Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ЭЛЕКТРОННОЕ РУКОВОДСТВО
«НАСТРОЙКА СИСТЕМЫ BIOSMART»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 073

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
И.о. заведующего кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЭЛЕКТРОННОЕ РУКОВОДСТВО «НАСТРОЙКА СИСТЕМЫ BIOSMART»

Исполнитель:
обучающийся группы ЗИБ-401С А. В. Новиков

Руководитель:
ст. преподаватель М. Ю. Черноскутов

Нормоконтролер: Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из электронного руководства, содержащего методические материалы для настройки системы контроля и управления доступом и пояснительной записки на 56 страницах, содержащей 36 рисунков, 30 источников литературы, а также 1 приложение на 2 страницах.

Ключевые слова: СКУД, BIOSMART, СИСТЕМА УПРАВЛЕНИЯ, ЭЛЕКТРОННОЕ РУКОВОДСТВО

Новиков А.В., Электронное руководство «Настройка системы Biosmart»: выпускная квалификационная работа / А. В. Новиков; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 56 с.

Актуальность настоящей работы обусловлена отсутствием структурированной упорядоченной информации на тему настройки системы Biosmart, доступной сотрудникам акционерного общества «Точка» (АО «Точка»), несущих ответственность за физический доступ в головное здание и офисы в регионах.

Цель данной выпускной квалификационной работы — разработать электронное руководство по настройке системы контроля и управления доступом Biosmart для специалистов области информационной безопасности АО «Точка».

Исходя из поставленной цели, предполагается решение ряда задач:

- проанализировать литературу и интернет-источники, посвященные системам контроля и управления доступа;
- изучить возможности систем контроля доступа;
- изучить комплекс организационных мер функционирования системы контроля и управления доступом;
- реализовать интерфейс электронного руководства по настройке системы контроля и управления доступом.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

У любого предприятия, имеющего конкуренцию, есть риски попасть во внимание выгодоприобретателей от простоя работы. Для того чтобы предотвратить потери, владельцы бизнеса задумываются об охранных системах, где-то это банальная сигнализация с договором, заключенным с группой быстрого реагирования, а где-то за предотвращение любых несанкционированных проникновений отвечает целая служба безопасности, которая может состоять из службы информационной безопасности, службы безопасности внутреннего порядка и охраны, ведущей посменное наблюдение за территорией компании. Любая система информационной безопасности начинается с обеспечения физической безопасности самой информационной системы, независимо от ее типа, размера или стоимости. В области физической безопасности термин «контроль доступа» относится к практике ограничения доступа к собственности, зданиям или помещениям, доступ к которым разрешен только уполномоченным лицам. Физический контроль доступа может быть достигнут с помощью человека (охранник, вахтер или администратор на стойке регистрации), с помощью механических методов, таких как замки и ключи на двери, или с помощью технических средств, таких как системы доступа, основанные на картах доступа или биометрической идентификации.

Очевидно, что для обеспечения безопасности в доме, вам нужно позаботиться о том, чтобы запереть двери перед отъездом. В основных компаниях, которые используют информационные системы для работы, если не на рабочем месте, то в здании находится специально обученное лицо с надписью «безопасность» или «служба безопасности» на значке или на обороте, обычно, этот человек контролирует наличие пропуска у тех, кто работает на предприятии, и записывает в гостевой журнал тех, кто должен попасть внутрь по рабочим вопросам. Как правило, современные офисные помещения оснащены камерами видеонаблюдения, поэтому в случае незаконных

действий посетителей их можно легко опознать. На смену охранникам, контролирующих вход в помещение, требующее особенного пропускного режима, приходят системы контроля и управления доступом (СКУД). СКУД является наиболее эффективным и востребованным подходом к решению задач комплексной безопасности организаций.

Компетентное использование СКУД в организации позволяет минимизировать риски несанкционированного доступа в помещения. При этом, подобные системы не являются преградой для прохода персонала и посетителей, в разрешенные для них зоны. Нужно понимать, что СКУД не исключают человеческий контроль, но эффективность работы службы безопасности значительно повышается, особенно при наличии множества зон риска.

К сожалению, в настоящее время не только сам процесс выбора СКУД несёт сложности, поскольку отсутствует систематизированная аналитическая информация по СКУД в мире, но и процесс настройки СКУД после монтажа вызывает множественные проблемы.

Важно подчеркнуть недобросовестность некоторых зарубежных компаний, пытающихся заполнить свободную нишу российского рынка. Проявляется это в неполном предоставлении технических и функциональных системных возможностях, особенностях эксплуатации и тонкостях настроек. В итоге, на важных объектах можно встретить СКУД, спроектированные непрофессионально.

Объектом исследования является система контроля и управления доступом головного офиса АО «Точка».

Предметом исследования является настройка системы контроля и управления доступом Biosmart.

Цель данной выпускной квалификационной работы — разработать электронное руководство по настройке системы контроля и управления доступом Biosmart для специалистов области информационной безопасности АО «Точка».

Исходя из поставленной цели, предполагается решение ряда задач:

- проанализировать литературу и интернет-источники, посвященные системам контроля и управления доступа;
- изучить возможности систем контроля доступа;
- изучить комплекс организационных мер функционирования системы контроля и управления доступом;
- реализовать интерфейс электронного руководства по настройке системы контроля и управления доступом.

Выпускная квалификационная работа состоит из введения, основной части (состоящей из двух глав — аналитической и проектной), заключения, списка использованных источников и приложений.

В аналитической главе представлена характеристика систем контроля и управления доступом, приведены определения и основные возможности СКУД, описаны источники и технологии, используемые в данных системах.

В проектной главе описано электронное руководство, указаны технологии и структура документа, а также интерфейс и навигация.

1 АНАЛИЗ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

1.1 Определение и основные возможности систем контроля и управления доступом

Для начала сформулируем понятие системы контроля и управления доступом (СКУД). Согласно ГОСТ Р 54831–2011 «Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний» [8]. СКУД — это совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Для рассматриваемого понятия, данная формулировка не дает полного понимания объекта исследования. Рассмотрим СКУД более подробно, как совокупность совместимых между собой аппаратных и программных средств, направленных на ограничение и регистрацию доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

В большинстве случаев СКУД включает в себя:

- устройства преграждающие управляемые (УПУ). Например, шлагбаумы, ворота, турникеты, шлюзы, двери, оборудованные управляемыми замками;
- устройства считывающие (УС), «считыватели». Например, дактилоскопические сканеры, устройства радиочастотной идентификации, устройства машинного зрения;
- контроллеры СКУД. Электронные микропроцессорные модули, реализующие аутентификацию объектов доступа, логику авторизации для доступа в те или иные помещения и области, управление УПУ;
- программное обеспечение СКУД. Элемент, позволяющий осуществлять централизованное управление контроллерами СКУД с персональ-

ного компьютера (ПК), формирование отчетов, разнообразные дополнительные функции;

- конверторы среды для подключения аппаратных модулей СКУД друг к другу и к ПК;
- вспомогательное неинтеллектуальное оборудование (блоки питания, кнопки), соединительные провода.

Одно из наиболее важных понятий в понимании работоспособности СКУД — это идентификатор доступа, носитель идентификационного признака: уникальный признак объекта или субъекта доступа. Идентификатором может быть цифровой код, графический ключ, вещественный код или биометрический признак (рисунок 1). Идентификатор с вещественным кодом представляет собой предмет, в который занесен идентификационный признак в виде кодовой информации (идентификационные бесконтактные индукционные карты, брелоки, электронные ключи, магнитные ключи и аналогичные устройства) [25].

В условиях индивидуальных характеристик экономических субъектов, возможности СКУД нужно использовать, рассматривая персональные потребности. Если анализировать потребности офиса банков, важно выделить индивидуальные аспекты, незначительные для промышленных предприятий и больших государственных объектов. Во всяком случае, все СКУД включают в себя базовые функции [28]:

- ведение и поддержание баз данных пользователей и идентификаторов;
- хранение фотографий пользователей в базе данных;
- фиксация даты и времени прохода в базе данных;
- задание уровней доступа;
- автономная работа контроллеров системы с сохранением основных функций управления при нарушении связи с компьютером;
- регистрация и хранение информации о событиях в энергонезависимой памяти контроллеров СКУД;

- сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;
- открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;
- запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака.

Рисунок 1 — Методы идентификации в системах контроля и управления доступом

Помимо типовых функций СКУД существуют дополнительные:

1. Запрет повторного прохода (правило antipassback). Используемый для запрета повторного входа посредством одного идентификатора, для входа в какую-либо зону доступа, предварительно не выйдя из неё. За нарушение правила antipassback, реакция контроллера доступа зависит только от установленного режима antipassback для уровня доступа рассматриваемого идентификатора. Может использоваться один из следующих режимов:
   - строгий — система запрещает повторный проход в зону доступа вплоть до выхода;
   - временной — в течение указанного времени система запрещает повторный проход в зону доступа вплоть до выхода;
   - мягкий — система не запретит доступ, но в журнале событий будет зафиксирован факт нарушения правила antipassback.

В системе можно настроить сетевой antipassback. При наличии сетевого контроллера, сообщения о проходах через точки доступа будут повторяться

всем контроллерам доступа, таким образом, правило antipassback сработает для всех точек доступа, впускающих идентификатор в зону ограниченного доступа (сетевой antipassback).

Правило antipassback можно ужесточить, если установить в уровне доступа параметр «Зональный antipassback». В этом случае учитываются проходы в любую зону доступа, и если предпринимается попытка прохода через один из считывателей контроллера доступа, то для выполнения правила antipassback требуется, чтобы последний зарегистрированный проход был в ту зону, где расположен данный считыватель. То есть, возможно проходить из зоны в зону только по порядку — 1, 2, 3 и в обратной очерёдности.

2. Доступ по правилу двух (или более) лиц. При контроле доступа к зонам доступа с повышенными требованиями безопасности, может использоваться режим прохода по «правилу двух лиц», имеющих санкционированные уровни доступа. При считывании первого идентификатора контроллер доступа перейдет в режим ожидания второго идентификатора. Если предъявленный после этого идентификатор имеет несанкционированный уровень доступа, то контроллер запретит проход. Если же уровень доступа будет согласован, доступ предоставится (в случае использования доступа по правилу трёх лиц эта процедура повторится и для третьего ключа). Такой режим прохода является параметром доступа для идентификатора и настраивается независимо для каждого направления прохода (для каждого считывателя).

3. Доступ с подтверждением. Если предполагается вход в зону ограниченного доступа не всех лиц, участвующих в процедуре доступа по правилу «двух (трёх) лиц» (например, сотрудник службы безопасности подтверждает доступ другого сотрудника), то для уровня доступа таких лиц устанавливается режим прохода «Подтверждающий». Самостоятельный доступ по ключу с таким режимом прохода невозможен, а при проходе по правилу двух (трёх) лиц по такому ключу не сформируется сообщения «Доступ предоставлен» и «Проход».

4. Двойная идентификация. Каждый считыватель контроллера способен работать в режиме, когда он распознает, что необходимо представить два идентификатора (например, Proxy-карта и отпечаток пальца). Данный режим может быть включен независимо для каждого считывателя. При двойной идентификации процедура предоставления доступа начинается с предоставления основного кода (первого идентификатора). Если ключ идентифицирован и режим доступа не нарушен, контроллер переходит в режим ожидания для получения дополнительного кода. Если появляется дополнительный код, процесс распознавания считается успешным.

5. Закрытый режим прохода. В этом случае все типы доступа с помощью контроллера запрещены.

6. Открытый режим прохода. Доступ к контроллеру свободный, без необходимости предъявления идентификатора.

Кроме того, в некоторых случаях есть возможность настроить следующие параметры в контроллере доступа:

1. Вид интерфейса подключенных считывателей — Touch Memory, Wiegand, Aba Track. Этот параметр отвечает за способ передачи прочитанного кода идентификатора в контроллер.

2. Датчик прохода — этот параметр указывает, что датчик используется в контроллере. В этом случае после предоставления доступа контроллер ожидает через точку доступа, пока дверь не откроется, (либо до истечения заданного параметра «Время ожидания прохода») предъявление новых идентификаторов контроллером не воспринимается. Датчик прохода обязательно задействовать, если в системе используется правило antipassback, а также учитывается рабочее время сотрудника, поскольку эти функции могут работать только по правилу «Проход».

3. Контроль блокировки двери — при попадании в зону ограниченного доступа, по истечению времени, превышающее «Тайм-аут блокировки» формируется тревожное сообщение «Дверь заблокирована».

4. Контроль взлома — когда эта опция включена, при открытии двери без доступа, генерируется предупреждение «Дверь взломана».

5. Номер зоны доступа — от 0 до 65535. Номер зоны доступа, вход в которую контролируется данным считывателем (65535 — номер зоны доступа не определён — для проходных дверей).

6. Выключить при открывании двери — досрочное прекращение «открывающей» программы реле при открытии двери (реле выключается после срабатывания датчика прохода). Рекомендуется активировать эту функцию при использовании электромеханических замков (которые могут оставаться без питания, когда дверь уже открыта).

7. Выключить при закрытии двери — досрочное завершение «открывающей» программы реле после закрывания двери (реле отключается после восстановления датчика прохода). Рекомендуется включать при использовании вращающейся двери. Когда дверь вращается перед дверью, вы можете запустить новую программу для обеспечения доступа. Этот параметр всегда включен при использовании шлюза, потому что при выходе из шлюза, если идентификатор не указан, его нельзя ввести снова и выйти из него можно только после нажатия кнопки выхода.

1.2 Общие принципы работы

Существующие системы контроля доступа делятся на две категории:

1. Простые, рассчитанные на одну входную дверь. Обычно при такой архитектуре используются автономные контроллеры.

2. Сложные, предназначенные для контроля доступа на крупных объектах [23].

Независимо от того, из чего состоит СКУД, в нее входят несколько обязательных узлов, это — контроллеры для управления, считыватели для идентификации, а также всевозможные исполнительные устройства ограничения доступа: ворота, шлагбаумы, шлюзы, турникеты, электромагнитные

замки и защелки. Электронные бесконтактные карты в качестве пропусков являются самым распространенным и удобным средством идентификации в системах контроля доступа.

Принцип работы всех систем сводиться к трем базовым действиям:

1. Предоставление права доступа.
2. Идентификация.
3. Доступ.

Работа системы контроля и управления доступом выглядит следующим образом: после внедрения системы контроля доступа на объект, сотрудники получают уникальный идентификатор (магнитная карточка, бесконтактная карта, отпечаток пальца, в случае использования биометрических систем) и различные защищенные зоны делятся по правам доступа. На входе в требующие контроля зоны, подключаются считыватели идентификаторов, контроллеры и электромагнитные замки. При размещении идентификатора у считывателя, считыватель передает информацию контроллеру, определяющему, наделен ли данный идентификатор соответствующими полномочиями, и, при наличии соответствующих прав, открывает доступ (рисунок 2). При активной функции учета рабочего времени, в базу данных сохраняется информация о событии [18].

Идентификатор может быть одновременно пропуском на территорию организации и ключом к помещению, куда сотруднику разрешен доступ.

Все ограничивающие устройства подключены к контроллерам системы контроля доступа. Контроллеры предназначены для получения и анализа информации о представленных картах доступа, а также для управления различными приводами. Оборудование системы контроля доступа может включать в себя два типа контроллеров: контроллеры блокировки и контроллеры турникетов, каждый из которых отвечает за мониторинг работы своего собственного узла.

