МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Политехнический институт: Заочный
Кафедра «Системы автоматического управления»

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой

_____/ В.И. Ширяев

«_____» _____ 2018 г.

Биометрическая система учета рабочего времени

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 09.03.01.2018.897.00 ПЗ ВКР

Руководитель работы

Рук. сект. пр. ООО “НГ-СЕРВИС”

_____/ А. В. Гамов

«____» _____ 2018 г.

Автор работы

студент группы **ПЗ-597**

_____/ А.А. Сигуев

«____» _____2018 г.

Нормоконтролер

Доц. каф. САУ, к.т.н.

_____/ А. А. Брагина

«____» _____ 2018 г.

Челябинск 2018

АННОТАЦИЯ

Сигуев А.А. Биометрическая система учета рабочего времени: ЮУрГУ (НИУ), ПИ: Заочный; 2018, 49 с. 7 ил., библиогр. список – 30 наим., 10 листов слайдов презентации ф. А4.

В работе проведены исследования наиболее эффективных биометрических систем учета рабочего времени в организациях, имеющих разветвленную сеть офисов и представительств. Обоснованы причины внедрения биометрических систем, представлены современные технические средства биометрического контроля доступа к информации, основные технические характеристики, особенности перспективных сканирующих устройств на основе технологии «отпечатков пальцев» на примере предприятия Группа компаний «НГ-Сервис» (далее ГК «НГ-Сервис»). Приведен анализ применения биометрических систем на примере других организаций, представлена система контроля удаленного доступа (СКУД) Biosmart на предприятиях с разной численностью сотрудников и удаленностью объектов.

Предложены современные мероприятия по защите информации.

					09.03.01.2018.897.00 ПЗ			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Сигуев А.А.			Биометрическая система учета рабочего времени	Лит.	Лист	Листов
Провер.		Брагина А.А.				Д	4	52
Н. Контр.		Брагина А.А.				ЮУрГУ Кафедра САУ		
Утверд.		Ширяев В.И.						

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность работы. Для оптимизации рабочего процесса, повышения эффективности труда и соблюдения сроков выполнения задач необходимо планирование и контроль использования рабочего времени.

На сегодняшний день защита информации и контроль рабочего времени играет значительную роль в различных организациях, где речь идёт о финансовой незащищенности, денежных потерях. В связи с этим возрастает популярность биометрических систем, особенностью которых является аутентификация на основе биометрических параметров пользователя.

Под биометрией понимают методы автоматической идентификации человека и подтверждения личности, основанные на физиологических или поведенческих характеристиках. В настоящее время наиболее часто на практике применяются три основных биометрических метода: распознавание по отпечаткам пальцев, по радужной оболочке глаза и по изображению лиц.

Основные цели создания на предприятии биометрических комплексов:

– обеспечение безопасности персонала;

– контроль всей цепочки производственных процессов;

– предотвращение несанкционированного прохождения на объект.

В составе данных комплексов работает система контроля доступа с большим количеством точек прохода и сложной логикой управления доступом в помещения со строгим или ограниченным режимом допуска. На предприятии биометрии реализуются в режиме верификации. Для прохода на охраняемую территорию сотрудник сначала предъявляет карту, а потом свою биометрическую характеристику: отпечаток пальца. Сочетание биометрических технологий с другими системами идентификации позволяет предприятию значительно повышать надежность работы системы контроля и управления доступом, исключать случаи прохода нескольких человек в сопровождении сотрудника, который имеет право доступа в помещение. При выборе биометрической системы для объекта в работе изучены все технические характеристики и результаты тестирования задокументированных характеристик данного решения.

В настоящее время биометрические технологии внедряются во всех странах мира для защиты важной информации, а также в современных системах обеспечения безопасности. Обеспечение конфиденциальности информации говорит об актуальности использования биометрических программных интерфейсов.

Объектом исследования являлось предприятие ГК «НГ-Сервис». В компании пятнадцать отдаленных подразделении находящихся в Челябинске, ЯНАО, ХМАО-Югре.

Подробно рассматривался ценный конечный продукт отдела информационных технологий ГК «НГ-Сервис», текущее состояние, структура опорной системы передачи данных, текущие состояние и изменение ОТ-Инфрастуктуры.

Цель работы - внедрение биометрической системы контроля учета рабочего времени на предприятии.

Для достижения поставленной цели в работе нужно решить следующие задачи:

1. Определить наиболее эффективный способ системы учета рабочего времени сотрудников.
2. Провести анализ наиболее выгодной биометрической системы.
3. Выявить плюсы и минусы по результатам внедрения системы.
4. Осуществить установку, настройку и монтаж оборудования.

