Настройка сервиса верификации по отпечаткам пальцев на базе контроллеров BioSmart

Содержание:

Контроллеры БОРЕЙ обеспечивают контроль доступа с функцией биометрической верификации по лицам и отпечаткам пальцев. Функциональность обеспечивает плагин биометрической верификации. При работе с сервисом верификации владельцев пропусков по отпечаткам пальцев в качестве сканеров отпечатков поддерживаются контроллеры Biosmart 4, Biosmart 5M производства «Прософт-Биометрикс» (планируется поддержка контроллера BioSmart ProxE), в качестве сервера верификации выступает компьютер под управления ОС Windows (рекомендуется версия 10 IoT) с установленной сервисной службой.

> В данном разделе приведена информация по настройке верификации на базе контроллеров BioSmart. Полная информация о возможностях биометрической верификации приведена в следующих разделах:
>
> - [Биометрия по лицам и отпечаткам пальцев]
> - [Настройка биометрической верификации | Биометрия по лицам и отпечаткам пальцев, термометрия]

Общие сведения

Плагин биометрической верификации позволяет проводить двухфакторную идентификацию с биометрической верификацией владельцев карт по отпечаткам пальцев посредством сканеров отпечатков пальцев Biosmart 4, Biosmart 5M производства ООО «Прософт-Биометрикс», планируется поддержка модели Biosmart ProxE.

Сервером верификации выступает компьютер под управления ОС Windows с установленной «Службой НЕЙРОСС Интеграция» или АРМ НЕЙРОСС.

Для первичной идентификации владельца пропуска на контроллере БОРЕЙ может использоваться:

1. Отдельный считыватель карт с Wiegand или 1-Wire-интерфейсом, с возможностью идентификации по карте и/или по пин-коду.
2. Встроенный в контроллер BioSmart считыватель. Есть ограничение на тип используемых карт. Поддерживаются EM-Marine и Mifare. Подключение считывателя к Борей осуществляется по интерфейсу Wiegand.

Порядок передачи данных в системе с биометрической верификацией

1. На считыватель БОРЕЙ предъявляется идентификатор (карта и/или пин-код).
2. Контроллер БОРЕЙ по предъявленной карте находит запись владельца пропуска и проверяет наличие шаблонов отпечатков пальцев. При отсутствии шаблонов формируется отказ доступа, при наличии — отправляет эти данные Серверу верификации, работающему под ОС Windows. находит в своей базе данных шаблоны отпечатков отправляет эти данные Серверу верификации («Службе НЕЙРОСС Интеграция» или НЕЙРОСС АРМ) вместе с информацией о «привязанном» к точке доступа контроллере BioSmart.
3. Сервер верификации начинает управление контроллером BioSmart: отправляет команду на считывание отпечатка и инициирует получение результата считывания (отпечатка).
4. По получению отпечатка Сервер верификации осуществляет сверку с шаблонами, полученными от контроллера БОРЕЙ, и, если находится совпадение, — отправляет в БОРЕЙ положительный ответ, не находится — отрицательный.
5. БОРЕЙ принимает решение о разрешении или запрете доступа.

Подготовка к настройке

Для обеспечения совместной работы Платформы НЕЙРОСС, контроллера БОРЕЙ, Сервера верификации и контроллеров BioSmart, перед началом настройки сервиса верификации необходимо проверить, что каждый из узлов удовлетворяет перечисленным ниже требованиям, и, при необходимости, — выполнить рекомендуемые действия.

Узел	Порядок проверки
Платформа НЕЙРОСС	1. Лицензия включает требуемое количество пропусков с биометрическими данными [параметры лицензии]. В противном случае требуется приобрести лицензию; 2. В разделе Пользователи, роли и права настроена «облачная» учётная запись с правами Общее/Обслуживание.