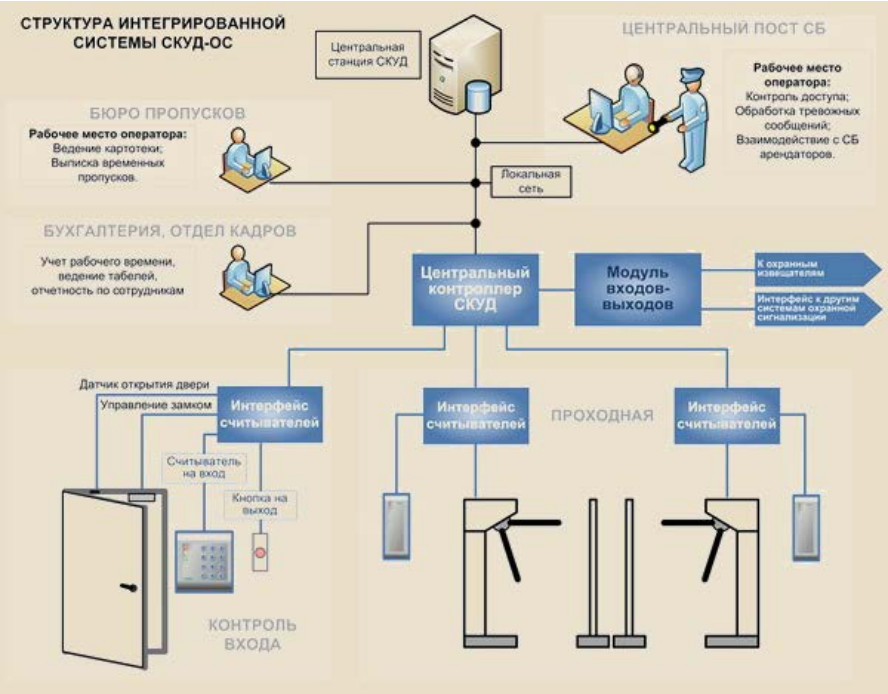


Рисунок 2 — Схема работы системы управления доступом

Чтобы пройти через турникет или войти в ответственное помещение, сотрудники предприятия должны прислонить свою карту доступа к считывателю, после чего считыватель отправляет код представленной карты контроллеру, и контроллер доступа решает, разрешить или пропустить пройти на основе информации. Если доступ разрешен, система контроля доступа автоматически разблокирует турникет или дверной замок (рисунок 3).

Рисунок 3 — Идентификация пользователя

Кроме того, используя систему контроля доступа, можно управлять въездом транспортных средств, и в этом случае ворота открываются или шлагбаум поднимается после представления персонального идентификатора (рисунок 4).

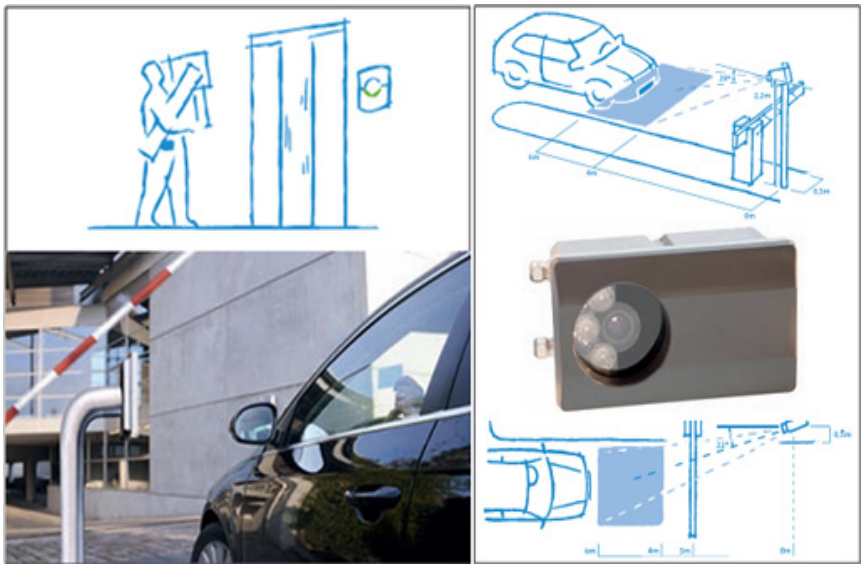


Рисунок 4 — Идентификация автомобиля

Для организации групповых политик, контроллер СКУД можно запрограммировать так, чтобы определенные сотрудники могли входить в определенные помещения только в определенное время.

Все события о проходах через контрольные пункты фиксируются в памяти системы управления доступом и могут использоваться для автоматизированного учета рабочего времени, блокировок учетных записей во внутренней компьютерной сети, а также для получения отчетов по дисциплине труда или для возможных служебных расследований на предприятии.

1.3 Общие принципы биометрической идентификации

Любая аутентификация человека строится на трёх традиционных принципах:

- по собственности. Имущество может включать пропуска, пластиковые карты, ключи или гражданские документы;

- по знаниям. Знания включают пароли, коды или информацию (например, девичья фамилия матери);
- по биометрическим характеристикам. Биометрическими характеристиками являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук.

Эти три принципа как могут использоваться по отдельности, так и использоваться в группах. Эта методология и порождает два основных направления биометрии: верификация и идентификация.

Верификация — это идентификация личности с помощью биометрического атрибута, которая выполняется с использованием одного из первых двух методов, описанных выше. Простейшим верификатором можно назвать пограничника и использующего паспорт для проверки вашего лица. Проверка означает более высокую надежность системы. Вероятность того, что система пропустит преступника, который не использует средства преодоления, равна «ложной тревоге» или «пропуск цели», а наиболее устоявшееся понятие — False Acceptance Rate (FAR), используемого биометрического метода. Даже для самых слабых биометрических систем эта возможность незначительна. Основными недостатками проверки являются два момента. Во-первых, человек должен иметь при себе файл или запомнить системный пароль. Всегда существует проблема пропущенной или забытой информации. Так же верификация принципиально невозможна для скрытной аутентификации.

Работу системы доступа, основанной на биометрической верификации, можно представить следующим способом (рисунок 5).

Биометрической идентификацией называется такое использование биометрического признака, которое не требует дополнительной информации. Поиск объекта осуществляется по всей базе данных и не требует предварительного ключа.

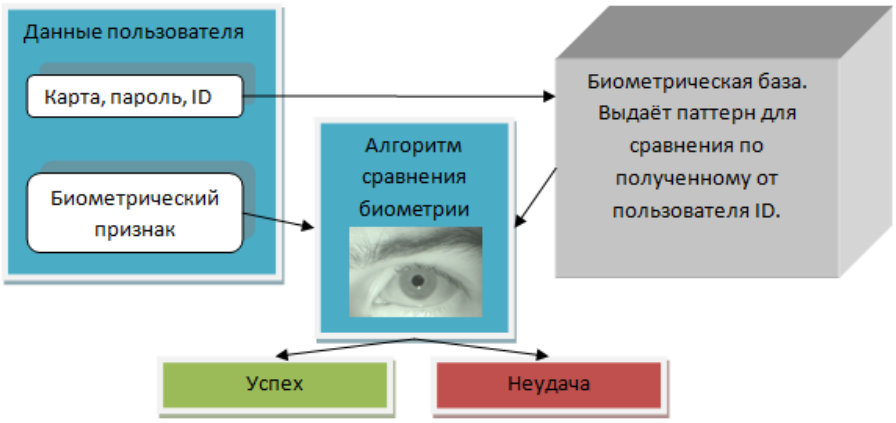


Рисунок 5 — Система работы биометрической верификации

Наглядно познакомиться со схемой биометрической идентификации можно далее (рисунок 6).

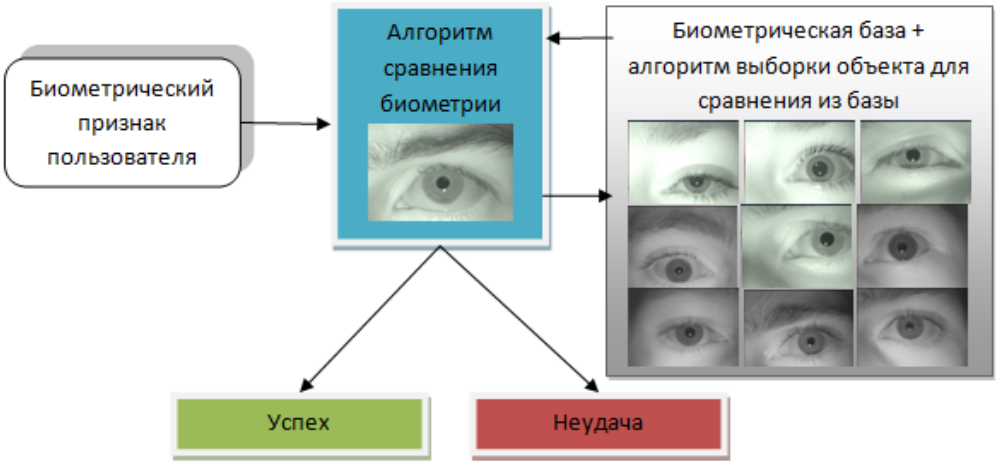


Рисунок 6 — Система работы биометрической идентификации

Понятно, что основным минусом этого является то, что чем больше человек в базе, тем больше вероятность ложного доступа произвольного человека. Плюс идентификации — все ключи всегда будут с вами, не нужно ни паролей, ни карточек.

1.4 Обзор источников по системам контроля и управления доступом

В книге «Системы контроля и управления доступом» [6] изложен обширный круг вопросов, связанных с использованием контрольно-

пропускного режима на различных объектах и применением СКУД. Большая часть внимания уделена средствам идентификации и аутентификации. Охарактеризованы устройства идентификации (считывания) различных видов; средства биометрической аутентификации личности и нюансы их использования; различные виды контроллеров и исполнительные устройства СКУД. Приведен обзор различных вариантов реализации СКУД. Даны фундаментальные рекомендации по выбору средств и систем контроля доступа. В приложении приведены ключевые выдержки из официальных нормативных материалов, связанных с использованием СКУД.

В книге «Электронная идентификация» [9] обсуждается тема создания и использования электронных средств идентификации для обеспечения точности учета и контроля во всех сферах человеческой деятельности. Детально анализируется технология бесконтактной RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) с индуктивной, электромагнитной и емкостной связью между мобильным электронным носителем данных и считывающим устройством. Рассмотрим перспективную электронную систему идентификации, основанную на использовании эффектов поверхностных акустических волн. Значительное внимание было уделено перспективным инструментам электронной идентификации, таким как смарт-карты. Описаны принципы электронных идентификаторов, особенно защита шифрованием смарт-карт, современные алгоритмы и протоколы. Приводится множество примеров практического применения электронных средств идентификации в различных сферах человеческой деятельности.

В учебнике «Системы контроля и управления доступом» [5] безопасность и защита информационных ресурсов, материальных ценностей и коммерческой тайны, а также дисциплины сотрудников рассматриваются как необходимое условие нормального существования и успешного развития. Автор рассмотрел систему контроля доступа. Анализируются функциональные характеристики, основные характеристики и параметры, которые должным

образом учитываются при проектировании системы, и выбирается алгоритм работы и конкретное оборудование для реализации.

Учебное пособие «Проектирование и исследование комплексных систем безопасности» [22] рассматривает все компоненты обеспечения безопасности. Автор детально описывает каждую составляющую. Проводит обзор, в том числе устройств идентификации, видов исполнительных устройства и контроллеров СКУД. Дается оценка влияния СКУД на обеспечение безопасности объекта.

На сайте-блоге «habr.com» [24] можно найти огромное количество публикаций, новостей, аналитических статей, мыслей, связанных с технологиями систем контроля и управления доступом. Контент сайта формируется пользователями-добровольцами, которые пишут в коллективные и персональные блоги. Именно в этих блогах и постах можно найти полезную информацию по применению, настройке, и работе с различными средствами защиты информации.

Сайт «cyberleninka.ru» [4] — это научная электронная библиотека открытого доступа, основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии, повышение цитируемости российской науки и построение инфраструктуры знаний. КиберЛенинка строится на основе парадигмы открытой науки.

На сайте «bio-smart.ru» [20] можно найти полноценное описание деятельности и продуктов инженерной компании «Прософт–Биометрикс», являющейся ведущим российским разработчиком систем информационной и технической безопасности и входит в состав мировых лидеров, активно продвигающих высокотехнологичные биометрические решения и комплексы.

«Прософт–Биометрикс» предлагает комплексные решения в области систем контроля и управления доступом, учета рабочего времени и информационной безопасности с использованием методов биометрической идентификации.

Исходя из вышеизложенного, проведенный анализ литературы и интернет-источников показал, что, несмотря на огромное количество интернет-порталов, книг, статей и других изданий, описывающих основные аспекты систем контроля и управления доступом, конкретного пособия, которое объединяло бы этот объемный по содержанию перечень информации, и которое можно было бы использовать при проведении практических и лабораторных работ не обнаружено. Исключением стал сайт компании «Прософт–Биометрикс», «bio-smart.ru».

1.5 Общие требования к руководству пользователя

Документ «Руководство пользователя» относится к пакету эксплуатационной документации. Основная цель руководства заключается в обеспечении пользователя необходимой информацией для самостоятельной работы с программой или автоматизированной системой.

Таким образом, документ должен отвечать на следующие вопросы: что это за программа, что она может, что необходимо для обеспечения ее корректного функционирования и что делать в случае отказа системы.

Мы можем выделить следующие основные разделы руководства пользователя:

1. «Назначение системы».
2. «Условия применения системы».
3. «Подготовка системы к работе».
4. «Описание операций».
5. «Аварийные ситуации».

Раздел «Назначение системы» должен содержать информацию о назначении системы, ее целях и задачах.

Пример: «Корпоративный интранет портал предназначен для повышения корпоративной культуры организации эффективного взаимодействия сотрудников. Основной целью портала является создание единого информаци-

онного пространства предприятия и оптимизация работы сотрудников путем облегчения коммуникаций между ними и оптимизации ряда бизнес-процессов».

«Условия применения системы». Данный раздел документа «Руководство пользователя» должен включать все те факторы, которые необходимы для корректной работы системы. Здесь можно выделить несколько подразделов:

1. Требования к аппаратному обеспечению — сюда можно включить требования к конфигурации компьютера пользователя, программное обеспечение необходимое для работы системы, а также наличие дополнительного оборудования (принтер, сканер и т.п.), если таковое необходимо.

2. Квалификация пользователя — данный подраздел руководства должен содержать требования к навыкам и знаниям пользователя (пример: «Пользователи должны обладать навыками работы с операционной системой Windows XP»).

«Подготовка системы к работе». Данный раздел руководства должен содержать пошаговую инструкцию для запуска приложения. К этапу подготовки системы к работе можно отнести установку дополнительных приложений (при необходимости), идентификацию, аутентификацию и т.п.

«Описание операций». Это основной раздел руководства, который содержит пошаговую инструкцию для выполнения того или иного действия пользователем.

Если работа автоматизированной системы затрагивает целый бизнес-процесс, то в руководстве пользователя перед описанием операций целесообразно предоставить информацию о данном процессе его назначении и участниках. Подобное решение позволяет человеку четко представить свою роль в данном процессе и те функции, которые реализованы для него в системе.

Далее в документе «Руководство пользователя» следует представить описание функций, разбитых на отдельные операции. Необходимо выделить подразделы, описывающие функции данного процесса, и действия, которые необходимо совершить для их выполнения.

Пример:

«4.1 Согласование проекта

Данный процесс предназначен для организации работы сотрудников, участвующих в разработке и согласовании проекта.

Автор проекта создает запись в «Системе» и прикрепляет пакет необходимой документации, далее проект передается на согласование руководящими лицами. Руководители после ознакомления с проектом могут подтвердить его или отправить на доработку автору.

4.1.1 Создание проекта

Для того чтобы создать Проект необходимо на панели «…» нажать на кнопку «…» и в появившейся форме заполнить следующие поля:

- наименование проекта;
- описание проекта.

Следующие поля заполняются автоматически:

- дата создания проекта — текущая дата;
- автор — ИФО и должность автора проекта».

Руководство пользователя может представлять собой как краткий справочник по основному функционалу программы, так и полное учебное пособие. Методика изложения материала в данном случае будет зависеть от объема самой программы и требований заказчика.

Чем подробнее будут описаны действия с системой, тем меньше вопросов возникнет у пользователя. Для более легкого понимания всех принципов работы с программой стандартами в документе «Руководство пользователя» допускается использовать схемы, таблицы, иллюстрации с изображением экранных форм.

Для крупных автоматизированных систем рекомендуется создавать отдельное руководство для каждой категории пользователя (пользователь, модератор и т.п.). Если в работе с системой выделяются дополнительные роли пользователей, то в документе «Руководство пользователя» целесообразно поместить таблицу распределения функций между ролями.