1 ОЗНАКОМЛЕНИЕ С ПРЕДМЕТНОЙ ОБЛАСТЬЮ

1.1 Методы контроля рабочего времени

Понятие «рабочее время» означает период, в течение которого сотрудник исполняет трудовые обязанности. Понятие закреплено в статье 91 Трудового кодекса Российской Федерации. Длительность периода зависит от условий трудового контракта, распорядка рабочего дня и внутренних правил компании. Законодательство не запрещает задействовать сотрудников для выполнения профессиональных обязанностей в другое время.

Для оптимизации рабочего процесса, повышения эффективности труда и соблюдения сроков выполнения задач необходимы планирование и контроль использования рабочего времени. Организация рабочего времени также нужна не только подчиненным, но и руководителям. Контроль со стороны компании, руководителя поддерживает необходимую дисциплину в коллективе и гарантирует честную оплату труда.

Руководители больших организаций с большим штатом сотрудников не в состоянии уследить за всеми подчиненными. Кроме функции контроля менеджер, начальник отдела или руководитель проекта исполняет и другие обязанности. Во время работы возникают непредвиденные дополнительные задачи или обстоятельства, не предусмотренные планом, и рабочий процесс полностью угадать и распланировать не удается даже квалифицированным специалистам.

Способы контроля, учета и оценки рабочего времени персонала со временем эволюционировали, и все же организации, особенно государственные учреждения, придерживаются традиционных подходов.

Например, назначают ответственного, табельщика или дежурного, за ведение журнала учета рабочего времени. Сотрудник фиксирует время прихода-ухода и систематически готовит отчеты для руководителя.

При необходимости вводят в штат должность администратора, который будет находиться в одном помещении с коллегами или в отдельном кабинете, и контролировать непрерывность рабочего процесса[4].

Другой способ содержит в себе ведение личной отчетности сотрудников, самостоятельный контроль и своевременное фиксирование израсходованного рабочего времени. Метод оценивает проделанную работу с точки зрения исполнителей и развивает самостоятельность.

Более распространенный способ - установить систему контроля и управления доступом с применением пропусков или сканеров отпечатка пальца. Информация по каждому работнику сохраняется в файле и доступна для просмотра в нужный момент.

Беспроигрышный, но дорогой способ прогноза и учета рабочего времени персонала организации – система видеонаблюдения. Понадобится израсходовать способы не только на покупку и установку видеокамер, но и на заработную плату отдельного сотрудника, в чьи прямые обязанности входит постоянный контроль работы персонала и фиксация нарушений правил внутреннего трудового распорядка. Не считая такого, внедрение системы видеонаблюдения вызывает у служащих психологический дискомфорт от неизменного исследования.

Держать под контролем работу коллектива вручную способен конкретный начальник или же специалист. Но в случае если штат фирмы количество более ста человек, которые работают в подразделениях или удаленно, преодолеть с подобную задачу сложнее, и наиболее удобно при помощи автоматики.

Прогноз работы персонала необходим не только для фиксации результативности труда каждого сотрудника, но и для обеспечения защищенности организации. Автоматические системы укрепляют информацию, проводят тест и формируют отчетность.

Стоимость внедрения автоматической программы мониторинга рабочего времени перекрывается за счет минимизации затрат работодателя, относящихся к отсутствию персонала на рабочем месте, обусловленного прогулами, опозданиями, длительными перерывами. IT-инструменты фиксируют и анализируют данные, на основе которых руководство награждает «передовиков» офиса, тем самым мотивируя весь коллектив работать более продуктивно и дисциплинированно.

Автоматизированные IT-системы позволяют выявить:

– нарушителей дисциплины – сотрудников, которые постоянно опаздывают и уходят раньше положенного времени, курильщиков и любителей кофе, длительность коротких перерывов, которые превышают установленные нормы времени;

– работников, которые в период рабочего дня решают личные вопросы, читают новости и ленты социальных сетей, ведут дружескую, а не служебную переписку, играют на компьютере;

– сотрудников, которые перегружены рабочими задачами и вынуждены систематично задерживаться на работе, что грозит профессиональным истощением и, в крайнем случае, нервным срывом;

– сотрудников, которые не удовлетворены позицией по тем или иным вопросам и заняты поиском новой работы.