Контроллер БОРЕЙ	1. Подключен считыватель карт. Схема подключения считывателя, в том числе, — встроенного в контроллер BioSmart, — приведена в справочнике монтажника. 2. Настроены параметры точек доступа. 3. Настроена сетевая доступность контроллера БОРЕЙ и Платформы НЕЙРОСС: статус узлов в разделе Сеть — [Норма], узлы принадлежат одному домену и настроены сетевые параметры; 4. Настроены параметры даты и времени, нет расхождения времени: рекомендуется настроить автоматическую синхронизацию по IP-адресу Платформы НЕЙРОСС; 5. Посредством АРМ НЕЙРОСС Доступ введены данные владельцев пропусков, включая отпечатки пальцев. Ввод отпечатков пальцев в Платформу НЕЙРОСС осуществляется посредством дактилоскопического сканера Futronic FS80H или сканера Biosmart. Ввод данных также возможен посредством ПАК Интеграция/ITRIUM с помощью Драйвера устройств BioSmart, при этом может использоваться любой контроллер BioSmart. 6. Данные пропусков с Платформы НЕЙРОСС загружены в контроллер БОРЕЙ: выполнена синхронизация данных . Также для загрузки «облачных» учётных записей в БОРЕЙ, необходимо проверить, что узлы синхронизированы по типу данных «Общий ресурс». Процедура синхронизации данных является точкой начала отслеживания изменений между узлами. В дальнейшем синхронизация будет проводиться автоматически.
Контроллер Biosmart	1. Настроены сетевые параметры контроллера. 2. В случае использования для первичной идентификации лица считывателя карт, встроенного в контроллер Biosmart, включите режим bypass: при включении этого режима доступна передача ID proximity карты, не зарегистрированной в базе ПО BioSmart-studio, на контроллер БОРЕЙ/ЯРС через wiegand-выход контроллера BioSmart.

Выбор сервера верификации

В качестве сервера верификации требуется использовать компьютер, работающий под управлением операционной системы Windows.

Требования к серверу верификации:

1. Работа СТРОГО под управлением операционной системы Windows. Рекомендуемая версия: 10 IoT. Эти требования обусловлены необходимостью поддержки SDK от компании BioSmart. Возможно использование сервера в виртуальной среде.
2. Установка всех обновлений ОС Windows.
3. Установка Microsoft Visual C++ 2013 Redistributable (x86) и VisualCppRedist_AIO_x86_x64 или всех последних обновлений.
4. Круглосуточная сетевая доступность для контроллера БОРЕЙ и считывателя BioSmart.

> В целях оптимизации программные средства интеграции со считывателями BioSmart могут поставляться отдельно в виде «Службы НЕЙРОСС Интеграция», а также включены в комплекс программ АРМ НЕЙРОСС.

Таким образом, если в организации есть рабочие места операторов с установленным АРМ НЕЙРОСС, работающие под управлением операционной системы Windows, включённые круглосуточно, вы можете использовать любой из этих рабочих мест в качестве сервера верификации. Для использования АРМ достаточно на этапе настройки плагина интеграции указать IP-адрес рабочего места. В этом случае пропустите нижеследующий этап и перейдите к настройке плагина [Порядок настройки сервиса].

В случае отсутствия рабочего места с требуемыми параметрами, а также при наличии административных задач выделения отдельного сервера верификации, выполните настройку сервера верификации [Порядок настройки сервера верификации].