«Аварийные ситуации». Данный раздел документа «Руководство пользователя» должен содержать пошаговые инструкции действий пользователя в случае отказа работы системы. Если к пользователю не были предъявлены особые требования по администрированию операционной системы и т.п., то можно ограничиться фразой «При отказе или сбое в работе системы необходимо обратиться к системному администратору».

Интерактивные электронные технические руководства применяются для решения широкого спектра задач:

- обеспечение справочным материалом об устройстве и принципах работы изделия (в виде электронных документов с элементами мультимедиа);
- обеспечение персонала справочным материалом при использовании изделия по назначению;
- обеспечение справочным материалом при техническом обслуживании и ремонте изделия;
- обеспечение персонала информацией о проведении технологических операций с изделием (необходимый инструмент и материалы, количество и квалификация персонала);
- оперативный интеллектуальный поиск необходимой информации об изделии;
- автоматизированный сбор, хранение и обработка данных, полученных с диагностических приборов;
- поиск и выявление причин неисправностей, выдача рекомендаций по их устранению;
- планирование и учет проведения регламентных работ;
- автоматизированный заказ материалов и запасных частей;
- накопление полученных в процессе эксплуатации технических данных, их анализ и выдача рекомендаций пользователям по дальнейшей эксплуатации изделия;
- обмен данными между потребителем и поставщиком.

2 ОПИСАНИЕ ЭЛЕКТРОННОГО РУКОВОДСТВА

Разработанное электронное руководство «Настройка системы Biosmart» предназначено для сотрудников службы безопасности АО «Точка», инженеров поддержки информационных систем и ответственных сотрудников за систему контроля доступа в регионах.

2.1 Структура электронного руководства

Структура электронного руководства представлена 10 блоками:

- главная страница руководства;
- принятые в документе сокращения и термины;
- установка программного обеспечения (ПО) Biosmart Studio v5;
- общие сведения;
- запуск ПО;
- подключение и настройка оборудования и ПО Biosmart;
- настройка параметров сервера идентификации;
- общие сведения о работе с устройствами;
- поиск и добавление устройств;
- управление пользователями.

Данное руководство представлено набором одностраничных блоков с привязкой ссылок глав блоков к перемещению на начало главы.

Блок «Главная страница руководства» представлен основным логотипом банка АО «Точка» — акварельной кляксой, и содержанием руководства.

В разделе принятых сокращений документа можно ознакомиться с основными использующимися в документе сокращениями и терминами.

В блоке установка ПО Biosmart Studio v5 размещен подробный алгоритм установки основной используемой программы.

Блок «Общие сведения» хранит в себе информацию о технических возможностях сети внутри структуры настраиваемой системы Biosmart.

Блок о запуске ПО обладает информацией для первичного входа в ПО.

Подключение и настройка оборудования и ПО Biosmart, в этом блоке размещена основная информация по настройкам системы контроля и управления доступом.

2.2 Интерфейс и навигация

Руководство «Настройка системы Biosmart» включает в себя методические указания необходимые для получения навыков работы с системой Biosmart. Руководство разработано средствами веб-программирования и может работать в любом браузере, как при наличии интернета, так и без. В ходе разработки интерфейса руководства были использованы следующие технологии:

- sphinx doc — свободный набор инструментов для создания веб-документаций;
- язык разметки гипертекста — HTML (HyperText Markup Language);
- каскадные таблицы стилей — CSS (Cascading Style Sheets);
- раздвижная навигационная панель — JavaScript.

При разработке интерфейса электронного руководства были учтены требования, определяемые психофизическими особенностями человека. Конкретно, информационное оформление на экране, цветовая гамма страницы. В соответствии с этими принципами были выделены основные функционально-рабочие зоны: заголовок, навигация и рабочая область.

Конкретно, информационное оформление на экране, цвет страницы. На основе этих принципов определены основные функциональные рабочие области: заголовок, навигация и рабочая область.

На главной странице электронного руководства находится логотип, ставший визитной карточкой банка АО «Точка» — акварельная клякса. Глав-

ная страница руководства показана на рисунке 7. Под логотипом представлены разделы руководства в виде списка тем с главами. С данной страницы руководства можно перейти в любую часть руководства одним нажатием на соответствующую ссылку.

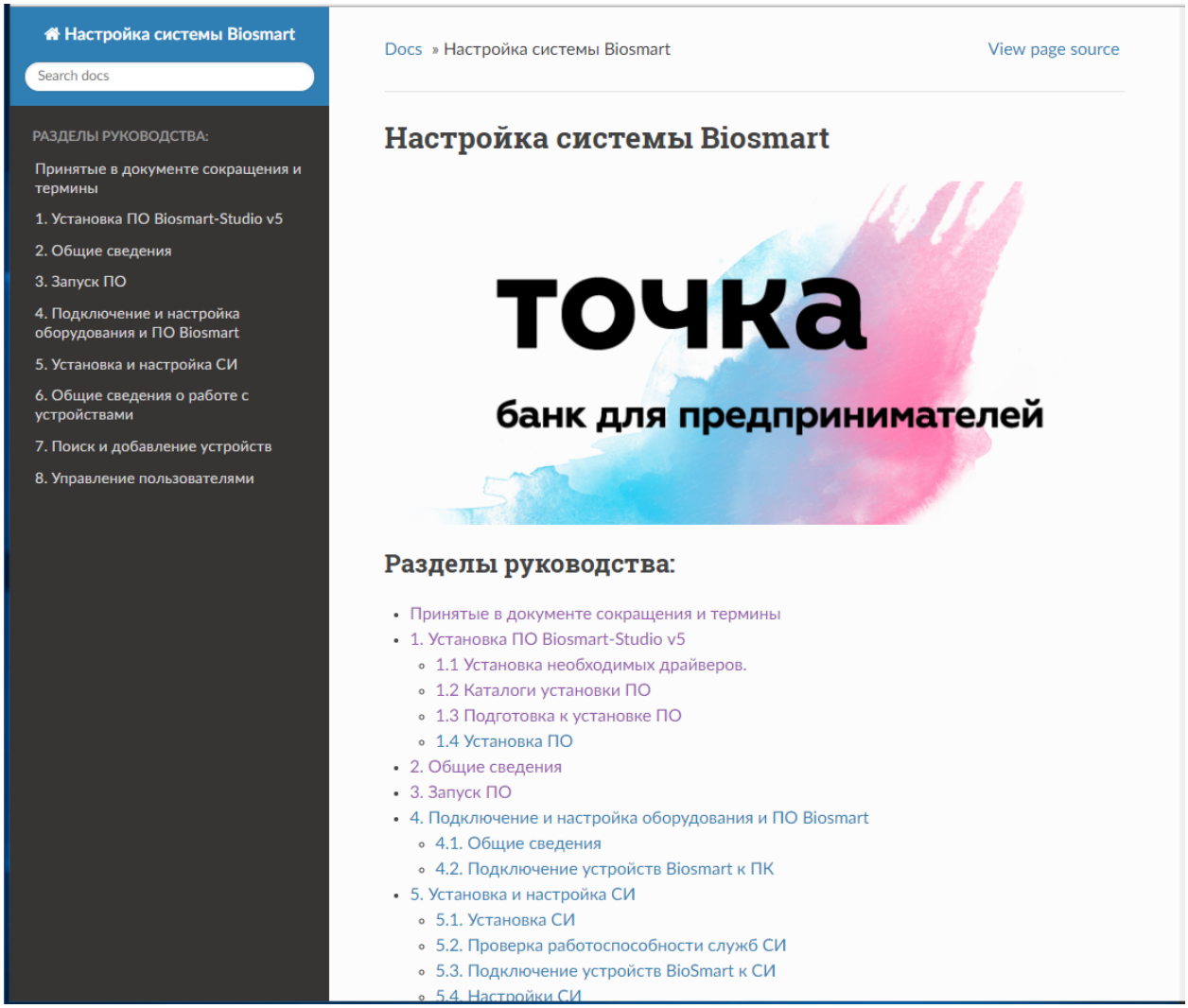


Рисунок 7 — Главная страница

В области навигации используется выпадающее меню для удобства перемещения по руководству.

Навигационное меню является основным и включает в себя 8 глав руководства, раздел принятых в документе сокращений и терминов, и поисковое окно (рисунок 8). Каждый из пунктов навигационного меню имеет список выпадающих подзаголовков при нажатии на соответствующий раздел. Данное решение помогает пользователям быстро и комфортно перемещаться внутри руководства.

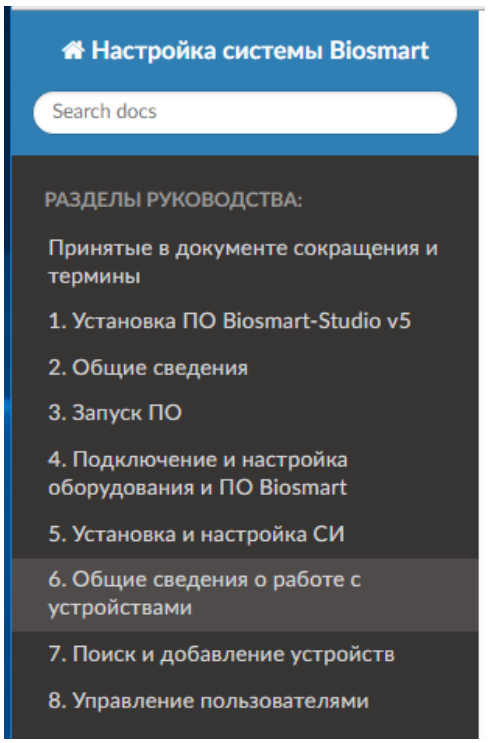


Рисунок 8 — Навигационное меню

Для удобства в руководстве имеется список используемых в тексте терминов и сокращений с описанием (рисунок 9).

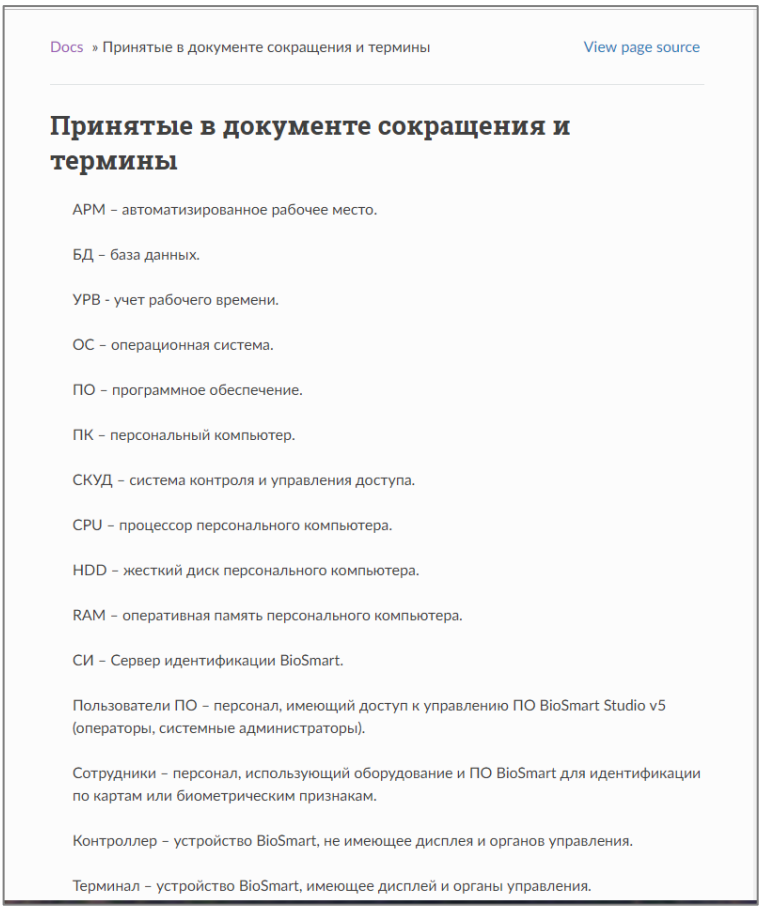


Рисунок 9 — Принятые в документе сокращения и термины

Как и любая другая система, требующая подключения нескольких внешних устройств, для работы с ними, система контроля и управления доступом на основе программного обеспечения и биометрических модулей фирмы Biosmart, перед началом работы требует установки необходимых драйверов и программ. В разделе 1 указаны все необходимые драйвера и программы со ссылками на дистрибутивы для скачивания с официального сайта компании Biosmart, www.bio-smart.ru (рисунок 10).

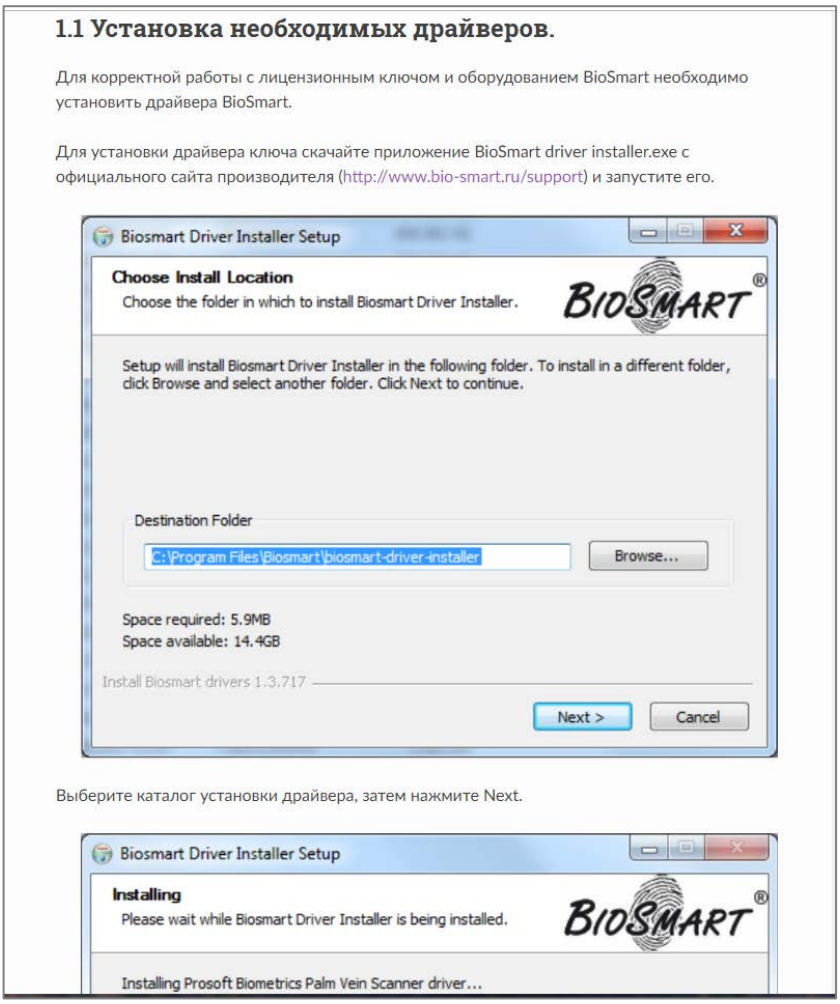


Рисунок 10 — Установка драйверов

Список каталогов устанавливаемого программного обеспечения Biosmart Studio 5 используется, в основном, для быстрого поиска необходимой базы, либо исполняемого файла для настройки режимов запуска файла, например, в постоянном режиме администратора, либо для выбора режима совместимости с необходимой операционной системой (рисунок 11).

1.2 Каталоги установки ПО

Данные	Каталог
Исполняемые файлы сервера BioSmart	%programfiles%BioSmart Studio 5
Исполняемый файл клиентского ПО	%programfiles%BioSmart Studio 5
Сервер лицензий	%programfiles%BioSmart Studio5licenseserver
Сервер базы данных PostgreSQL	%programfiles%BioSmart Studio 5db
Настройки сервера BioSmart	%programdata%BioSmart
Настройки клиентского ПО	%appdata%BioSmart
Данные БД	%programdata%bsdb

Рисунок 11 — Каталоги установки программного обеспечения

Важно помнить, что установка основного программного обеспечения возможно только в режиме запуска файла дистрибутива от имени администратора (рисунок 12).