Автоматический прогноз рабочего времени не ограничивается аппаратом специализированного ПО и подключает еще установку контрольного оснащения при входе/выходе из здания; оснащение пунктов пропуска; внедрение системы собственных личных номеров для работника; фиксацию передвижения персонала во время работы по территории предприятия с поддержкой GPS-маячков.

Комплексных подход к контролю рабочего времени предполагает анализ работы специалистов по контрольным точкам: штатному расписанию, плану работ, срокам выполнения задач, территории исполнения обязанностей, производственного графика.

При выборе программного обеспечения для учета рабочего времени и оценки эффективности персонала стоит учитывать специализацию решения, с какой целью устанавливается программа: собирать данные или анализировать эффективность работы персонала.

Дальше нужно определить, достаточно ли целей для внедрения программы, которая дает количественные отчеты о приходе-уходе сотрудника, или же потребуется заключение, зафиксирущее, какой деятельностью занимался сотрудник в рабочее время.

Руководители заинтересованы в эффективности не только каждого сотрудника, но и всего коллектива в целом. Чаще всего топ-менеджера интересует не информация, на какие конкретные игры отвлекался сотрудник или с кем именно переписывался, а общее количество времени, потраченное на нерабочие процессы. Поэтому дополнительным преимуществом программы является возможность генерировать не только детализированные, но и сводные отчеты [5].

1.2 Выбор биометрической системы.

В организации ГК «НГ-Сервис» работает более четырехсот человек, поэтому становится сложно учитывать рабочее время сотрудников и вести его учет. Для точного контроля и минимизации затрат времени предлагается установить биометрические системы BioSmart во всех подразделениях компании.

Системы аутентификации сотрудников подразделяются на три группы:

1) Парольная защита.

2) Использование ключей.

3) Биометрия. Пользователь предъявляет параметр, который является частью его самого. Биометрический класс отличается тем, что идентификации подвергается личность человека — его индивидуальные характеристики (рисунок папиллярного узора, отпечатки пальцев, термограмму лица и т. д.).

В работе рассматривается биометрический способ аутентификации

Биометрические системы аутентификации — системы аутентификации, использующие с целью удостоверения личности людей их биометрические данные.

Биометрическая аутентификация — процедура подтверждения и проверки подлинности заявленного пользователем имени через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации.

Их существует несколько видов:

1) Аутентификация по отпечатку пальца.
2) Аутентификация по радужной оболочке глаза.
3) Аутентификация по сетчатке глаза [24].
4) Аутентификация по геометрии руки.
5) Аутентификация по геометрии лица [11].
6) Аутентификация по термограмме лица.
7) Динамические методы.
8) Аутентификация по голосу.
9) Аутентификация по рукописному почерку [8].

Для нашей организации будут рассмотрены две наиболее актуальные системы СКУД: Терминал PV-WTC, Терминал BioSmart-WTC2.

1) Терминал PV-WTC.

В основе работы терминала BioSmart PV-WTC применяется технология получения изображения ладони в инфракрасном свете определенной длины волны. Обедненная кислородом кровь имеет больший коэффициент поглощения инфракрасного (ИК) излучения по сравнению с остальной живой тканью ладони. Благодаря этому, скрытые под кожным покровом вены становятся видимыми при сканировании в ИК области спектра. Полученный рисунок вен уникален для каждого человека.

В области СКУД системы, обеспечивающие или ограничивающие доступ на объект на основе идентификации по венам ладони, появились сравнительно недавно.

Экспертами новинка уже была признана эффективной, поскольку позволила ощутимо повысить безопасность предприятий и иных объектов. Система также была признана более практичной и удобной по сравнению с терминалами, обеспечивающими доступ на предприятие по отпечаткам пальцев или специальным именным картам.

Идентификация по венам ладони основана на сканировании рисунка кровеносных сосудов инфракрасными лучами. Каждый человек обладает уникальным рисунком вен ладони, и по сравнению с отпечатками пальцев, он значительно сложнее. Эти особенности позволяют значительно повысить точность процедуры распознавания.

Данный метод имеет общие черты со СКУД по отпечаткам пальцев, но все же обладает некоторыми неоспоримыми преимуществами:

Распознавание по венам руки не зависит от влажности или загрязнения ладони, тогда как идентификация по отпечаткам может вызвать трудности, если у человека мокрые или грязные пальцы.

Система успешно работает вне зависимости от сезона (рисунок кожи на пальцах может меняться в разное время года или после порезов).

Считается наиболее гигиеничным методом считывания биометрических данных.