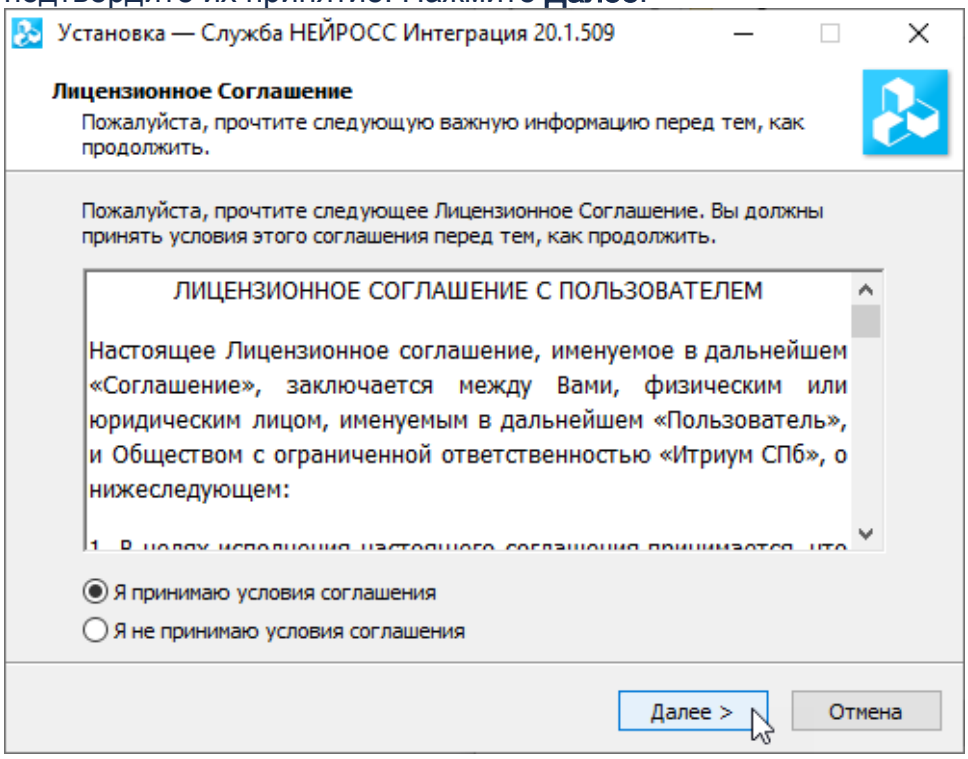
Порядок настройки сервера верификации

1. Выделите компьютер, работающий под управлением операционной системы Windows, который будет выступать в качестве сервера верификации.
2. Скачайте инсталлятор «Службы НЕЙРОСС Интеграция» или АРМ НЕЙРОСС. Ссылка для скачивания доступна с IP-адреса Платформы НЕЙРОСС, из раздела Основные настройки.

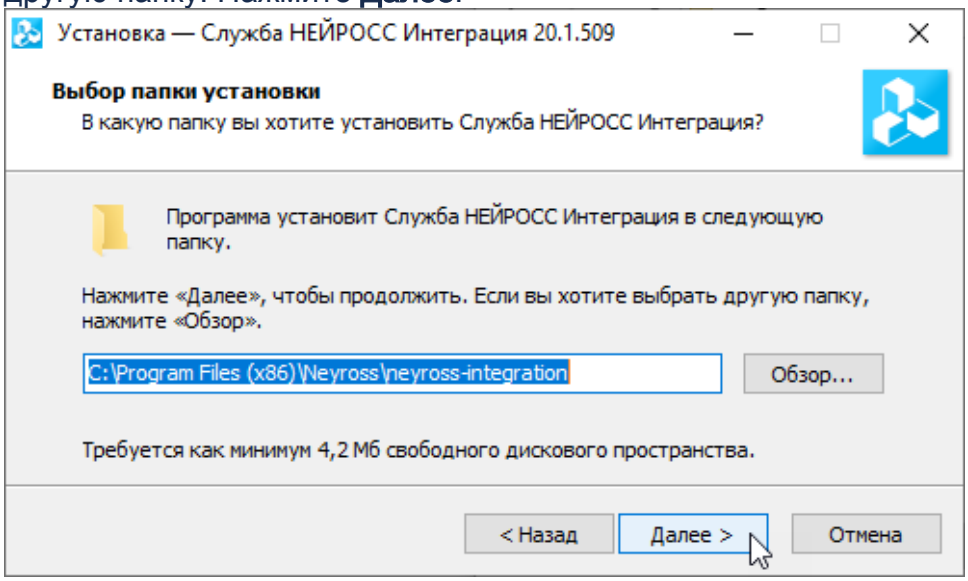
   > Ссылка для скачивания доступна с версии 20.10 Платформы НЕЙРОСС. При использовании предыдущих версий, либо работы в автономном режиме, обратитесь к представителю компании ИТРИУМ с требованием предоставления файла NeyrossIntergationSetup.exe.

