

## Биометрия по лицам и отпечаткам пальцев

Контроллеры БОРЕЙ обеспечивают контроль доступа с функцией биометрической верификации по лицам и отпечаткам пальцев. Функциональность обеспечивает плагин биометрической верификации.

**Плагин** — это независимый программный модуль, предназначенный для расширения базового функционала. Как правило, поставляется в составе продукта, но может быть загружен и установлен впоследствии. Использование плагина лицензируется.

**i** Компания ИТРИУМ выпустила плагины интеграции систем биометрической идентификации по отпечаткам пальцев, видеоверификации лиц, а также плагины интеграции депозитариев, камер хранения и систем хранения ключей. В виде расширений функциональности контроллеров БОРЕЙ, ЯРС для работы в условиях отсутствия **Платформы НЕЙРОСС** могут поставляться приложения «Фотоидентификация» и «Видеоинформационная консоль». Использование плагинов лицензируется. Полный перечень плагинов приведен [здесь](#).

### Общие сведения

Плагин биометрической верификации позволяет проводить двухфакторную идентификацию владельца пропуска на основе предъявленного идентификатора (карта и/или пин-код) и биометрическим данным.

**i** При заказе БОРЕЙ с функцией биометрической верификации, контроллер поставляется с установленным и активированным плагином биометрической верификации. При необходимости плагин может быть добавлен и активирован вручную.

- [Установка плагина биометрической верификации](#)
- [Переактивация плагина](#)

### Принцип двухфакторной идентификации

Контроллер БОРЕЙ по идентификатору пользователя (карта и/или пинкод) осуществляет поиск владельца пропуска и уточняет права владельца на доступ к точке доступа. При неуспешной проверке формируется отказ в доступе, биометрические признаки не проверяются. Если доступ по идентификатору разрешен, контроллер отправляет на сервер верификации эталон для сравнения (фотографию владельца либо шаблоны отпечатков пальцев).

Порядок верификации:

1. Сервер верификации запрашивает биометрические признаки лица, предъявившего карту и/или пин-код (интервал видео на предмет выделения лиц, отпечаток пальца) и осуществляет верификацию с эталоном. Если шаблонов несколько (в случае верификации по отпечаткам пальцев), осуществляется последовательное сравнение с каждым до получения первого успешного результата.

2. Контроллер БОРЕЙ по факту полученного результата верификации осуществляет принятие решения о разрешении и запрете доступа. При соответствии эталону формируется разрешение доступа, при несовпадении — проверяется режим верификации. Если задан жесткий режим, формируется отказ доступа по биометрии, если задан мягкий режим, — формируется разрешение доступа или запрос на подтверждение оператору [АРМ НЕЙРОСС Фотоидентификация](#).

БОРЕЙ поддерживает интеграцию следующего оборудования/сервисов:

№	Сервис, оборудование	Комментарий
1	<p><b>Neurotec Biometric</b></p> <p>Сервис биометрической верификации владельцев карт с использованием технологии распознавания лиц Neurotec Biometric производства Neurotechnology</p>	<p><i>Сервером верификации</i> выступает Платформа НЕЙРОСС. В качестве источника видео выступает любая камера системы видеонаблюдения. Платформа осуществляет видеоанализ потока камеры (заданного интервала видео, хранимого в кеше) на предмет выделения лиц и сверку с полученным от контроллера БОРЕЙ эталоном.</p> <p>Обеспечивается двухфакторная идентификация. Контроллер доступа БОРЕЙ по факту предъявленного идентификатора (карта, пин-код, карта и пин-код) осуществляет отправку изображения владельца пропуска на Платформу НЕЙРОСС, получает результат сравнения и принимает решение о разрешении и запрете доступа.</p> <p><a href="#">Настройка сервиса верификации лиц на базе Neurotec Biometric</a></p>
2	<p><b>VOCORD Face.Control</b></p> <p>Сервис биометрической верификации владельцев карт с использованием технологии распознавания лиц VOCORD Face.Control производства ЗАО «Вокорд Телеком»</p>	<p><i>Сервером верификации</i> выступает «внешний» сервер VOCORD.</p> <p>Обеспечивается двухфакторная идентификация. Контроллер доступа БОРЕЙ по факту предъявленного идентификатора (карта, пин-код, карта и пин-код) осуществляет отправку изображения владельца пропуска на сервер Vocord, получает результат сравнения и принимает решение о разрешении и запрете доступа.</p> <p><a href="#">Настройка сервиса верификации лиц на базе VOCORD Face.Control</a></p>

