5000
Очень высокий	1 / 100	1 / 20,000

Таблица 1 — Вероятности ложных отказов и пропусков по уровням секретности

В зависимости от типа считывателя идентификация может производиться по одному пальцу или по нескольким. Если выбрана идентификация по нескольким пальцам, то в поле **Время ожидания пальца** устанавливается время между предъявлениями. Функцию **Автообнаружение пальца** допускается включать не для всех типов считывателей (см. описание моделей V-серии).

5.4 Свойства верификации

Свойства верификации отображены на рисунке 4.

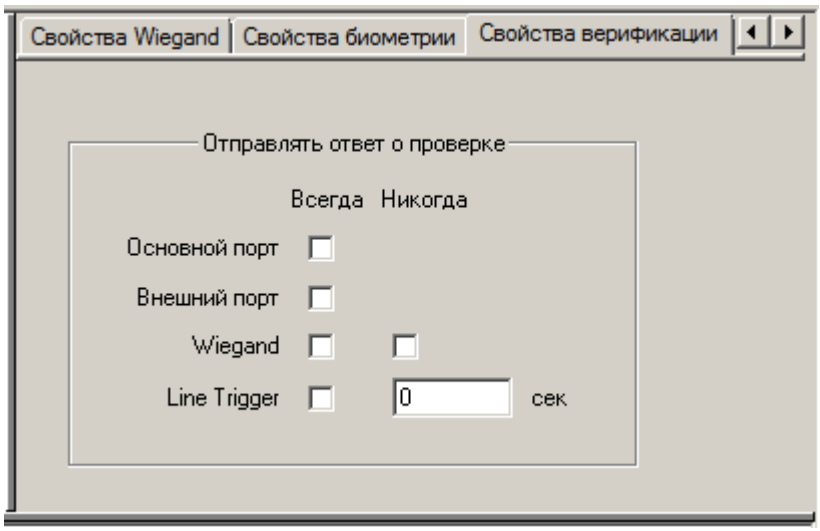

Рисунок 4 — Вкладка **Свойства верификации**

На этой вкладке задается способ отправки ответа о проверке. При нормальных условиях работы данные будут отправляться по тому каналу, по которому считыватель был инициализирован. Также можно выбрать дополнительный способ отправки ответа о проверке. Для этого:

1. Отметьте флаг **Основной порт** в столбце **Всегда** для постоянной отправки контрольных ответных пакетов на основной порт после завершения верификации.

2. Отметьте флаг **Внешний порт** в столбце **Всегда** для постоянной отправки контрольных пакетов на дополнительный внешний порт после завершения верификации.

3. Отметьте флаг **Wiegand** в столбце **Всегда** для постоянной отправки контрольных пакетов на Wiegand-порт после завершения верификации. Отметьте флаг в столбце **Никогда** для запрета использования данного порта при отправке контрольных пакетов.

4. Отметьте флаг **Line Trigger** для активации TTL-совместимых выходных сигналов на период, указанный в поле рядом.

5.5 Уровень доступа Bioscrypt

Для того чтобы добавить элемент **Уровень доступа Bioscrypt**, необходимо:

1. На элементе **Считыватель Bioscrypt** кликнуть правой кнопкой мыши, в контекстном меню выбрать пункт **Создать новый элемент**. В высветившемся окне **Свойства "Папка уровней доступа Bioscrypt"** необходимо нажать кнопку **Принять**. Этот элемент не имеет никаких свойств.

2. На элементе **Папка уровней доступа Bioscrypt** кликнуть правой кнопкой мыши, в контекстном меню выбрать пункт **Создать новый элемент**. В высветившемся окне **Свойства "Уровень доступа Bioscrypt"** необходимо нажать кнопку **Принять**.