3. Запустите на выполнение файл `NeyrossIntergationSetup.exe`.

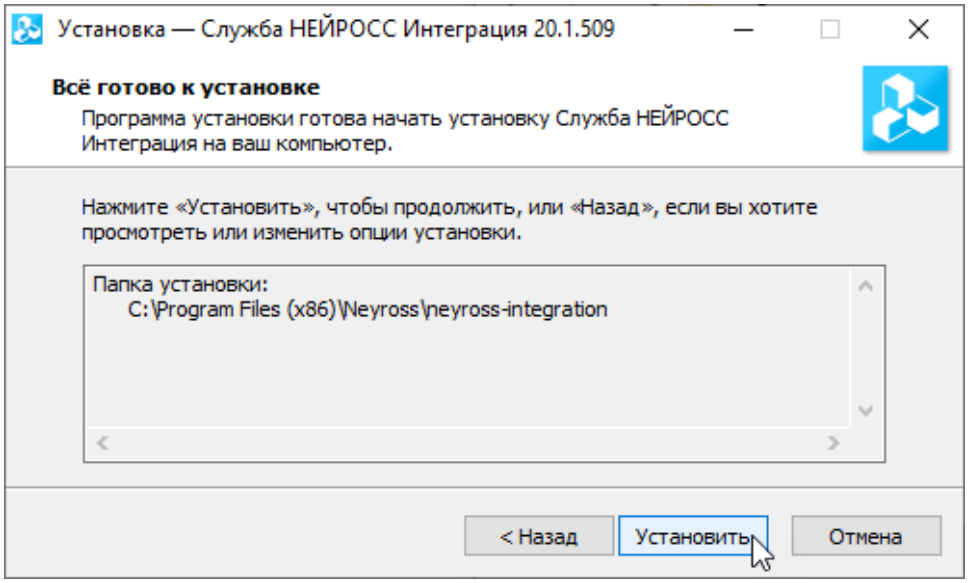
4. Прочитайте условия лицензионного соглашения и в случае согласия подтвердите их принятие. Нажмите **Далее**.



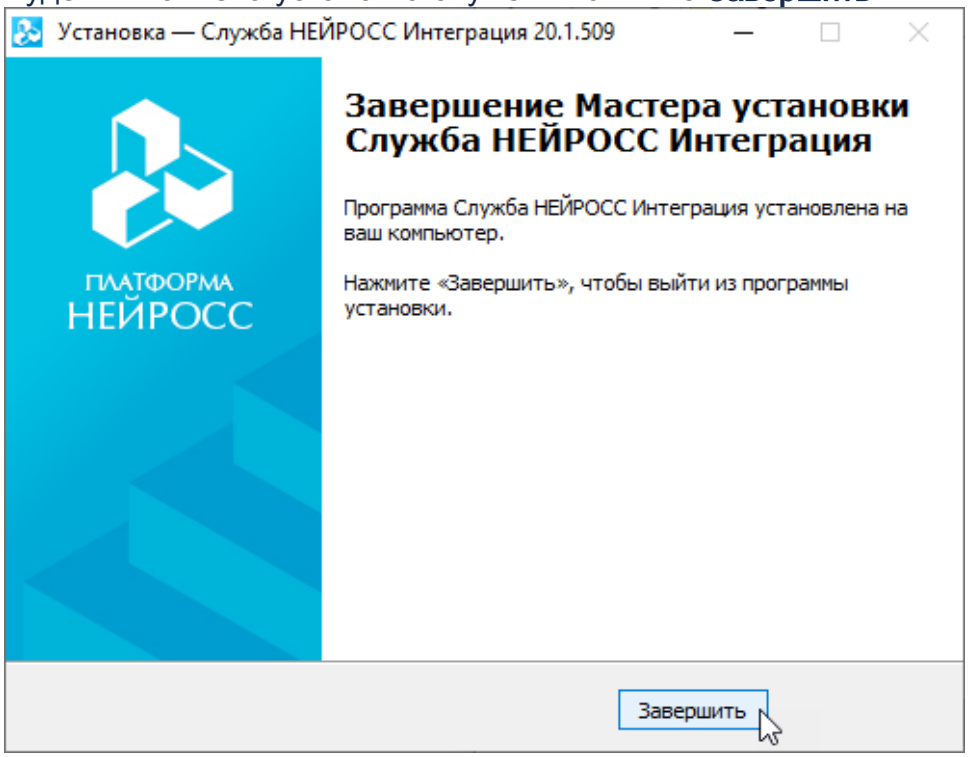
5. Согласитесь с выбором папки установки или нажмите на **Обзор** и укажите другую папку. Нажмите **Далее**.