3	<p><b>Сканеры Biosmart 4, Biosmart 5M</b></p> <p>Сервис биометрической верификации владельцев карт по отпечаткам пальцев посредством сканеров отпечатков пальцев Biosmart 4, Biosmart 5M производства ООО «Прософт-Биометрикс», планируется поддержка модели Biosmart ProxE</p>	<p><i>Сервером верификации</i> выступает компьютер под управления ОС Windows с установленной «Службой НЕЙРОСС Интеграция».</p> <p>Обеспечивается двухфакторная идентификация. Для первичной идентификации владельца пропуска может использоваться считыватель БОРЕЙ с Wiegand или 1-Wire-интерфейсом, с возможностью идентификации по карте и /или по пин-коду, либо встроенный в контроллер BioSmart считыватель (поддерживаются EM-Marine и Mifare).</p> <p>Контроллер БОРЕЙ находит в своей базе данных шаблоны отпечатков и отправляет эти данные Серверу верификации («Службе НЕЙРОСС Интеграция»). Служба начинает управление контроллером BioSmart: отправляет команду на считывание отпечатка и отправку результата считывания себе, затем проводит сверку с имеющимися шаблонами, и если находится совпадение — отправляет в БОРЕЙ положительный ответ, не находится — отрицательный. БОРЕЙ принимает решение о разрешении или запрете доступа.</p> <p><a href="#">Настройка сервиса верификации по отпечаткам пальцев на базе контроллеров BioSmart</a></p>
---	---	---

## Установка плагина биометрической верификации

Для обеспечения функций биометрической верификации плагин должен был установлен на контроллере.

 При заказе БОРЕЙ с функцией биометрической верификации, контроллер поставляется с установленным и активированным плагином биометрической верификации. При необходимости добавления и активации плагина вручную выполните следующие шаги.

1. Выполните подключение к [веб-интерфейсу](#) контроллера БОРЕЙ.
2. В разделе [Конфигурация узлов > Плагины и скрипты](#) в блоке **Загрузить плагин** укажите путь к файлу плагина формате NPF и нажмите **Загрузить**.

 Неизвестное вложение

- Плагин будет загружен и добавлен в список плагинов. Далее его требуется активировать. Для этого нажмите **Требуется активация**.

**Загрузить плагин**

ВНИМАНИЕ: после установки плагина необходимо создать резервную копию.

Вы можете загрузить \*.nrf файл плагина.

Файл:  neyrossbio.nrf

[Загрузить](#)

**Список плагинов**

Плагин	Версия	Разработчик	
Биометрическая верификация Для верификации биометрических идентификаторов в рамках процедуры доступа.	Требуется активация	12184	ИТРИУМ СПб <span style="float: right;">-</span>

- В отобразившемся окне активации скопируйте содержимое поля **Идентификатор плагина** и передайте менеджерам компании ИТРИУМ с указанием объекта эксплуатации. В ответ вы получите код активации, который нужно вставить в поле ниже. Далее нажмите **Активировать**. Вы получите сообщение об успешной активации плагина.

**Активация** Закреть

Для активации плагина «Биометрическая верификация» введите ниже код активации плагина для данного узла и нажмите «Активировать».

Идентификатор плагина:

744a605553442020100ba04c0011589-neyrossbio

Код активации:

```

Ct6MwGZer2k87DEJrYcBEGeJRd1R9pa+h1ShMxSXyteOXGtUJBBzJPdciOJ7bdTdpzqt6eYP4t8
6TKdgTIdbmyFkQsvx2wG57GfJ52nGx1Hudikd2Wusw85pdC8fwG3NYSWukjRUUGnNt0OrtmL/sh
CyN+LOvos8G9T0dAX7uNpltw0soQLJaGHA7Trkr0bBVe3WCnJbJjH73D7/Ty9XfChn5cCAV4ptQ
4ExK1LznQLylnWyB1dm+JE7fkUJV4Dntw9wQ=
```

[Активировать](#)

- Нажмите **Требуется перезапуск**, чтобы выполнить перезапуск узла.

**Список плагинов**

Плагин	Версия	Разработчик	
Биометрическая верификация Для верификации биометрических идентификаторов в рамках процедуры доступа.	Требуется перезапуск	12184	ИТРИУМ СПб <span style="float: right;">-</span>

- В отобразившемся окне подтверждения нажмите **Перезапустить**. Дождитесь окончания процедуры перезапуска.

? Неизвестное вложение

? Неизвестное вложение

- Создайте **резервную копию узла**. В случае, если файловая система на SD-карте вдруг будет повреждена или настройки контроллера будут сброшены, плагин будет восстановлен вместе с остальными конфигурационными данными из резервной копии. При отсутствии данных в резервной копии конфигурация плагина будет утеряна.

## Переактивация плагина

Код активации содержит лицензируемую информацию, например, — количество точек доступа с биометрической идентификацией. При приобретении дополнительных лицензий потребуются повторная активация плагина. Для этого:

- В разделе **Плагины и скрипты** наведите указатель мыши на требуемый плагин, нажмите на кнопку **Переактивировать**.
- Введите новый код активации.
- Нажмите **Активировать**.

4. Создайте [резервную копию узла](#).