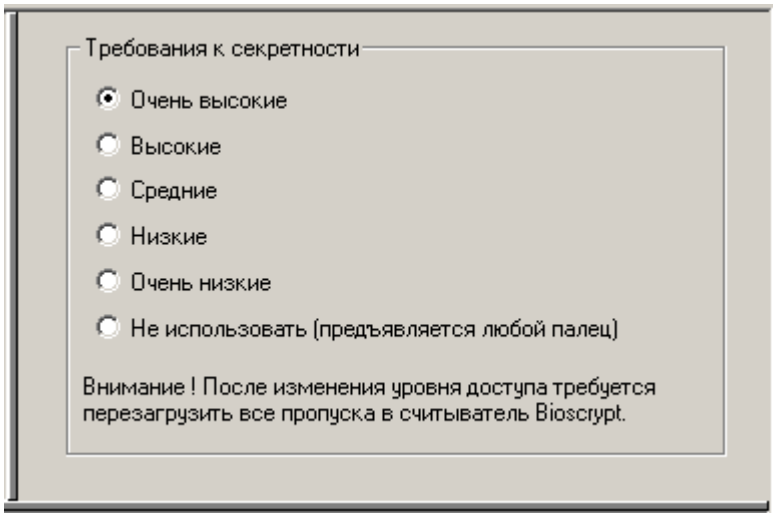

Рисунок 5 — Частные свойства элемента **Уровень доступа Bioscrypt**

3. На вкладке частных свойств элемента **Уровень доступа Bioscrypt** необходимо выставить локальные требования к секретности. Кроме свойств, описанных для считывателя Bioscrypt, здесь добавляется пункт **Не использовать**. В случае, когда выбран пункт **Не использовать**, можно предъявлять любой палец. Если требования секретности для уровня доступа и считывателя различаются, то выбирается низший из них.

После изменения требования к секретности необходимо перезагрузить все пропуска в считыватели Bioscrypt.

6 Настройка формы для ввода биометрии

Для настройки формы для ввода биометрии необходимо добавить окно **Биометрия** и назначить считыватель Bioscrypt в «Программе оформления пропусков».

Добавить окно **Биометрия** можно двумя способами:

1-й способ:

1. В программе «Администратор системы» в дереве элементов выберите папку **Доступ**.
2. В высветившемся справа от дерева конфигурации окне выберите вкладку **Форма**.
3. В окне **Форма** щелкните правой кнопкой мыши и выберите в контекстном меню пункт **Импорт из HTML**.

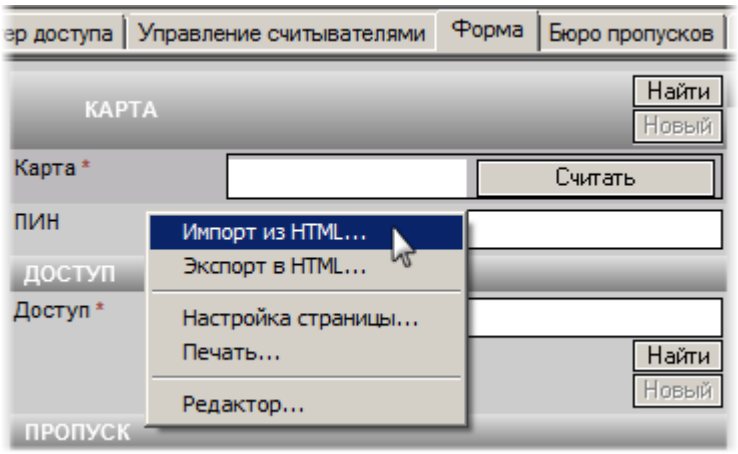

Рисунок 6 — Добавление окна **Биометрия** через **Импорт из HTML**

4. Далее откроется диалоговое окно выбора файлов, в котором нужно указать путь к файлу **C:/Program Files/Itrium/HTMLForms/input-biometric.htm**, выбрать файл из списка и нажать кнопку **Открыть**, после этого загрузится форма с элементом ввода биометрических данных, поставляемая с ПО ITRIUM®.

Рисунок 7 — Окно **Биометрия**

2-й способ:

1. Настроить считыватель для ввода биометрии в «Программе оформления пропусков» можно с помощью **Редактора форм**. Для этого необходимо в программе «Администратор системы» выбрать элемент **Доступ**.
2. На вкладке **Форма** необходимо кликнуть правой кнопкой мыши и выбрать в контекстном меню пункт **Редактор...**.

3. Установив курсор мыши в свободной области, необходимо выбрать пункт меню **Вставка** — **Дополнительно** — **Элемент ввода параметров биометрии (по отпечаткам пальцев)**.

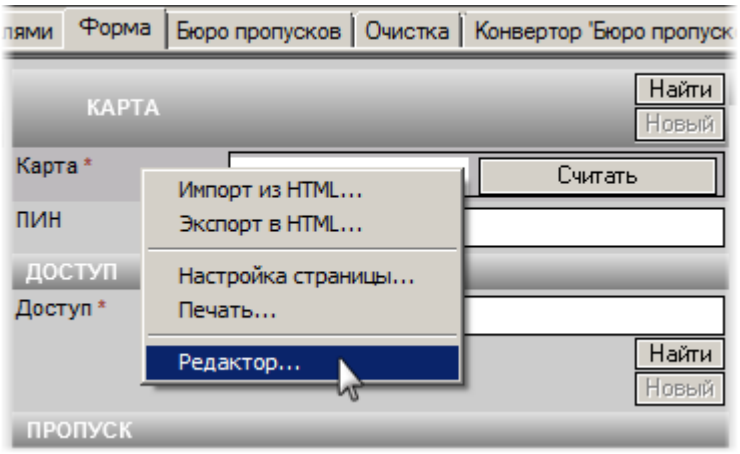

Рисунок 8 — Добавление окна **Биометрия** через **Редактор форм**

4. Отредактируйте размеры появившегося поля **ATL Composite Control**.