6. Нажмите **Установить**.



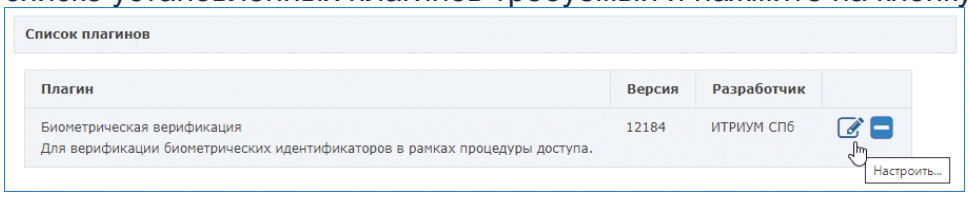
7. Будет выполнена установка службы. Нажмите **Завершить**.



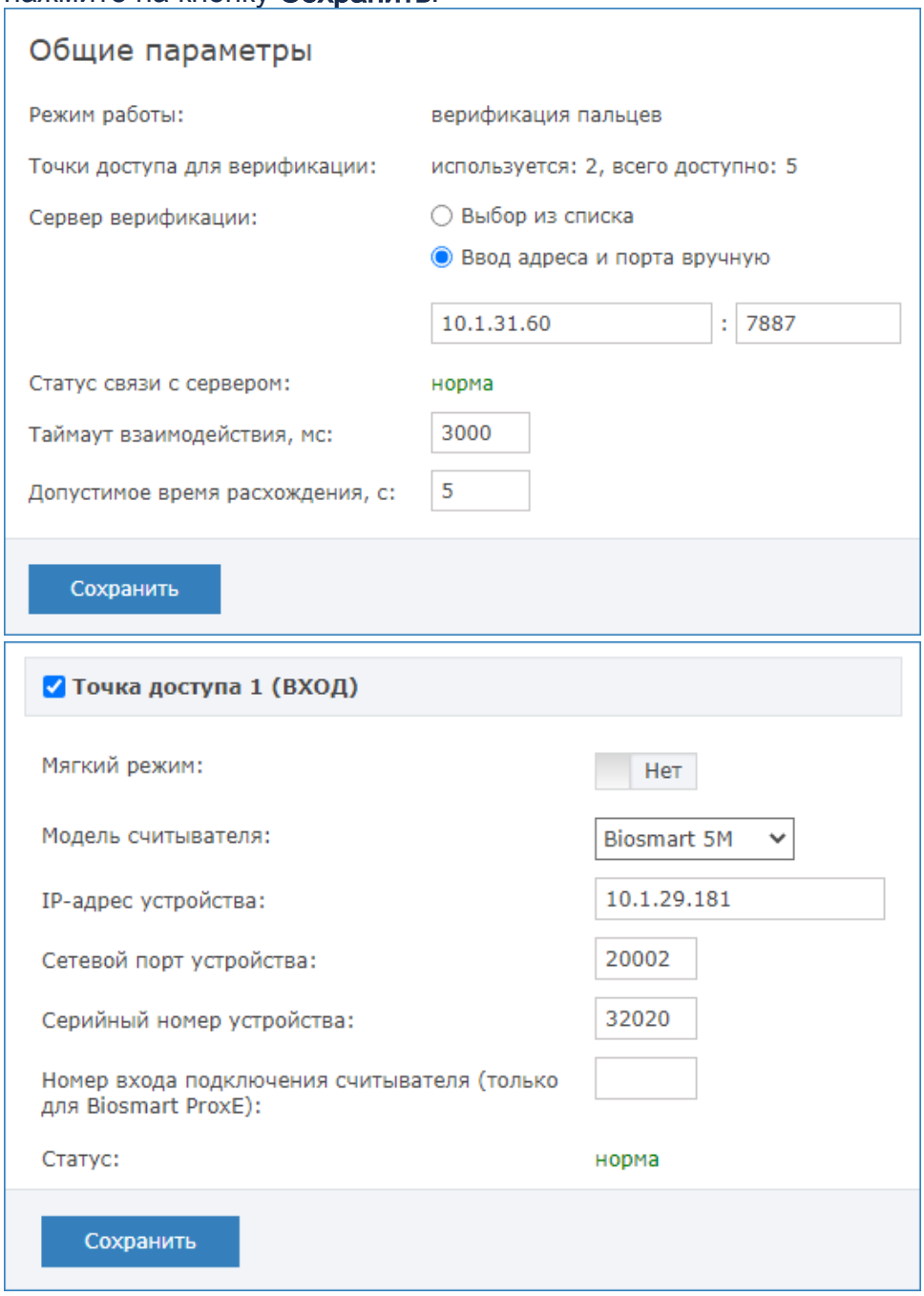
8. Проверьте доступность порта 7887 для «Службы НЕЙРОСС Интеграция».