Преимущества:

1)бесконтактная идентификация;

2)невозможность фальсификации (рисунок вен ладони виден только в ИК спектре);

3)идентификация не зависит от сухости/влажности и загрязненности ладоней;

4)низкий процент ошибок;

5)высокая надежность;

6)удобство использования.

Стоимость системы BioSmart и экономический эффект от внедрения представлен в таблице 1.1

Таблица 1.1– Затраты и экономический эффект системы

Количество сотрудников на предприятии	400
Средняя ЗП одного сотрудника в месяц, руб.	20 000
Неотработанное время сотрудника, минуты в день	5
Неотработанное время всего персонала, часы в день	9
Переплата за неотработанное время сотрудника, руб. в месяц	210,50
Переплата за неотработанное время по предприятию, руб. в месяц	84 200
Стоимость системы BioSmart , руб.	375 000
Итого: срок окупаемости в месяцах	4,5

2) Терминал BioSmart-WTC2.

Каждый контроллер, работающий по принципу идентификации по отпечаткам пальцев, представляет собой сканер, позволяющий ограничивать доступ в то или иное помещение по физическим характеристикам. Биометрический сканер, благодаря распознаванию отпечатков пальцев, дает возможность:

осуществлять контроль доступа;

выполнять функции учета рабочего времени.

Преимущества системы

Основным преимуществом замков со сканером отпечатка пальцев является полное исключение возможности фальсификации данных. Дело в том, что у каждого человека отпечатки пальцев индивидуальны и не изменяются ни после повреждений, ни с течением времени.

Сканеры надежны и просты в эксплуатации, а универсальность этой технологии позволяет применять данные устройства для решения самых разнообразных задач.

Аппарат имеет вид терминала: он выпускается в прочном корпусе, который оборудован специальным сканером для считывания данных отпечатков пальцев или с бесконтактных карт.

Идентификация по отпечаткам пальцев дает владельцам предприятий широкий спектр возможностей:

1)осуществлять контроль за деятельностью сотрудников;

2)ограничивать доступ работников в определенные помещения;

3)обеспечивает быстрый доступ к необходимым объектам;

4)позволяет централизованно управлять определенными пропускными пунктами из общего центра управления доступом.

Стоимость системы BioSmart и экономический эффект от внедрения представлен в таблице 1.2

Таблица 1.2– Затраты и экономический эффект системы

Количество сотрудников на предприятии	400
Средняя ЗП одного сотрудника в месяц, руб.	20 000
Неотработанное время сотрудника, минуты в день	5
Неотработанное время всего персонала, часы в день	9
Переплата за неотработанное время сотрудника, руб. в месяц	210,50
Переплата за неотработанное время по предприятию, руб. в месяц	84 200
Стоимость системы BioSmart, руб.	280 800
Итого: срок окупаемости в месяцах	3

После проведенного анализа представленных выше систем было принято решение по внедрению СКУД BioSmart-WTC2 по отпечатку пальца.

Основные плюсы данной системы заключаются в экономической выгоде, быстродействии системы и обслуживании. После установки система является автономной.

Цели обработки персональных данных на предприятии:

1. Заключение, исполнение и прекращение гражданско-правовых договоров с гражданами, юридическими лицами, предусмотренных законодательством и Уставом предприятия.

2. Организация кадрового учета организации, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам.

3. Ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами.

4. Исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физлиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование.

5. Заполнение первичной статистической документации в соответствии с Трудовым, Налоговым кодексом и федеральными законами.

Методы биометрии на предприятии

На предприятии, где предъявляются повышенные требования к безопасности, для контроля и управления доступом поставлена задача использования биометрических методов идентификации отпечатка пальца.

1.3 Биометрические системы BioSmart.

Биометрические системы «BioSmart» используются для:

1. Ограничения доступа в служебные помещения
2. Контроля перемещения сотрудников по зданию
3. Автоматического учета рабочего времени сотрудников
4. Постановки и снятия помещений с охраны по отпечатку пальца
5. Ограничения доступа к персональной информации (компьютерам)
6. Ограничения доступа к секретной информации, секретным архивам
7. Автоматизации оплаты питания на предприятии - переход на безналичный расчет с использованием биометрической идентификации.

Применяемые отдельно или используемые совместно со смарт-картами, ключами и подписями, системы могут применяться практически всех сферах экономики и частной жизни.