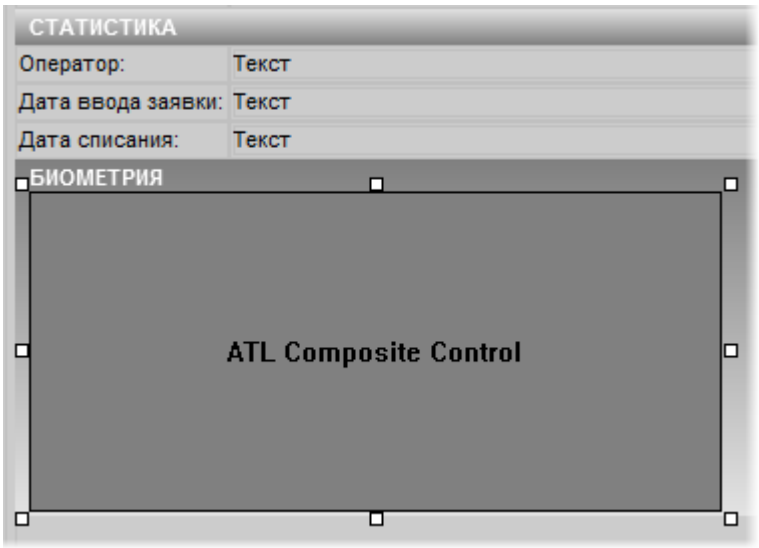

Рисунок 9 — Добавление окна **ATL Composite Control**

5. Нажмите кнопку **Сохранить**.

Внимание: данная форма пропусков будет у всех пропусков, для которых не определена никакая другая форма. Если надо сделать форму только для определенной папки пропусков, то необходимо в дереве конфигурации в папке **Доступ** выбрать необходимую папку пропусков, и в высветившемся справа от дерева конфигурации окне во вкладке форма добавить окно **Биометрия**. Нажать кнопку **Сохранить**.

6. В секции **Биометрическая информация** указаны две руки. Здесь определяется палец или пальцы, с которых будут считываться отпечатки.

7. В строке **Качество** указывается качество снятия отпечатка пальца.

8. В строке **Содержание** указывается величина, определяющая количество считываемых бороздок. Низкое содержание может привести к ложному срабатыванию (ложному пропуску).

9. Кнопка **Ввести биометрию** необходима для ввода отпечатка пальца в базу данных.

10. Кнопка **Дополнительно** имеет контекстное меню, состоящее из следующих пунктов: **Удалить**, **Удалить все**:

    - Команда **Удалить** означает удалить отпечаток из базы.
    - Команда **Удалить все** означает удалить все отпечатки.

7 Настройка считывателя Bioscrypt

Для того чтобы назначить **Считыватель Bioscrypt** в «Программе оформления пропусков», необходимо:

1. В дереве конфигурации выберите элемент **Программа оформления пропусков**.