Порядок настройки сервиса

1. Авторизуйтесь на узле БОРЕЙ под «облачной» учётной записью с правами общего конфигурирования [Пользователи, роли и права].
2. Перейдите к разделу Конфигурация узлов > Плагины и скрипты. Найдите в списке установленных плагинов требуемый и нажмите на кнопку **Настроить**.



3. В отобразившемся окне задайте общие параметры плагина, затем перейдите к вкладке **Точки доступа**, установите флаг для точки/точек, которые планируется использовать для доступа с верификацией отпечатков пальцев, настройте параметры точек доступа. Описание полей представлено в таблице ниже. По окончании процедуры настройки нажмите на кнопку **Сохранить**.



Поле **Режим работы** информационное. Плагин лицензируется на работу в определённом режиме. Поле **Точки доступа для верификации** отображает число точек доступа, настроенных на верификацию отпечатков, а также общее число точек доступа, доступных по лицензии. Поле **Допустимое время расхождения** не используется в настройках верификации отпечатков пальцев. В поле **Статус связи с сервером** отображается текущее состояние связи с сервером верификации. В поле **Статус** в настройках точки доступа отображается статус связи с контроллером Biosmart.

Параметры плагина

Поле	Диапазон значений	Комментарий
Вкладка Общее		
Сервер верификации	IP-адрес:порт	Выберите **Ввод адреса и порта вручную** и укажите IP-адрес сервера верификации и порт **7887** в разные поля, отделенные двоеточием.
Таймаут взаимодействия, мс	Целое число, рекомендуемый диапазон 8000 — 10000	Период времени, в течение которого ожидается ответ от сервера верификации о результате верификации. Если по истечению времени ответ не получен, верификация считается неуспешной, решение о разрешении или запрете доступа принимается на основе текущего режима верификации: при мягком режиме доступ разрешается, при жёстком — доступ запрещается. **ВАЖНО** Указанный интервал отсчитывается от сигнала считывателя. В указанный промежуток пользователь должен успеть приложить палец. При низкой скорости сетевого соединения или долгой подготовке пользователя к процедуре сканирования увеличьте временной интервал до 10 000 мс.
Вкладка Точки доступа		
Мягкий режим	Да/Нет, логическое поле	По умолчанию установлено в **Нет**, это означает, что при отсутствии положительного решения от сервера верификации, формируется отказ доступа. Использование