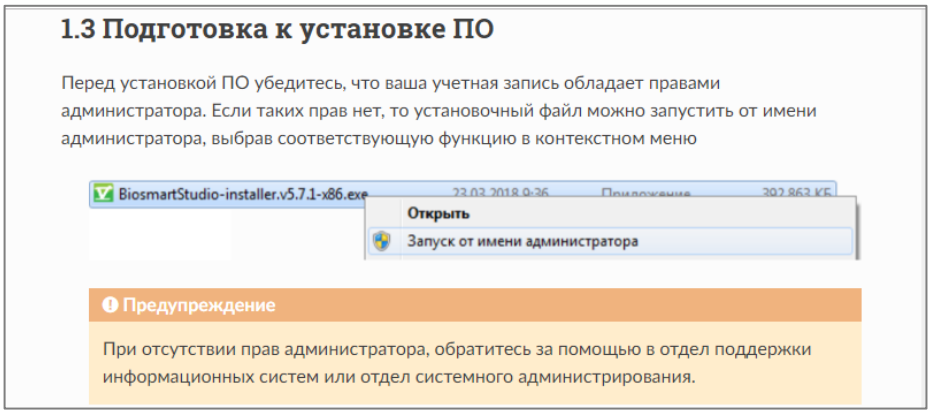


Рисунок 12 — Подготовка к установке программного обеспечения

Даже такой простой процесс, как установка программы через исполнительный файл важен для успешной настройки системы контроля и управления доступом.

Для начала, все просто. Запускаем ранее скачанный файл дистрибутива, после чего выбираем язык, по умолчанию русский (рисунок 13). В первом окне приветствия нажимаем далее, после чего переходим к ознакомлению с текстом лицензионного соглашения и принимаем его условия, ставя галочку напротив строки «Да, я принимаю условия лицензионного соглашения» и нажимаем кнопку «Далее».

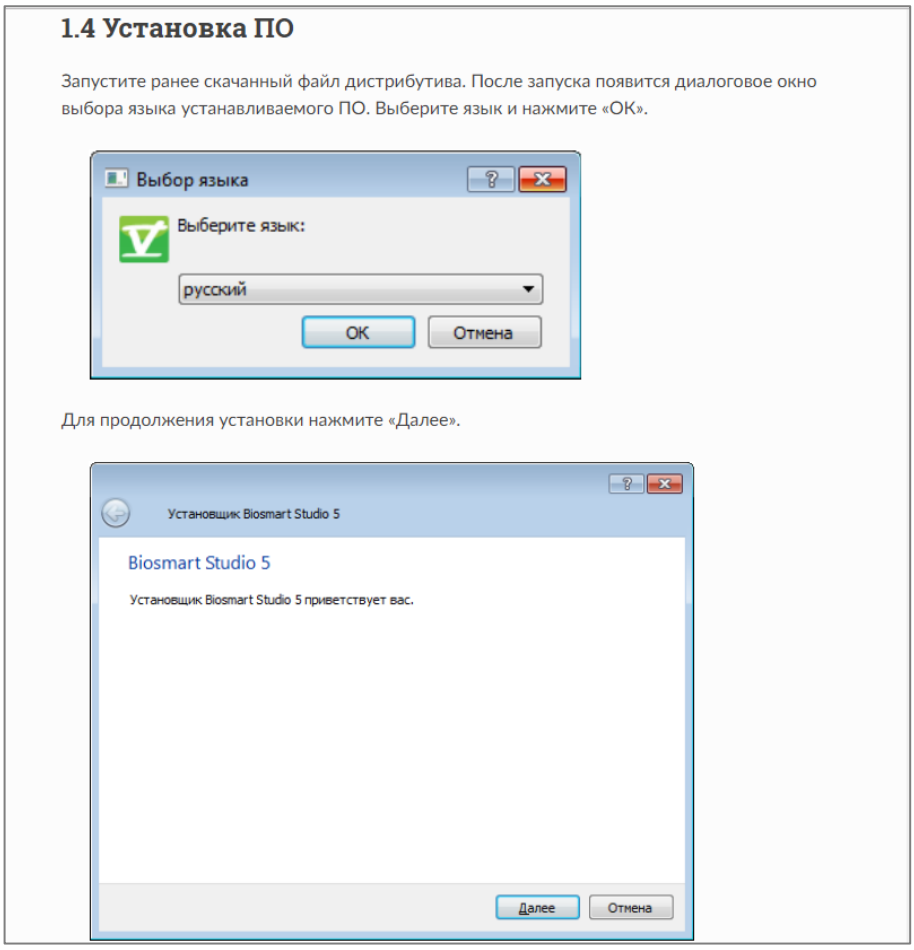


Рисунок 13 — Начало установки основного программного обеспечения

Если ранее была установлена версия Biosmart Studio и номер выпуска программы ниже, чем номер выпуска дистрибутива, программа предложит обновить версию до последней (рисунок 14).

Если производится первичная установка, выбираем компоненты системы, устанавливаемые на ПК:

1. Biosmart Studio v5 базовый — на данном компьютере будут установлены серверная и клиентская части ПО.
2. Biosmart Studio v5 NetWork Клиент — на данном компьютере будет установлена только клиентская часть ПО.
3. Biosmart Studio v5 NetWork Сервер — на данном компьютере будет установлена только серверная часть ПО.
4. Biosmart Studio v5 Мониторинг — на данном компьютере будет установлен только плагин «Мониторинг» клиентской части ПО.

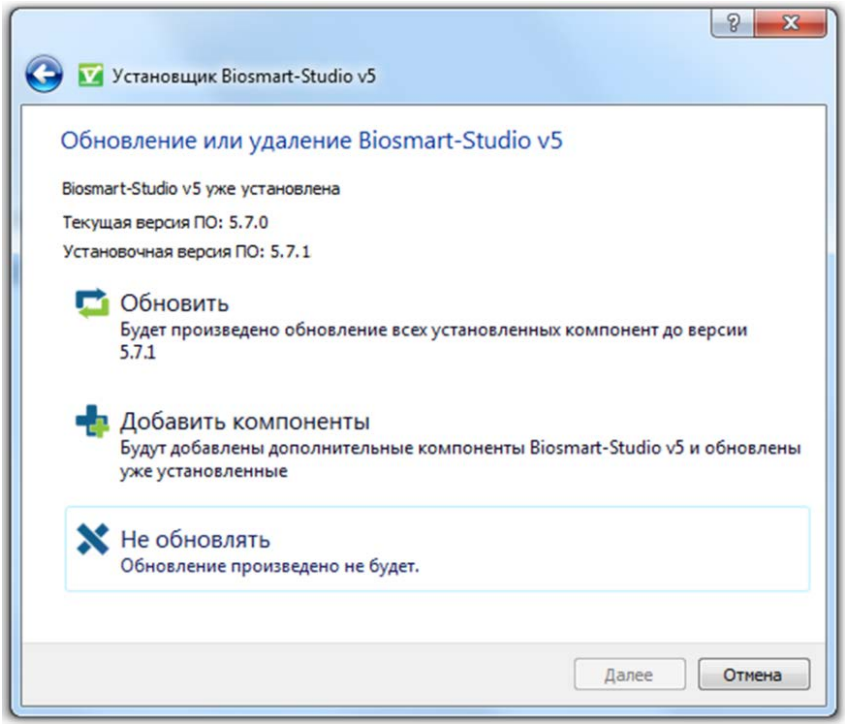


Рисунок 14 — Обновление предустановленной версии

Для типовой установки ПО рекомендуется Biosmart Studio v5 базовый. Для выборочной установки элементов ПО нужно выбрать «Режим эксперта». В этом режиме можно настроить установку отдельных программных модулей, например, установить сервер лицензий на отдельный ПК (рисунок 15).

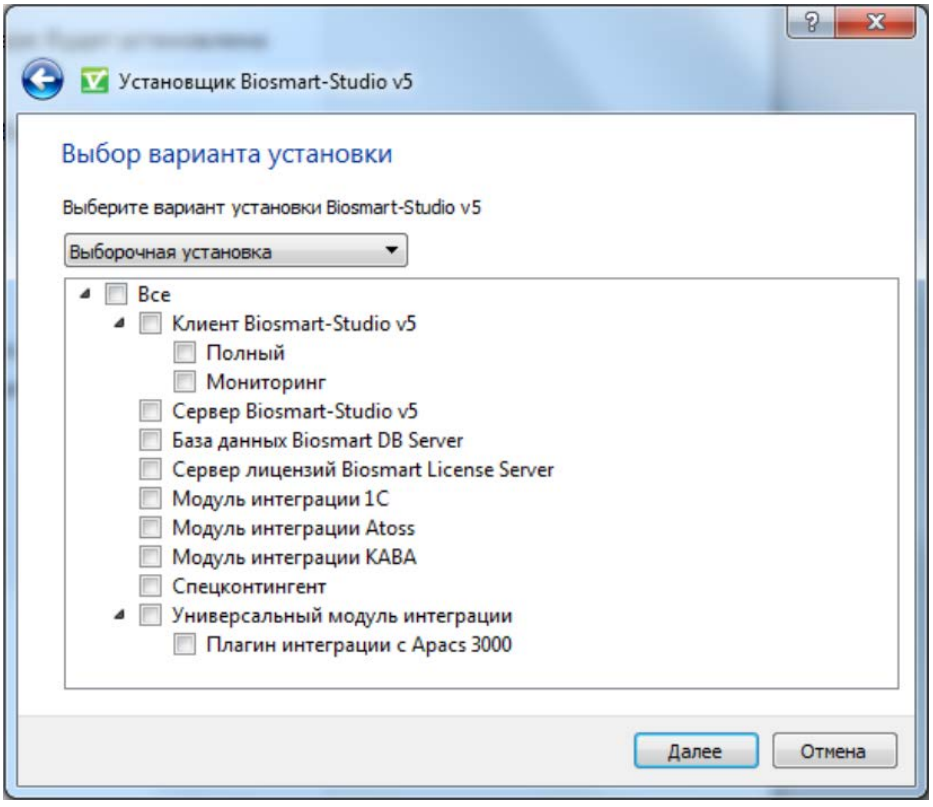


Рисунок 15 — Установка в режиме эксперта

После подтверждения установки, дистрибутив начнет распаковку, по ее завершению можно будет начинать настройку системы (рисунок 16).

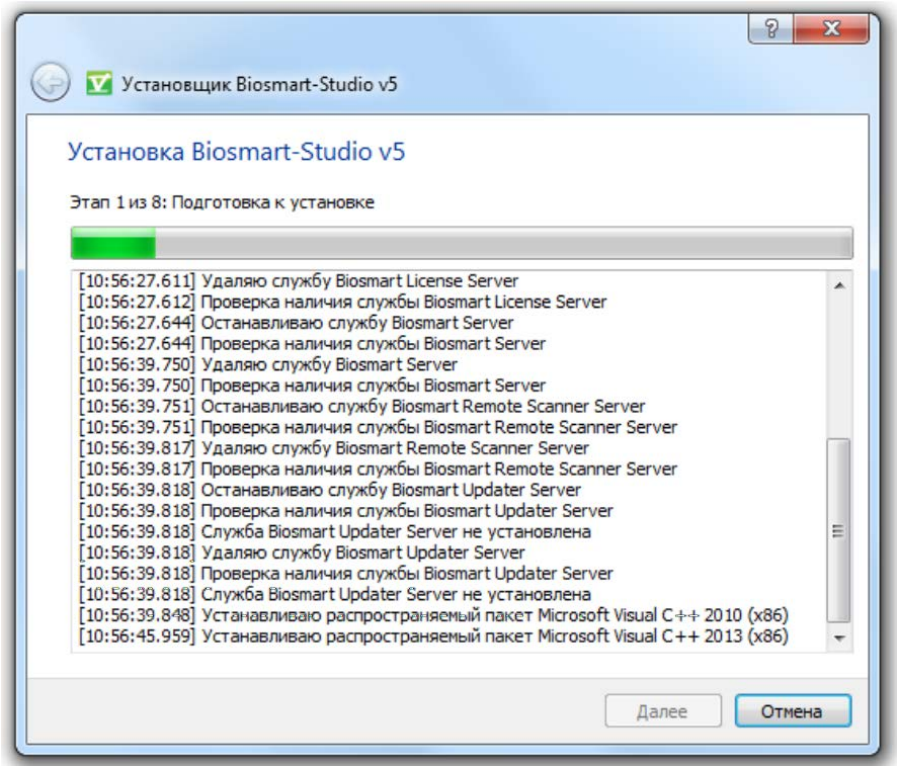


Рисунок 16 — Установка выбранного набора программного обеспечения

В разделе номер 2 располагается таблица с портами, используемыми ПО в сетевом протоколе TCP/IP (рисунок 17).

Порт	Назначение	Описание
20202, tcp	Сервер BioSmart	Соединение клиентского ПО с сервером BioSmart
5432, tcp	Сервер БД	Соединение сервера BioSmart с сервером БД
65432, tcp	Сервер лицензий	Соединение сервера BioSmart и клиентов с серверо
20203, tcp	Сервер Remote scanner	Соединение клиентского ПО Remote Scanner с сер
60003, 60004, tcp	Сервер BioSmart	Интеграция с 1С и другим сторонним ПОения.

Рисунок 17 — Таблица используемых портов

Третий раздел подскажет новому сотруднику, под какими учетными данными необходимо выполнять первый вход в клиентскую часть программного обеспечения Biosmart Studio v5 (рисунок 18).

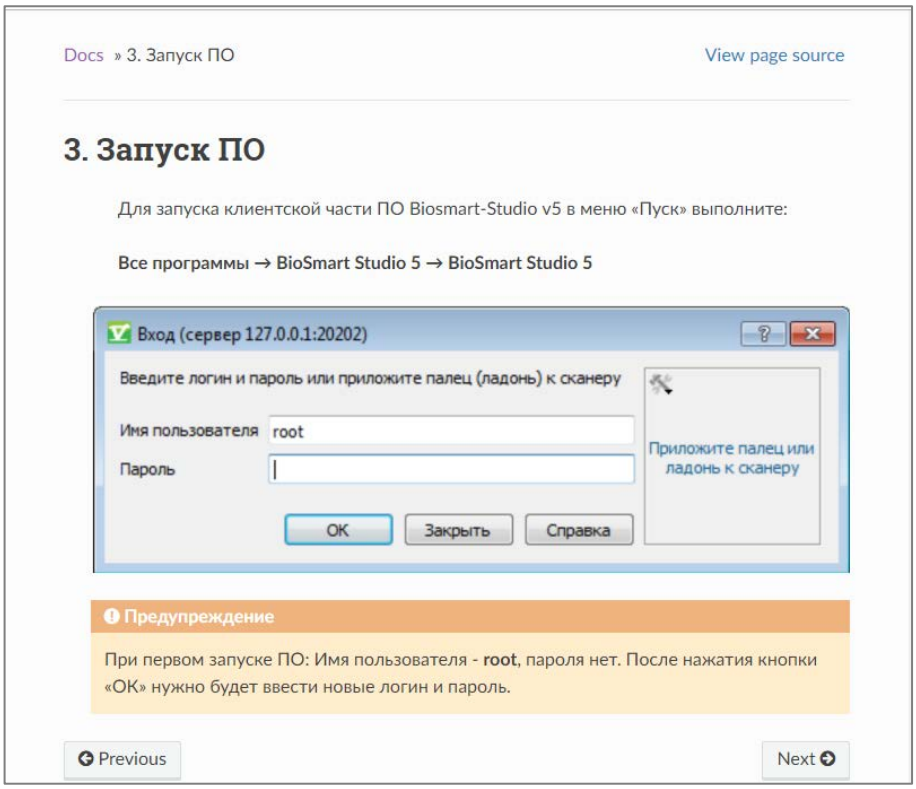


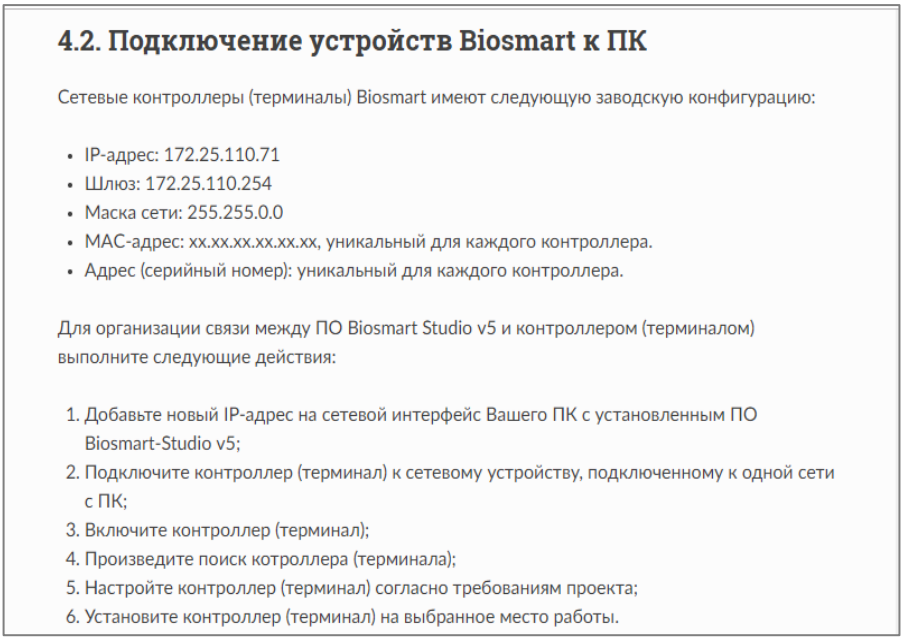
Рисунок 18 — Запуск программного обеспечения

Раздел под номером 4 начинается с обобщенных сведений для настройки биометрических контроллеров и объединения их и идентификационного сервера в одну систему (рисунок 19).