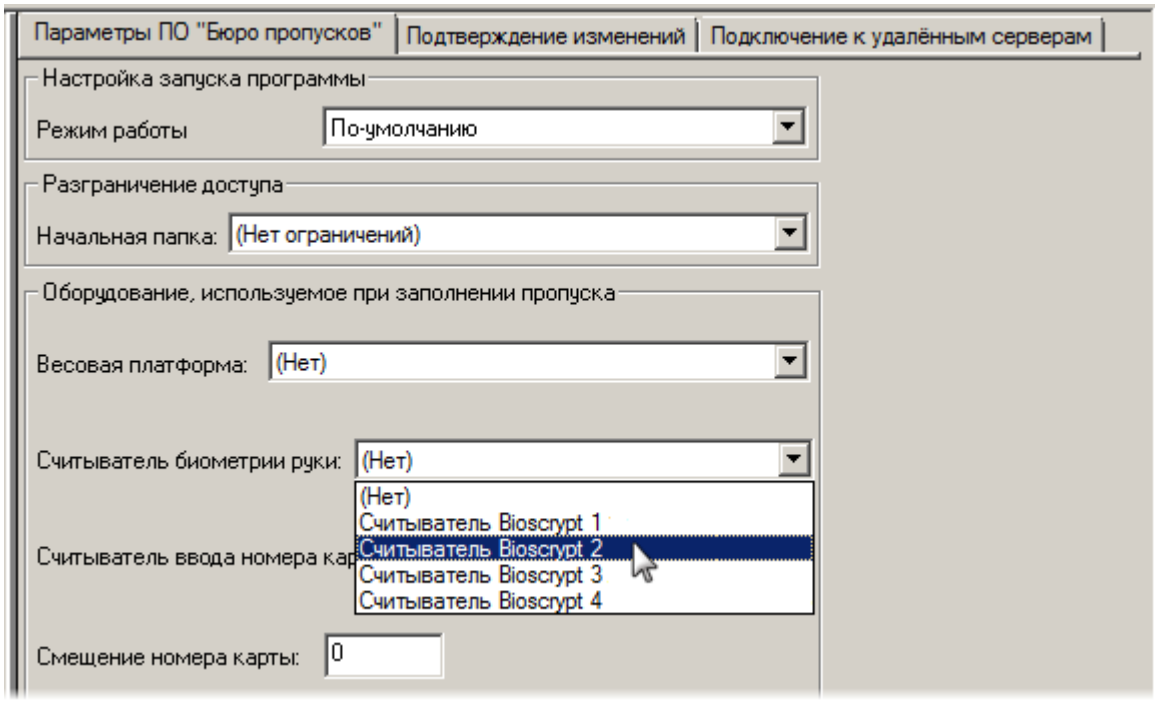

Рисунок 10 — Добавление считывателя Bioscrypt в **Бюро пропусков**

2. На вкладке **Параметры ПО "Бюро пропусков"**, в списке **Считыватель биометрии руки** выберите необходимый считыватель Bioscrypt.

3. Нажмите кнопку **Сохранить**.

4. После добавления **Считывателя биометрии руки** перезапустите «Программу оформления пропусков».

8 Настройка уровня доступа Bioscrypt

Для того чтобы создать **Уровень доступа Bioscrypt**, необходимо:

1. В программе «Администратор системы» в дереве конфигурации в папке **Доступ** выбрать элемент **Режим доступа**.
2. В высветившемся справа от дерева конфигурации окне выбрать вкладку **Мастер доступа**.
3. В этой вкладке для каждого считывателя Bioscrypt необходимо создать **Уровень доступа Bioscrypt**. Для этого необходимо в столбце **Уровень доступа** выбрать из списка пункт **Создать уровень доступа**. В высветившемся окне **Конфигурирование для элемента "Уровень доступа Bioscrypt…."** на вкладке **Свойства уровня доступа Bioscrypt** можно откорректировать требования к секретности.
4. Нажать кнопку **Принять**.
5. Для каждого считывателя Bioscrypt необходимо выбрать в столбце **Уровень доступа** из списка необходимый уровень доступа Bioscrypt.
6. Нажать кнопку **Сохранить**.

9 Использование считывателей

Использование считывателей Bioscrypt предполагает:

- ввод отпечатков пальцев в «Программу оформления пропусков»;
- рассылку их в считыватели Bioscrypt, установленные на проходных.

9.1 Команды считывателя Bioscrypt

В программе «Администратор системы» в дереве конфигурации в папке **Компьютер** выбрать элемент **Драйвер Bioscrypt**, кликнуть на нем правой кнопкой мыши, в контекстном меню появятся следующие команды:

- Получить биопараметры руки,
- Очистить базу данных,
- Загрузить конфигурацию.

Команда **Получить биопараметры руки** позволяет вводить отпечаток пальца со считывателя и отправлять его в ПО ITRIUM®.

Команда **Очистить базу данных** удаляет всю имеющуюся в базе данных считывателя Bioscrypt информацию. Она важна при подключении нового считывателя, т.к. база данных считывателя может оказаться непустой. Очистка базы данных служит мерой безопасности.

По команде **Загрузить конфигурацию** в считыватель загружается база данных пропусков и отпечатков пальцев из ПО ITRIUM®. Эта команда нужна при замене старого считывателя на новый или когда в считывателе была стерта база данных отпечатков пальцев.

9.2 Ввод отпечатка пальца

Для того чтобы ввести отпечаток пальца, выполните следующие действия:

1. В «Программе оформления пропусков» выберите пропуск, для которого вы хотите задать отпечаток пальца.
2. В поле **Карта** введите номер карты.
3. В поле **Биометрия** нажмите кнопку **Ввести биометрию**.
4. На вкладке **Ввести биометрию** появится счетчик времени. На считывателе должен загореться желтый индикатор. Это означает, что устройство готово считывать информацию.
5. Поднесите палец к считывателю Bioscrypt.
6. После успешного добавления отпечатка пальца загорается зеленый индикатор и подается короткий звуковой сигнал. В поле **Статус** появляется сообщение **Биометрия получена**. Определяется качество и содержание отпечатка пальца. Отпечаток успешно добавлен.

ООО «ИТРИУМ СПб»

194100, Санкт-Петербург, ул. Харченко, д. 5, Литер А.
interop@itrium.ru
www.itrium.ru