		«мягкого» режима рекомендуется в целях тестирования сервиса и/или использования функции видеоверификации и подтверждения доступа оператором.
Модель считывателя	• BioSmart 5M • BioSmart4 • BioSmart ProxE (временно не поддерживается)	Выберите из раскрывающегося списка модель используемого контроллера.
IP-адрес устройства	IP-адрес	Введите IP-адрес контроллера BioSmart, используемого для считывания отпечатков пальцев при верификации владельца пропуска.
Сетевой порт устройства	Номер порта, целое число	Введите порт, по которому осуществляется обмен данными с контроллером BioSmart. По умолчанию используется 20002.
Серийный номер устройства	Целое число	Введите серийный номер контроллера BioSmart.
Номер входа подключения считывателя	Целое число	Номер входа, на который подключен считыватель (0-5). Временно не используется.

Настройка уровня достоверности сравнения биометрических шаблонов Biosmart

С версии версии 3.3.0 SDK BioSmart появилась возможность настройки строгости идентификации. Новую версию АРМ НЕЙРОСС и «Службы НЕЙРОСС Интеграция» можно скачать из веб-интерфейса Платформы НЕЙРОСС, начиная с версии 20.10.

В предыдущей версии SDK уровень строгости идентификации эталонного и сканированного шаблонов отпечатков пальцев был достаточно высоким (уровень NORMAL), что повышало вероятность ошибочного отказа в доступе при низком качестве полученных отпечатков пальцев. Новая версия позволяет настроить порог, при котором отпечаток считается достоверным. Порог снижен согласно рекомендациям BioSmart (уровень LOW).

ВАЖНО

Так как в текущем алгоритме доступа используется двухфакторная идентификация, и отпечаток пальца является вторым признаком

подтверждения личности владельца, снижение уровня строгости не должно существенным образом повышать вероятность ошибочного предоставления доступа, однако решение о минимально-приемлемом уровне достоверности должен принимать администратор, выполняющий настройку системы на объекте.

Файл конфигурации config.conf

Настройка уровня достоверности осуществляется в конфигурационном файле config.conf, который должен быть создан и помещён в папку установки службы.

По умолчанию папкой установки является:

для АРМ НЕЙРОСС

```
c:\Program Files (x86)\Neyross\neyross-workstation\UltimaWorkstationService\
```

для Службы НЕЙРОСС Интеграция

```
c:\Program Files (x86)\Neyross\neyross-integration\
```

Создайте в требуемой директории файл со следующим содержимым:

```
services : [
{
service : "/biosmart/",

config : {matching_level:0},

enabled : "true"
}
]
```

, где **matching_level** — параметр, определяющий порог совпадения биометрических данных, полученных в процессе идентификации, с биометрическим шаблоном, хранящимся в базе данных; опциональная настройка, уровень достоверности; порог идентификации, соответствующие ему вероятность ошибочного предоставления доступа (FAR) и вероятность ложного отказа в доступе (FRR).

Задайте значение matching_level согласно таблице ниже.

Порог идентификации	FAR	Значение matching_level	config.conf
Максимальный (HIGHEST)	1e-8	1	{matching_level: 1}
Повышенный (HIGH)	1e-7	2	{matching_level: 2}

Нормальный (NORMAL)	1e-6	0	{matching_level: 0}
Пониженный (LOW)	1e-5	3 (значение по умолчанию, согласно рекомендации Biosmart)	{matching_level: 3}
Минимальный (LOWEST)	1e-4	4	{matching_level: 4}

ПОДСКАЗКА

При использовании порога, заданного по умолчанию ({matching_level:3}, LOW) дополнительных действий не требуется, файл конфигурации не обязателен.