Рисунок 19 — Общие сведения к настройке контроллеров

Пункт 4.2. необходим для настройки каждого из модулей, так как они имеют одинаковые заводские настройки (рисунок 20), имеет смысл подключать их поочередно, меняя сетевые реквизиты на актуальные для каждого ре-

гиона. Узнать сетевые настройки в необходимом регионе можно, связавшись с отделом системного администрирования по почте.



4.2. Подключение устройств Biosmart к ПК

Сетевые контроллеры (терминалы) Biosmart имеют следующую заводскую конфигурацию:

- IP-адрес: 172.25.110.71
- Шлюз: 172.25.110.254
- Маска сети: 255.255.0.0
- MAC-адрес: xx.xx.xx.xx.xx.xx, уникальный для каждого контроллера.
- Адрес (серийный номер): уникальный для каждого контроллера.

Для организации связи между ПО Biosmart Studio v5 и контроллером (терминалом) выполните следующие действия:

1. Добавьте новый IP-адрес на сетевой интерфейс Вашего ПК с установленным ПО Biosmart-Studio v5;
2. Подключите контроллер (терминал) к сетевому устройству, подключенному к одной сети с ПК;
3. Включите контроллер (терминал);
4. Произведите поиск котроллера (терминала);
5. Настройте контроллер (терминал) согласно требованиям проекта;
6. Установите контроллер (терминал) на выбранное место работы.

Рисунок 20 — Заводские сетевые реквизиты модулей

Идентификационный сервер является основным связующим узлом в рассматриваемой системе контроля и управления доступом. Установка программного обеспечения начинается аналогично установке общего программного пакета Biosmart Studio v5.

После предустановочной подготовки в виде запуска дистрибутива от имени администратора и запуска исполняемого файла установки, переходим к ознакомлению с лицензионным соглашением по программному продукту «Сервер биометрической идентификации». Ознакомившись, ставим маркер напротив варианта «Да, я принимаю условия лицензионного соглашения» для продолжения установочного процесса, и нажимаем кнопку «Next».

В появившемся окне задаем каталог установки сервера идентификации и каталог базы данных сервера идентификации, порт сервера базы данных (по умолчанию 54321). В строке «Серийный номер» необходимо указать серийный номер сервера идентификации, который был предоставлен при покупке модуля «Сервер биометрической идентификации» или был озвучен при обновлении лицензионного ключа. Если серийный номер сервера был

утерян, необходимо связаться со службой технической поддержки клиентов Biosmart, подав заявку через их официальный сайт. Если планируется использовать бесплатную версию сервера идентификации, серийный номер по умолчанию — 120000. Далее необходимо указать IP-адрес компьютера, на который устанавливается сервер биометрической идентификации, порты для связи сервера идентификации с сервером Biosmart и контроллерами по умолчанию 20002 и 20003, соответственно. После завершения выбора и указания параметров идентификационного сервера необходимо нажать кнопку «Проверить сетевые параметры», так проверяется занятость выбранных портов (рисунок 21). После проверки сетевых параметров нажимаем «Next».

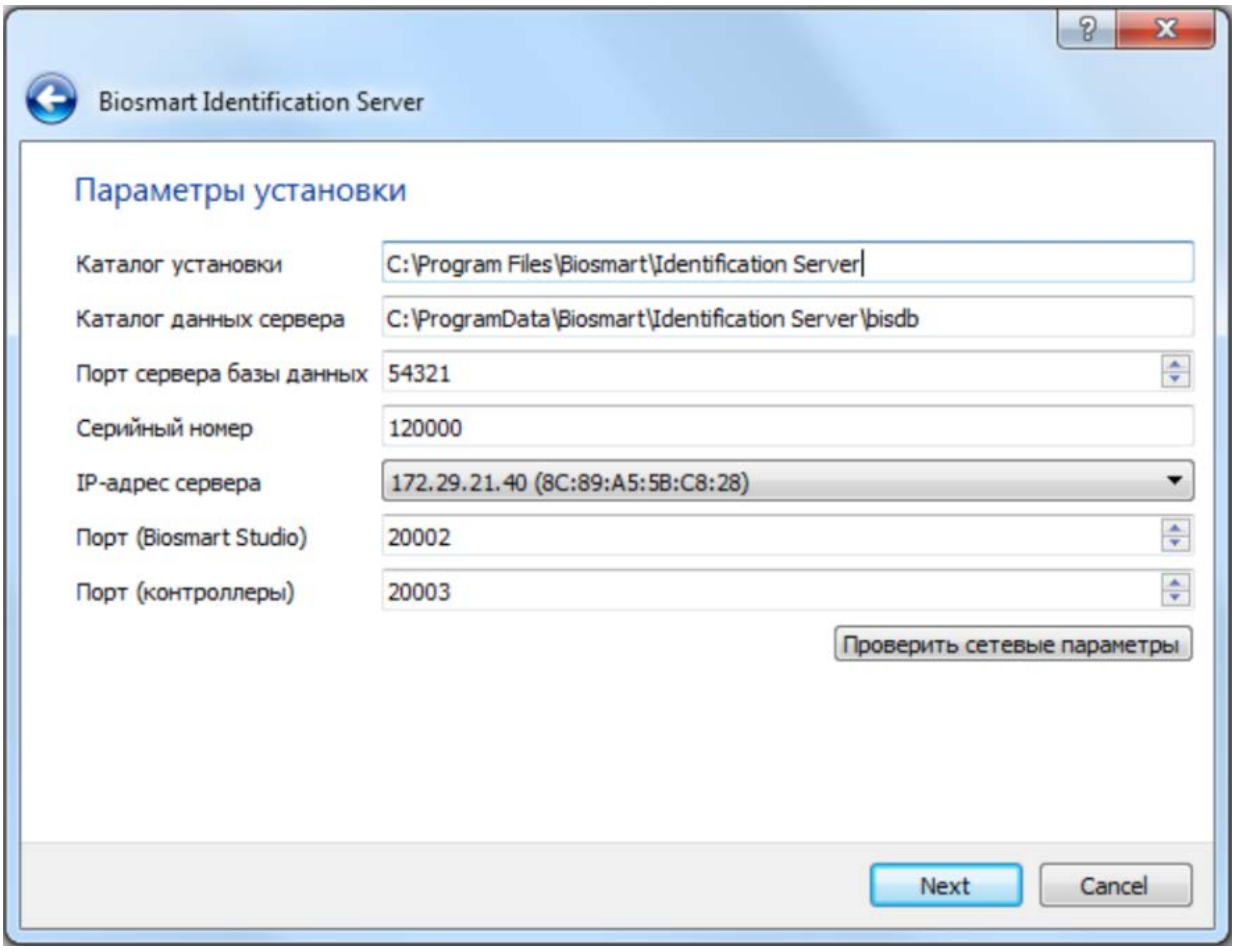


Рисунок 21 — Параметры установки сервера идентификации

Перед началом настройки сервера идентификации необходимо убедиться, что службы Biosmart находятся в рабочем состоянии (рисунок 22).

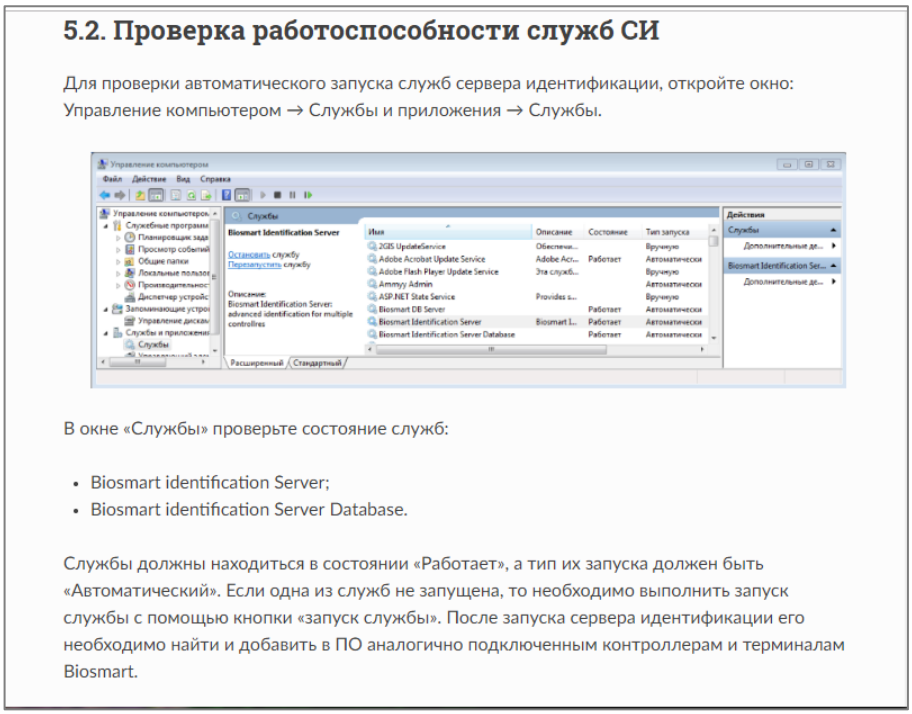


Рисунок 22 — Проверка работы служб сервера идентификации

Настройка сервера идентификации начинается с подключения устройств Biosmart, контроллеров (рисунок 23), предназначенных для идентификации пользователей по отпечаткам пальцев, например, Biosmart 4-O или 4-E (рисунок 24).

Рисунок 23 — Подключение контроллеров Biosmart к серверу идентификации

Рисунок 24 — Контроллер Biosmart 4-O-E

Основная настройка контроллеров выполняется в меню «Свойства контроллера». На вкладке «Общие» (рисунок 25) доступны следующие параметры сервера идентификации (СИ):

- название — название СИ, под которым он будет отображен в ПО;
- серийный номер — серийный номер СИ, задается при установке;
- подключаться автоматически — параметр определяет, будет ли автоматически установлена связь с СИ при его появлении в сети;
- прошивка — отображение текущей версии СИ;
- имя хоста — DNS-имя компьютера, на котором установлен СИ;
- IP-адрес — внешний IP компьютера, на котором установлен СИ;
- порт — порт обмена СИ с сервером Biosmart. Не изменяется, по умолчанию 20002;
- порт устройств — порт обмена СИ с устройствами Biosmart. Не изменяется, по умолчанию 20003;
- часовой пояс — устанавливает часовой пояс, в котором будет работать СИ, что позволит отображать события с привязкой к времени часового пояса, в СИ физически расположено;
- время ожидания ответа — устанавливает время ожидания ответа от СИ сервером Biosmart, в мс., по истечении которого будет зафиксирована ошибка связи с СИ;
- максимальный размер пакета, байт — параметр регулирует максимальный размер пакета данных, отправляемый СИ;
- количество пользователей — количество сотрудников для которых назначен доступ на СИ;
- количество шаблонов — количество отпечатков пальцев (шаблонов вен ладоней) в базе данных (БД) СИ на данный момент;
- количество журналов в памяти — количество журналов событий в БД СИ на данный момент.

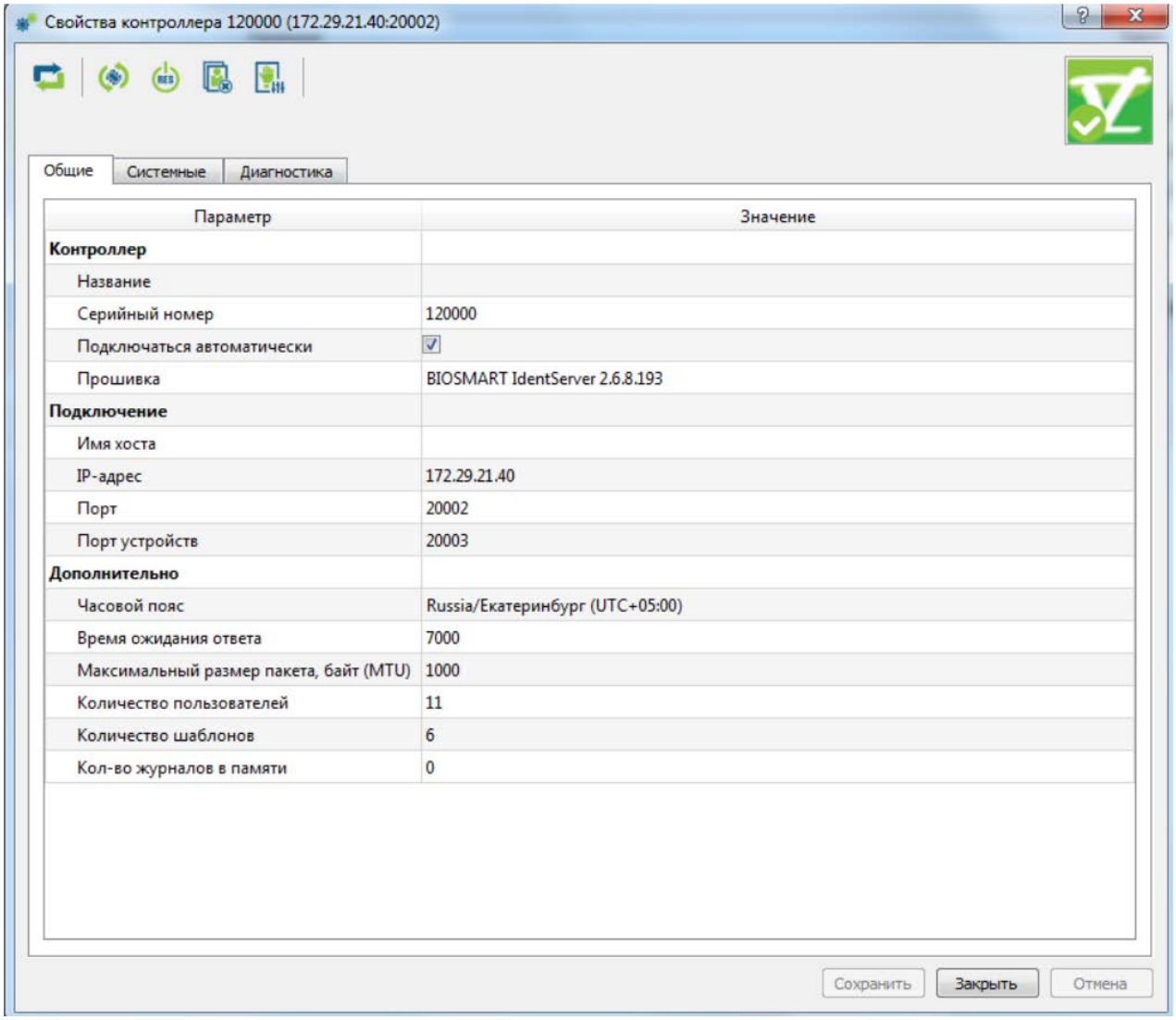


Рисунок 25 — Вкладка «Общие» в свойствах контроллера

На вкладке «Системные» (рисунок 26) доступны следующие параметры СИ:

- режим anti-pass-back — настройка позволяет перевести работу контроллеров, связанных с сервером идентификации в режим запрета повторного прохода сотрудника в одном направлении;
- максимальное количество пользователей — информационный параметр. Указывает на максимальное число сотрудников, прописанных в ключе лицензии на сервер идентификации;
- информация о пользователях в помещениях — при включении данного параметра сервер идентификации начинает формировать логи о количестве сотрудников в помещениях для учета их в плагине «Объекты доступа»

ПО Biosmart Studio v5;

- максимальное время нахождения в зоне АРВ — задает время (в часах), при превышении которого, сотрудник может осуществить переход между зонами.

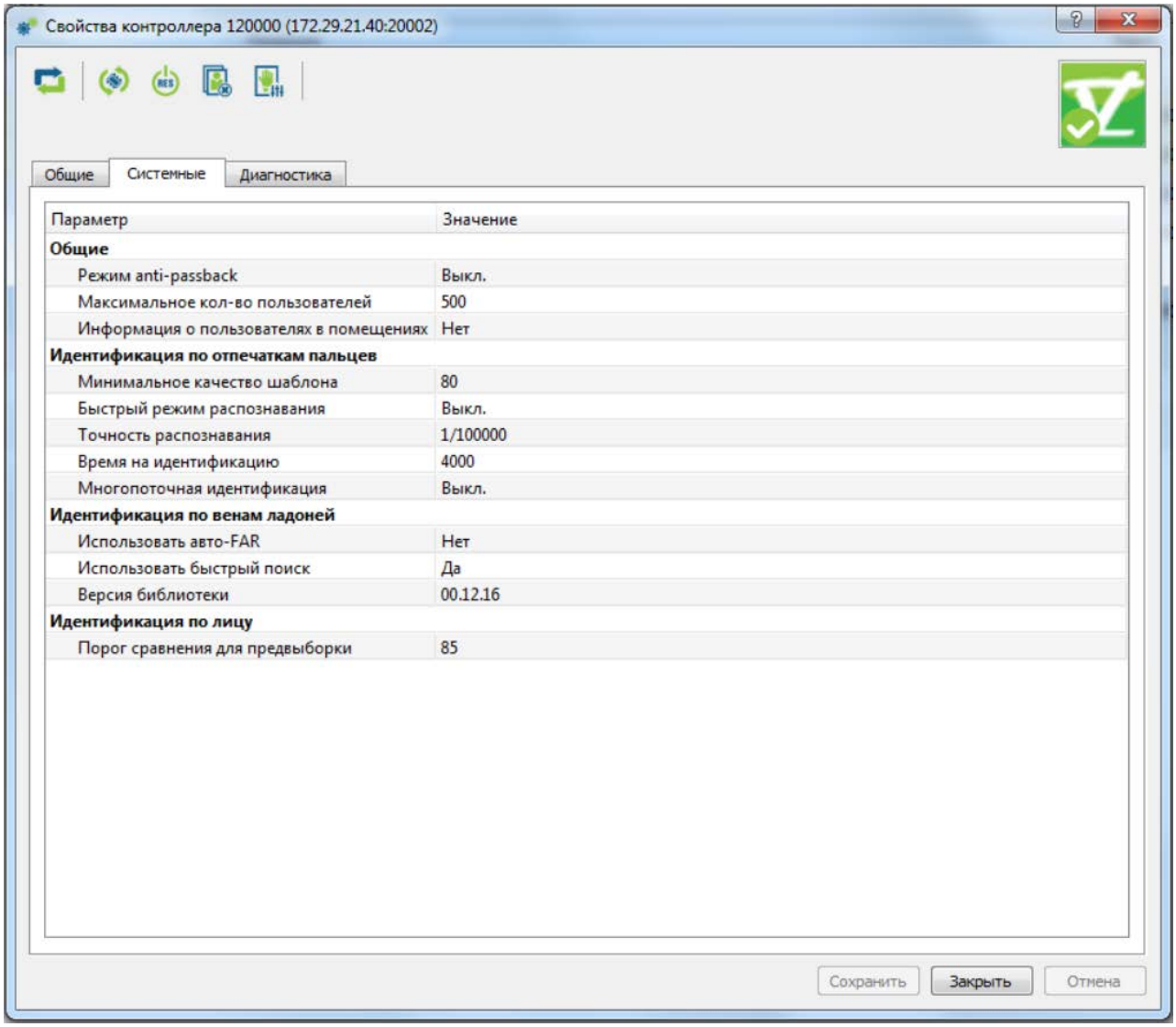


Рисунок 26 — Вкладка «Системные» в свойствах контроллера

Идентификация по отпечаткам пальцев:

- минимальное качество шаблона — настройка задает минимальное качество шаблона, пришедшего с контроллера Biosmart на сервер идентификации, при котором будет осуществляться поиск сотрудника в базе. Если качество шаблона будет меньше, то сервер идентификации сразу отправит контроллеру событие «Идентификация неудачна»;
- быстрый режим распознавания — при включении режима умень-

шается количество контрольных точек для совпадения при поиске шаблона отпечатка сотрудника. Скорость поиска при этом возрастает, но увеличивается вероятность ложной идентификации;

- точность распознавания — системная настройка для работы с базами отпечатков пальцев. Не рекомендуется изменять значение, установленное по умолчанию;
- время на идентификацию — настройка задает время в мс., в течение которого СИ производит поиск шаблона в БД. По истечении данного времени СИ прекратит поиск и отправит контроллеру событие «Идентификация неудачна»;
- многопоточная идентификация — данная настройка позволяет производить параллельную обработку событий на нескольких ядрах процессора. Не рекомендуется изменять значение по умолчанию.

Идентификация по венам ладоней:

- использовать авто-FAR — Автоподстройка FAR. Не рекомендуется изменять значение по умолчанию;
- использовать быстрый поиск — включение программного ускорения поиска. Рекомендуется использовать на базах с большим количеством сотрудников (более 1000);
- версия библиотеки — используемая версия библиотеки математики Biosmart.

В блоке номер 6 представлен интерфейс программы Biosmart v5 в разделе настройки устройств. Интерфейс данного раздела (рисунок 27) представлен следующими составляющими:

1. Панель управления.
2. Список устройств.
3. Свойства устройства.
4. Сервер опроса устройств.

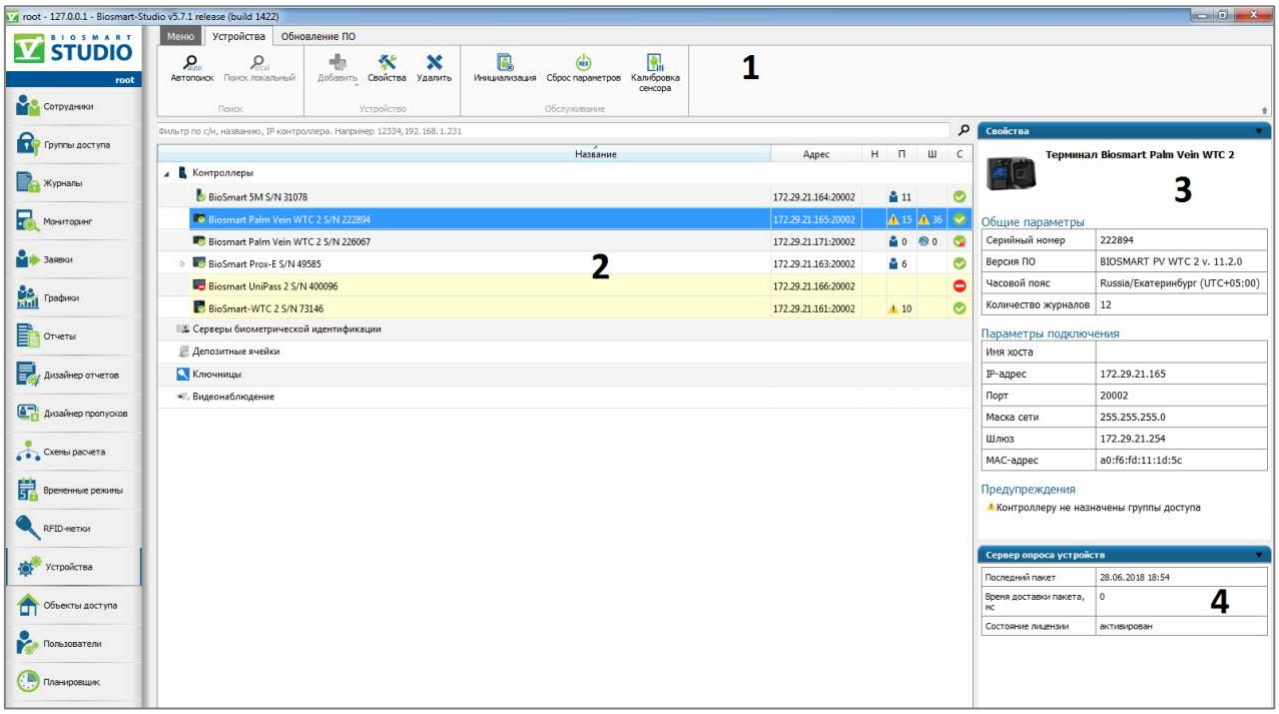


Рисунок 27 — Интерфейс раздела по работе с устройствами

Блок под номером 7 позволяет узнать, как производится поиск и добавление контроллеров идентификации. Быстрее и легче выполнить автоматический поиск устройств в данном сегменте сети. Если сетевые настройки идентификационных контроллеров и сервера идентификации выполнены верно, настроены порты, IP-адреса, маска и шлюз сети, процесс занимает не больше минуты. Автоматический поиск представляет собой широковещательный запрос, направляемый всем устройства Biosmart, находящимся в сети. Для запуска процесса автоматического поиска нажмите «Автопоиск» на панели управления. В окне списка устройств отобразится прогресс процесса поиска. При наличии большого количества устройств в сети, можно воспользоваться фильтром по серийному номеру, типу устройства или IP-адресу. При отметке чекбокса «Инициализировать контроллеры после добавления», выбранные устройства будут проинициализированы после добавления в ПО.

Для добавления устройства в ПО Biosmart Studio v5, выберите его в списке, установив отметку в соотвествующем чекбоксе. После этого, нажмите «Подтвердить» (рисунок 28).

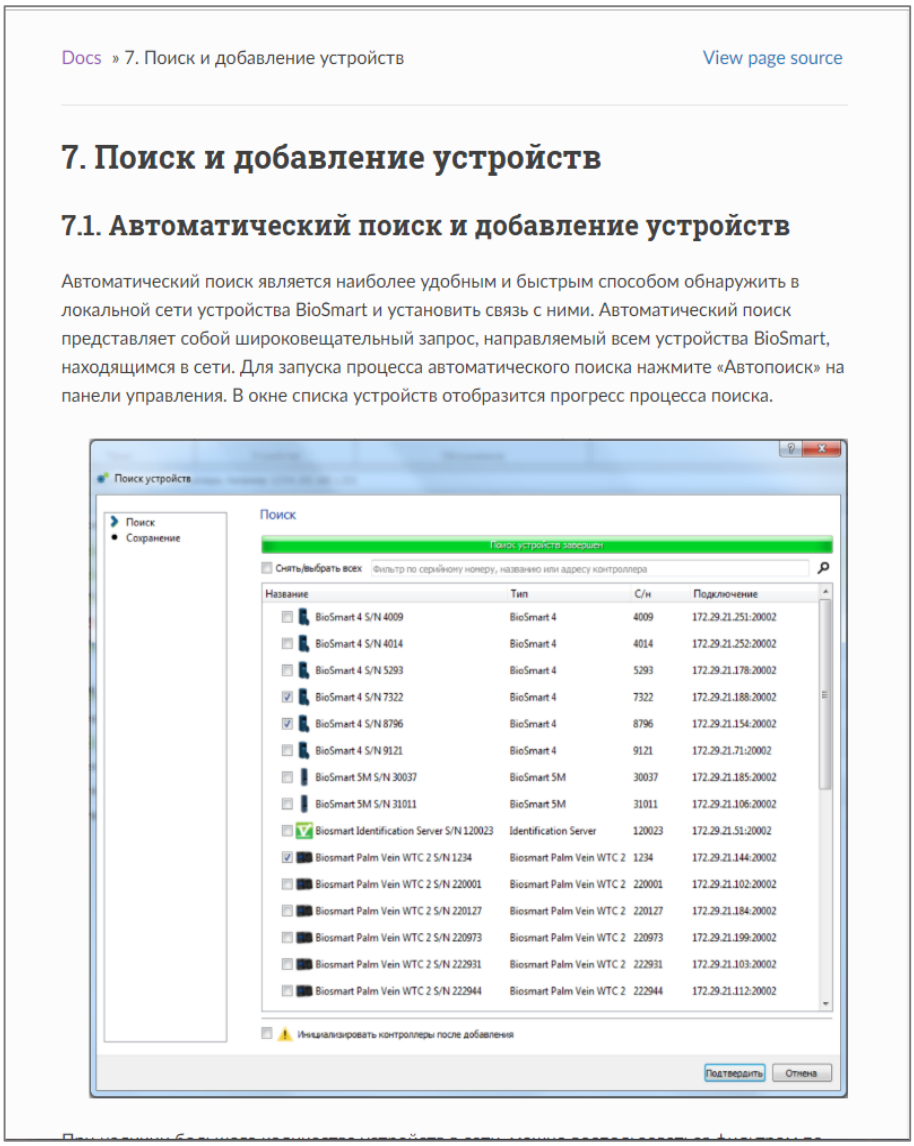


Рисунок 28 — Поиск и добавление контроллеров

Для удаления устройства необходимо нажать кнопку «Удалить». Можно выделить несколько устройств предварительно для удаления их одновременно. После выбора одного или нескольких устройств нужно нажать кнопку «Далее», после чего устройства будут удалены из списка (рисунок 29).

Важно помнить, что для восстановления идентификационных контроллеров в список устройств, необходимо пройти процедуру добавления их с начала. Настройки контроллеров при этом не меняются, так как хранятся в запоминающем блоке устройства.

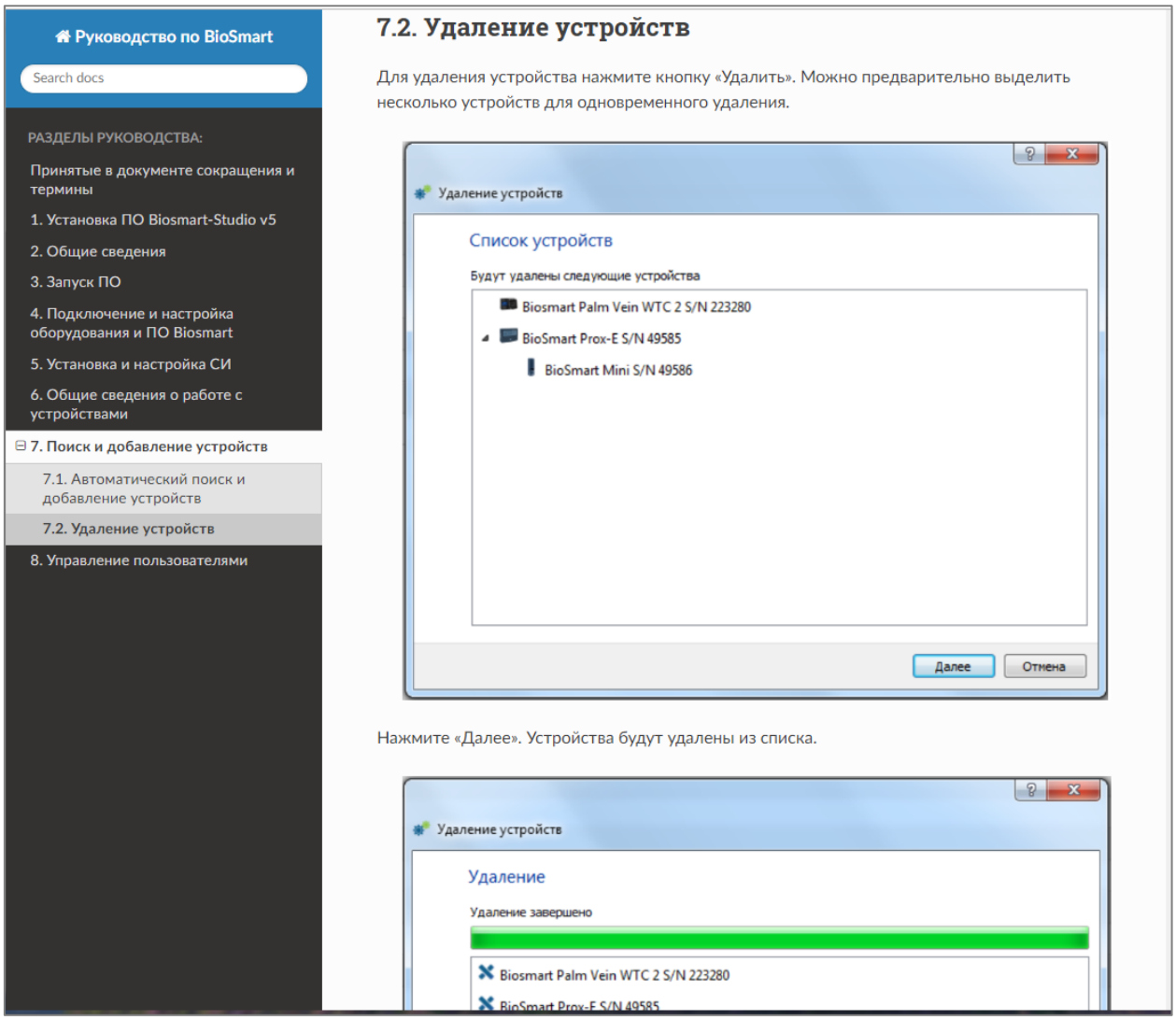


Рисунок 29 — Удаление контроллеров из списка

Блок номер 8 — управление пользователями, делится на два раздела, на добавление профиля пользователя и на добавление биометрической информации пользователя.

При добавлении нового пользователя программы Biosmart Studio v5 необходимо помнить, что права добавляемого пользователя не могут быть выше прав добавляющего, они могут быть либо такими же, либо ниже.

Для добавления нового пользователя нажмите кнопку «Добавить». В открывшемся окне мастера добавления нового пользователя укажите логин, фамилию, имя и отчество пользователя. Нажмите «Далее» (рисунок 30).

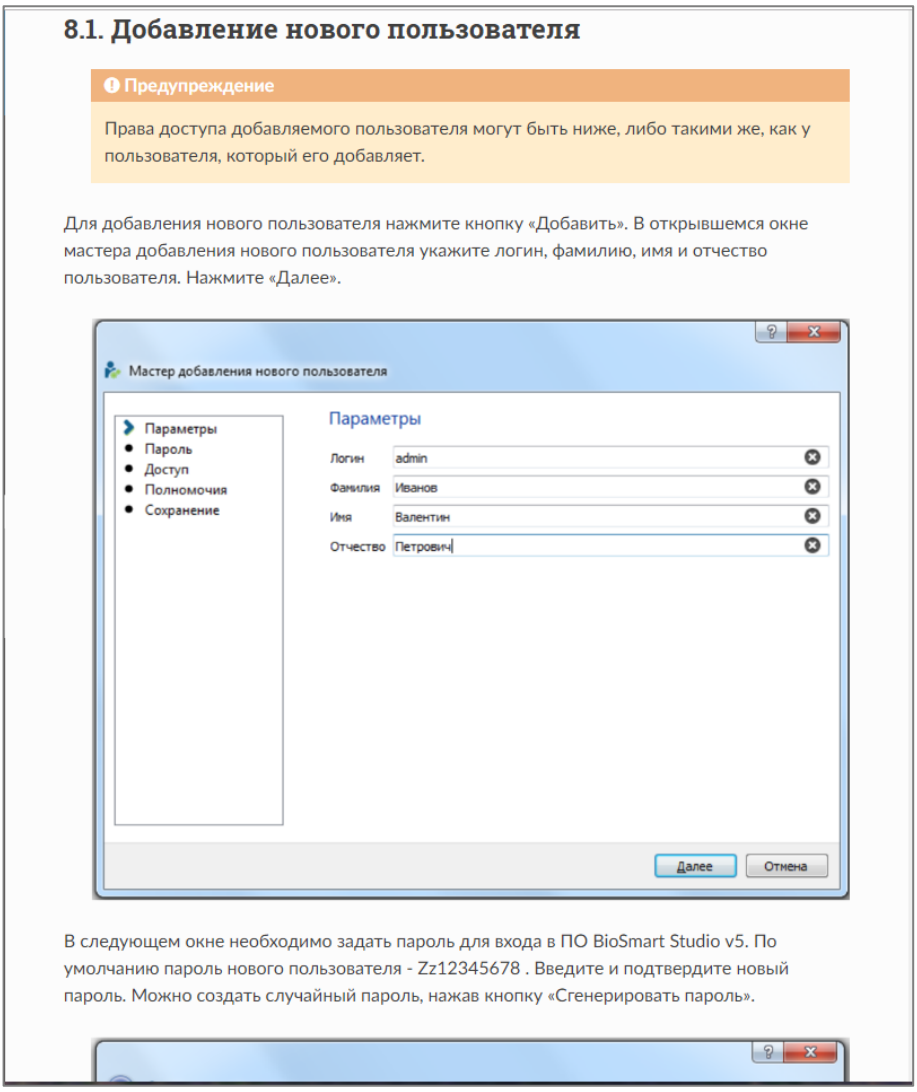


Рисунок 30 — Добавление нового пользователя

В следующем окне необходимо задать пароль для входа в ПО Biosmart Studio v5. По умолчанию пароль нового пользователя — Zz12345678. Введите и подтвердите новый пароль. Можно создать случайный пароль, нажав кнопку «Сгенерировать пароль», находящуюся справа от поля для ввода пароля (рисунок 31). Пароль для пользователя может быть как бессрочным, так и иметь ограничение по сроку действия, по истечении которого пароль необходимо сменить. Выберите в строке «Срок действия пароля» из выпадающего списка дату смены пароля и установите дату, до которой пароль должен быть заменен на новый. При установке параметра «Сменить пароль при первом входе» потребуется изменить пароль при первом входе. Для продолжения нажмите «Далее».

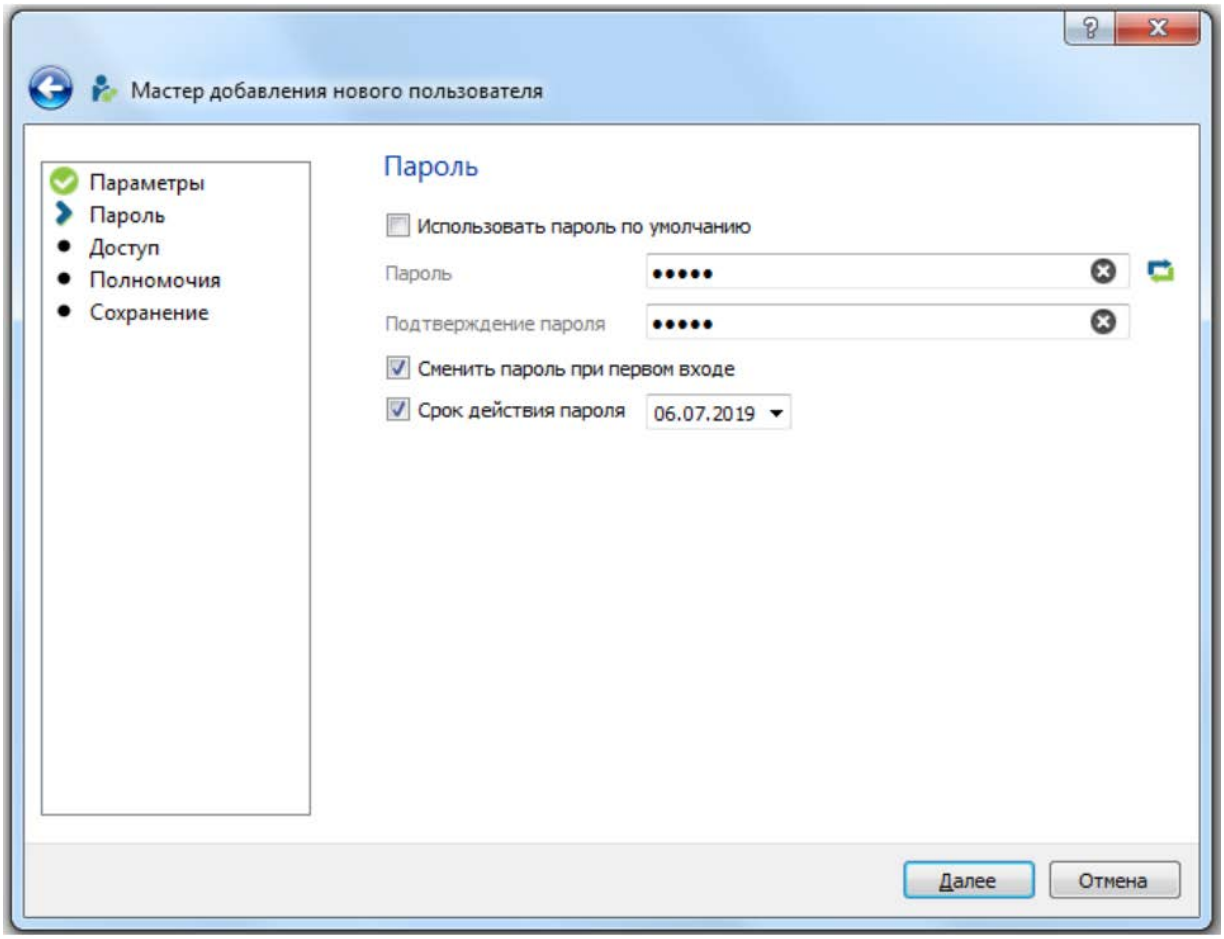


Рисунок 31 — Добавление пароля пользователю

В появившемся окне «Доступ» выберите из выпадающего списка политику идентификации пользователя, как показано на рисунке 32 (логин + пароль, логин + биометрическая информация, логин + пароль + биометрическая информация, пользователь AD). При выборе параметра «Пользователь AD», личные данные пользователя и пароль будут загружены из Active Directory. Для обновления данных пользователя установите параметр «Синхронизировать данные пользователя с AD». Для продолжения нажмите «Далее».

Для внесения биометрической информации пользователя, выберите его в списке пользователей и нажмите кнопку «Сканировать» панели управления. В открывшемся окне проведите сканирование отпечатка пальца или вен ладони. Для регистрации отпечатков откройте вкладку «Сканирование» и нажмите на кнопку «Отпечатки» (рисунок 33).

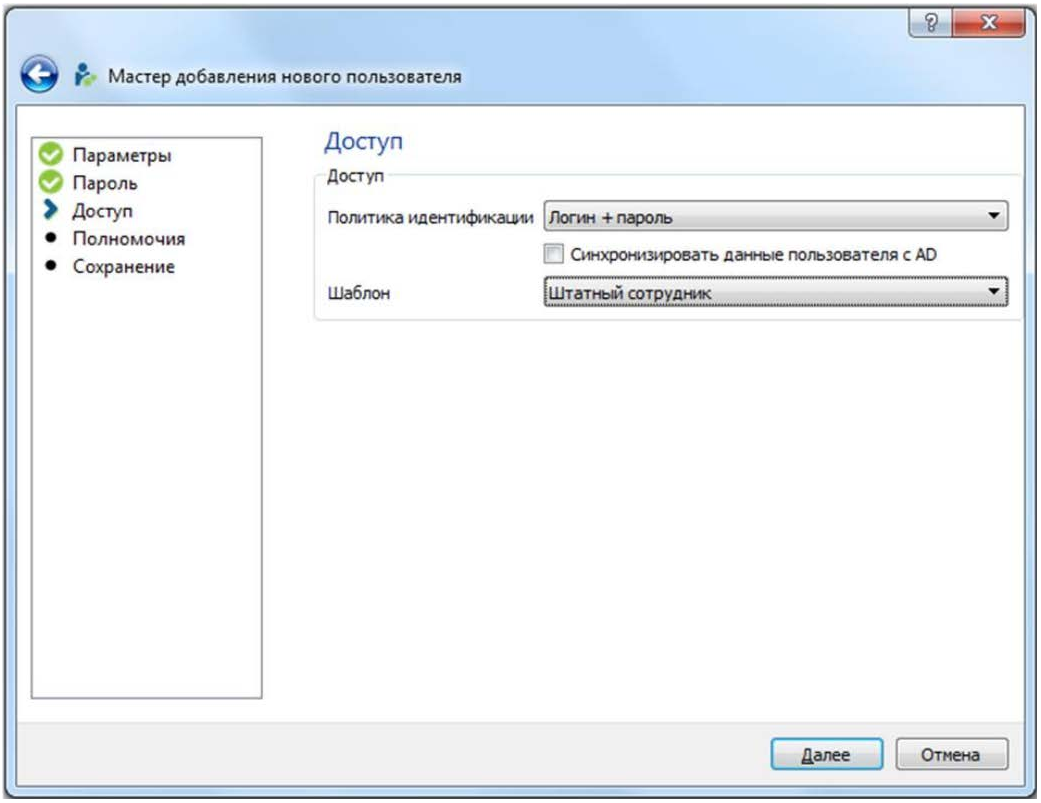


Рисунок 32 — Выбор политики идентификации пользователя

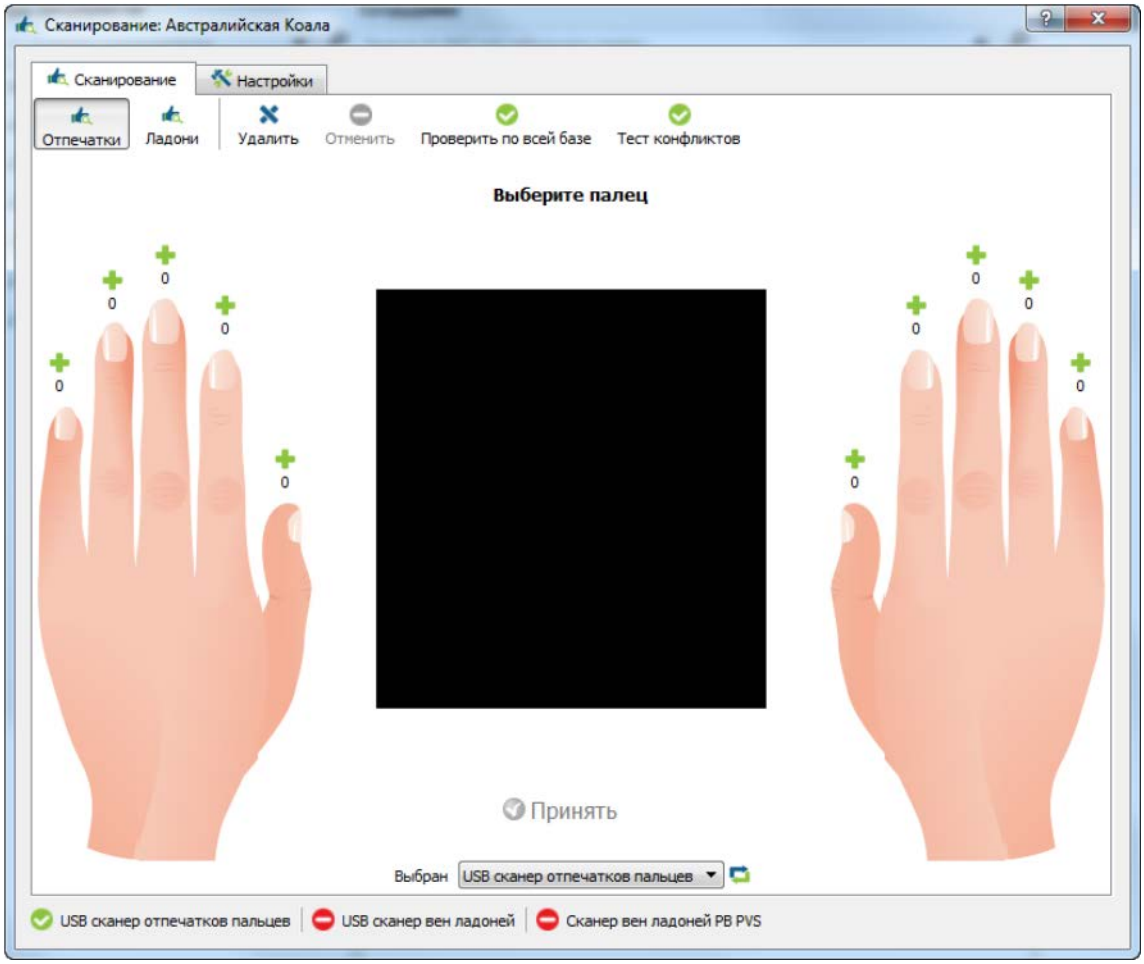


Рисунок 33 — Выбор пальца для считывания отпечатка

Выберите тип устройства, с которого будет производиться регистрация отпечатков пальцев из выпадающего списка. Такими устройствами могут являться настольные считыватели отпечатков пальцев (USB сканеры отпечатков FS-80, FPS150) и считыватели контроллеров или терминалов Biosmart.

Выберите любой палец желательно нерабочей руки (для правши это левая рука), нажмите на плюс около изображения пальца (или на сам палец), шаблон отпечатка которого будет занесен в базу ПО. Появится надпись «Приложите палец к сканеру». При выборе в качестве считывателя USB-сканера отпечатков приложите выбранный палец к сканеру отпечатков пальцев в соответствии с приведенным ниже рисунком 34.

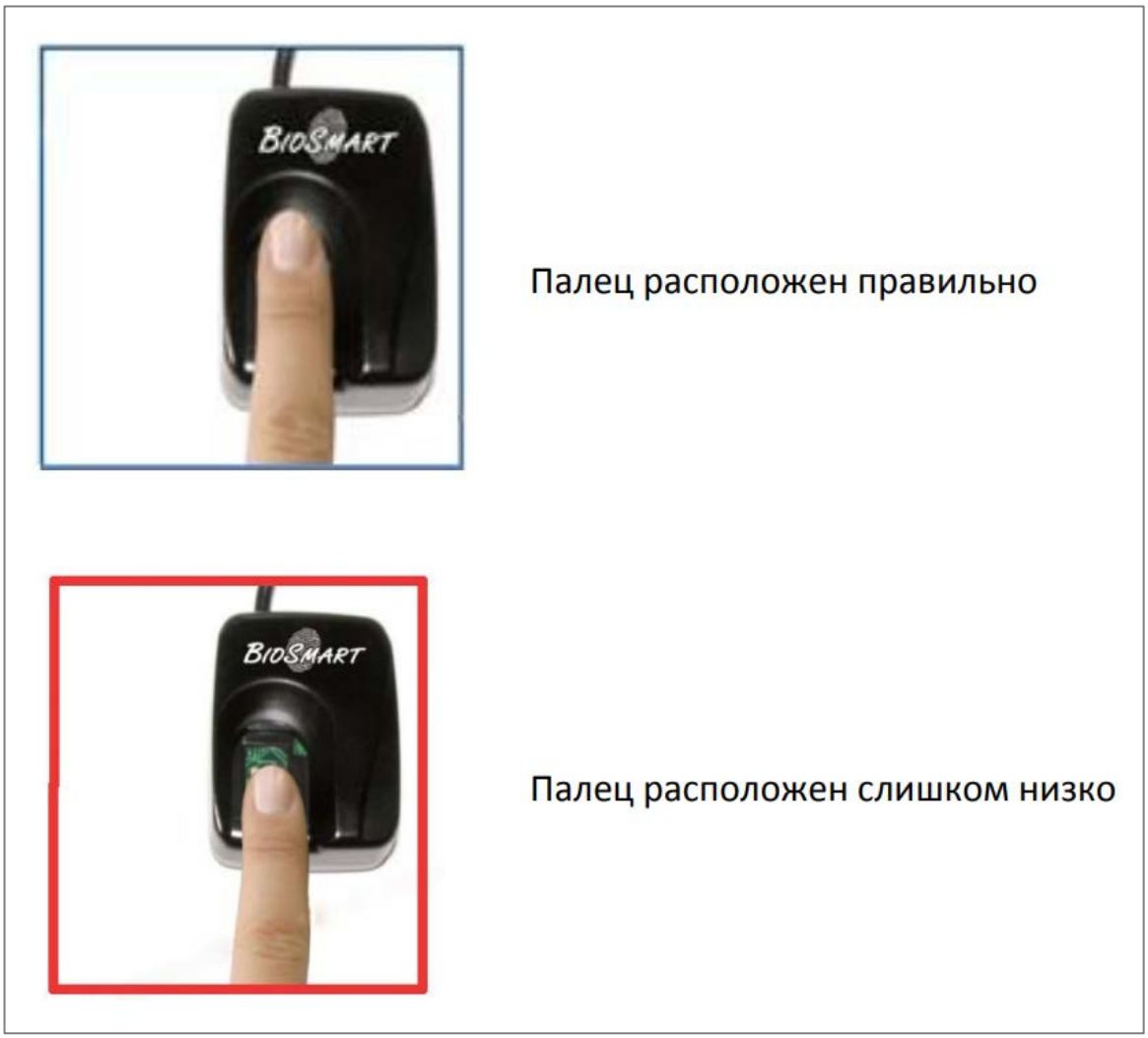


Рисунок 34 — Указания к правильному считыванию отпечатка

При проведении регистрации необходимо контролировать правильность прикладывания пальца к сканеру. При появлении стрелочки возле

изображения отпечатка выполнить смещение пальца в указанном стрелочкой направлении. Появление зеленой рамки вокруг отпечатка означает, что шаблон отпечатка готов к сохранению в базу. В большой рамке отображается текущее изображение отпечатка. В маленькой рамочке отображается изображение отпечатка с наилучшим качеством, полученным системой на данный момент. Необходимо добиться того, чтобы качество изображения (цифра в левом углу) отпечатка в маленькой рамочке было максимально возможным для данного пальца. Визуально оцените, что изображение отпечатка занимает как можно большую площадь в рамке, ядро отпечатка располагается в середине изображения, контрастность линий папиллярного узора высокая. Нажмите «Принять». Успешный результат считывания отпечатка пальца показан на рисунке 35.

Рисунок 35 — Идеальный вариант сканирования отпечатка

Нажмите «Принять». При успешном завершении операции около изображения выбранного пальца появится число занесенных в базу шаблонов его

отпечатка. Вверху окна появится сообщение «Сканирование завершено». Приступайте к занесению в базу шаблонов отпечатков других пальцев, повторив вышеперечисленные операции, или закройте окно «Отпечатки».

Рекомендация: регистрировать один отпечаток в разных положениях (со смещением влево/вправо как показано на рисунке 36).

Рисунок 36 — Варианты смещения пальца при считывании отпечатка

Это повысит вероятность правильного распознавания отпечатка контроллерами и считывателями Biosmart.

ЗАКЛЮЧЕНИЕ

Насколько бы ни был важным фактор информационной безопасности, грамотно организованная система контроля и управления доступом, с использованием современных технологий, покрывает риски несанкционированного физического доступа, несущие в себе не только простой работы банка, но и полную парализацию одного или сети офисов, а то и технического вывода всего банка из рабочего состояния. В этом службе безопасности приходится отличным помощником СКУД, состоящая из контроллеров, предоставляющих доступ на основе идентификации пользователей по биометрическому признаку, либо индукционной карте, и одного или нескольких серверов, управляющих системой.

Мероприятия по внедрению СКУД начинаются на стадии ремонта нового офиса, после прокладки основной локальной сети и предоставлением провайдером выделенного тоннеля для подключения и удаленной настройки оборудования.

В ходе выполнения выпускной квалификационной работы были решены следующие задачи:

1. Проанализирована литература и интернет-источники, посвященная системам контроля и управлению доступа.
2. Изучены возможности систем контроля доступа.
3. Изучен комплекс организационных мер функционирования системы контроля и управления доступом.
4. Реализовано электронное руководство по настройке системы контроля и управления доступом.

Полученное в ходе работы электронное руководство по настройке системы контроля и управления доступом Biosmart может быть использовано для настройки СКУД, при открытии нового офиса, инженерами поддержки информационных систем и ответственными сотрудниками за систему доступа в офисе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Банк АО «Точка» [Электронный ресурс]. — Режим доступа: https://tochka.com/ (дата обращения: 20.12.2018).

2. Бойко Е. В. Объектно-ориентированный подход к созданию электронных учебников [Текст] / Е. В. Бойко // Вестник Красноярского государственного педагогического университета. — 2011. — №2. — С. 39–46.

3. Википедия [Электронный ресурс]. — Режим доступа: http://ru.wikipedia.org (дата обращения: 23.12.2018).

4. Внедрение и развитие систем контроля и управления доступом на предприятии [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/vnedrenie-i-razvitie-sistem-kontrolya-i-pravleniya-dostupom-na-predpriyatii (дата обращения: 10.12.2018).

5. Волхонский В. В. Системы контроля и управления доступом [Текст]: учебник / В. В. Волхонский, В. Д. Волковицкий. — Санкт-Петербург: Университет ИТМО, 2015. — 53 с.

6. Ворона В. А. Системы контроля и управления доступом [Текст]: учебник / В. А. Ворона, В. А. Тихонов. — Москва: Горячая линия: Телеком, 2010. — 272 с.

7. Гитхаб [Электронный ресурс]. — Режим доступа: https://github.com (дата обращения: 02.01.2019).

8. ГОСТ Р 54831–2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний [Текст]. — Введ. 13.12.2011. — Москва: Стандартинформ, 2011. — 20 с.

9. Джхунян В. Л. Электронная идентификация [Текст]: учебник / В. Л. Джхунян, В. Ф. Шаньгин. — Москва: АСТ; НТ Пресс, 2014. — 696 с.

10. Зимина О. В. Печатные и электронные учебники в современном высшем образовании, теория, методика, практика [Текст]: учебное пособие / О. В. Зимина, А. И. Кириллов. — Москва: МЭИ, 2008. — 214 с.

11. Ильина М. А. Электронные учебные пособия, и их важность в учебном процессе [Электронный ресурс] / М. А. Ильина // Информационно-коммуникационные технологии в педагогическом образовании. — 2012. — № 3. — Режим доступа: http://journal.kuzspa.ru/articles/87/ (дата обращения: 10.01.2019).

12. Информационная безопасность для профессионалов [Электронный ресурс]. — Режим доступа: http://Anti-Malware.ru (дата обращения: 24.12.2018).

13. Козлова Е. И. Электронные учебные издания в современном вузе: учебно-методическое пособие [Текст] / Е. И. Козлова. — Москва: Форум, 2013. — 207 с.

14. Лыньков Л. М. Методы и средства защиты объектов от несанкционированного доступа [Текст]: учебно-методическое пособие / Л. М. Лыньков. — Минск: БГУИР, 2011. — 243 с.

15. Марченко А. Л. Актуальные вопросы разработки и использования электронных изданий и ресурсов в обучении электротехнике и электронике в вузе [Электронный ресурс] / А. Л. Марченко. — Москва: ДМК Пресс, 2010. — 272 с. — Режим доступа: http://e.lanbook.com/book/1183 (дата обращения 13.01.2019).

16. Народная база ГОСТов в PDF [Электронный ресурс]. — Режим доступа: http://gostpdf.ru (дата обращения: 20.12.2018).

17. Новые педагогические и информационные технологии в системе образования [Текст]: учебное пособие для студентов вузов. — под ред. Полат Е. С. — 3-е изд., испр. и доп. — Москва: Академия, 2008. — 269 с.

18. Обзор возможностей СКУД [Электронный ресурс]. — Режим доступа: http://www.sistema-dostupa.ru/i03.htm/ (дата обращения: 16.12.2018).

19. Основы биометрии [Электронный ресурс]. — Режим доступа: https://habr.com/ru/post/126774/ (дата обращения: 15.12.2018).

20. Программное обеспечение Biosmart Studio v5 [Электронный ресурс]. — Режим доступа: http://www.bio-smart.ru/product/programmnoe-obespechenie-biosmartstudio-v5 (дата обращения: 12.12.2018).

21. Рабочая программа программного модуля «Применение инженерно-технических средств обеспечения информационной безопасности». Для студентов СПО специальности 100203 — Информационная безопасность автоматизированных систем [Текст] / А. Г. Уймин. — Екатеринбург: ГАПОУ СО «УРТК им. А.С. Попова», 2017. — 28 с.

22. Рыжова В. А. Проектирование и исследование комплексных систем безопасности [Текст]: учебно-методическое пособие / В. А. Рыжова. — Санкт-Петербург: НИУИТМО, 2012. — 157 с.

23. Система контроля и управления доступом. Принцип действия [Электронный ресурс]. — Режим доступа: http://www.intersyst.ru/solutions/165/460/ (дата обращения: 14.12.2018).

24. Современные биометрические методы идентификации [Электронный ресурс]. — Режим доступа: https://habr.com/post/126144/ (дата обращения: 10.12.2018).

25. Сорокин К. Применение биометрических технологий в обеспечении информационной безопасности бизнеса [Текст]: учебник / К. Сорокин. — Москва: Антитерроризм, 2013. — 47 с.

26. Сфинкс документация [Электронный ресурс]. — Режим доступа: https://www.sphinx-doc.org/en/master/contents.html (дата обращения: 20.12.2018).

27. Сфинкс темы [Электронный ресурс]. — Режим доступа: http://www.writethedocs.org/guide/tools/sphinx-themes (дата обращения: 21.12.2018).

28. Тихонов О. О. Функции универсальных СКУД: что нужно потребителю [Текст]: учебное пособие / О. О. Тихонов, А. С. Малышева, А. В. Шаповалов, А. Е. Гамбург, и др. — Москва: Системы безопасности, 2011. — С. 108–119.

29. Торокин А. А. Инженерно-техническая защита информации [Текст]: учебное пособие для студентов, обучающихся по специальностям в обл. инф. безопасности / А. А. Торокин. — Москва: Гелиос АРВ, 2005. — 960 с.

30. Учебный план программы академического бакалавриата [Текст]: утвержден Ученым советом университета 27.06.2016 №10/406. — Екатеринбург: РГППУ, 2016.

ПРИЛОЖЕНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
И.о. заведующего кафедрой

_____ И.А. Суслова
подпись и.о. фамилия

« ___ » _____ 2018 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) *4* курса группы *ЗИБ-401С*

Новикова Антона Владимировича
фамилия, имя, отчество полностью

1. Тема ***Электронное руководство «Настройка системы Biosmart»***

утверждена распоряжением по институту от «_____» _____ 20 г. № ___

2. Руководитель ***Черноскутов Михаил Юрьевич***
фамилия, имя, отчество полностью

–	–	*старший преподаватель*	*РГППУ*
ученая степень	ученое звание	должность	место работы

3. Место преддипломной практики *АО Банк Точка КИВИ Банк*

4. Исходные данные к ВКР *официальный сайт Biosmart, Ворона В.А. Системы контроля и управления доступом*

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов):
проанализировать литературу и интернет-источники, изучить возможности систем контроля доступом, изучить комплекс организационных мер функционирования систем систем контроля доступом, реализовать электронное руководство по настройке системы контроля и управления доступом

6. Перечень демонстрационных материалов *презентация, выполненная в MS Power Point. электронное руководство по настройке системы Biosmart*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	18.12.2018	10%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Анализ проблем	22.12.2018	10%	подпись
2.2	Изучение возможностей систем контроля доступа	24.12.2018	10%	подпись
2.3	Изучение комплекса организационных мер функционирования системы контроля доступа	26.12.2018	10%	подпись
2.4	Разработка электронного руководства	28.12.2018	15%	подпись
2.5	Исправление недочетов конфигурации	30.12.2018	15%	
3	Оформление текстовой части ВКР	03.01.2019	10%	
4	Выполнение демонстрационных материалов к ВКР	07.01.2019	10%	подпись
5	Нормоконтроль	15.01.2019	5%	подпись
6	Подготовка доклада к защите в ГЭК	18.01.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ _____ *Задание получил* _____ _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить ***Новикова А.В.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.
Руководитель _____ _____
подпись дата

10. Допустить ***Новикова А.В.*** к защите выпускной квалификационной работы
фамилия и. о. студента
в государственной экзаменационной комиссии (протокол заседания кафедры от «__» _____ 20___г., № _____)
И.о. заведующего кафедрой _____ _____
подпись дата