СКУД BioSmart является сетевой, распределенной системой, с разграничением прав доступа пользователей, при необходимости наращиваемой, открытой для интеграции с оборудованием других производителей. В точках прохода устанавливаются контроллеры, подключаемые к управляющему персональному компьютеру (ПК) или серверу по интерфейсу RS485 или локальной сети Ethernet. Магистраль RS485 организуется при помощи преобразователей (USB-RS485, LAN-RS485, GPRS-RS485). Регистрация пользователей производится в программе BioSmart-Studio. Для регистрации отпечатков пальцев применяется контрольный считыватель, подключаемый через USB порт персонального компьютера. На каждого пользователя можно зарегистрировать до пяти отпечатков пальцев и один код бесконтактной карты формата Em-Marine, Mifare или HID. В базу данных записываются математические шаблоны отпечатков, что делает невозможным обратное воссоздание их графического изображения. Далее пользователю присваиваются права доступа на конкретные точки прохода, информация о пользователе передается на контроллер или сервер идентификации в защищенном виде. Когда пользователь прикладывает палец или пластиковую карту к сканеру, происходит поиск в базе данных зарегистрированных шаблонов. В режиме серверной идентификации, поиск и сравнение шаблонов происходит на внешнем сервере, что увеличивает скорость обработки больших баз данных. При успешной идентификации контроллер генерирует управляющий сигнал на исполнительные устройства (электро-магнитный замок, турникет и пр.). Блок управления реле (БУР) устанавливается внутри помещения, что исключает возможность несанкционированного доступа в помещение путем замыкания проводов или имитации сигнала управления. При успешной идентификации в журнал событий записывается соответствующая информация, используемая в дальнейшем для учета рабочего времени и генерации различных отчетов. Существует возможность вывода всех событий в реальном времени в режиме мониторинга. События неуспешной идентификации или попытки несанкционированного доступа пользователей фиксируются в системе. СКУД BioSmart может работать с внешними датчиками. В системе предусмотрены дискретные входы для подключения выносной кнопки выхода из помещения, датчика открытия двери,

датчика турникета, пожарной сигнализации. Все события по внешним датчикам фиксируются в журнале[14].

Для организации контроля доступа и учета рабочего времени на малом предприятии возможно применение СКУД BioSmart в минимальной конфигурации. Персональный компьютер может использоваться как для регистрации пользователей в системе, так и для ведения журнала событий и формирования отчетов по рабочему времени. Контроллеры подключаются к ПК при помощи преобразователя USB-RS485, да одной линии RS485 одновременно может работать до 32 контроллеров.

На рисунке 1.1 представлена СКУД Biosmart на малом предприятии (численность до 100 человек).

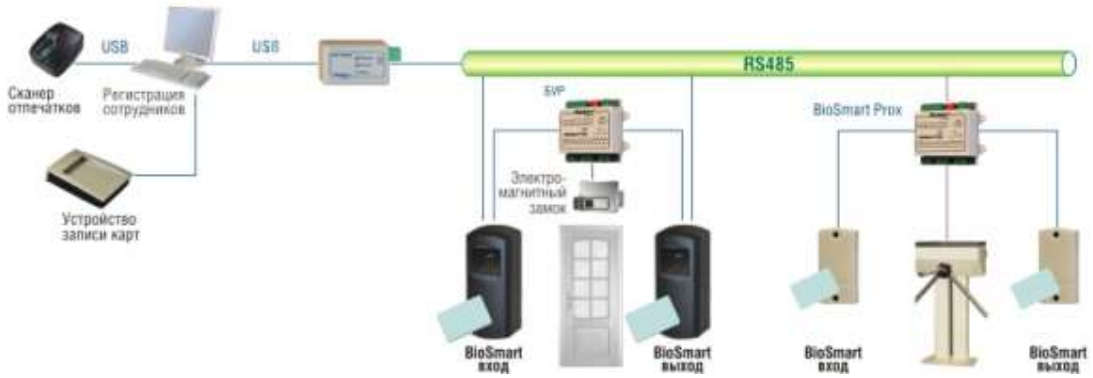

Рисунок 1.1 – СКУД BioSmart на малом предприятии

Особенностью применения СКУД BioSmart на среднем предприятии является использование линии связи RS485 и локальной сети Ethernet. К локальной сети контроллеры могут подключаться через преобразователь LAN-485 или напрямую, при использовании BioSmart со встроенным портом Ethernet. Биометрический терминал BioSmart управляет турникетом, установленным на проходной предприятия, при этом применение терминала с встроенными считывателями бесконтактных карт дает возможность организовать проход сотрудников предприятия по отпечатку пальца, а гостей или посетителей - по пластиковой карте. Отдельные помещения на территории предприятия в зависимости от уровня доступа могут быть оборудованы как биометрическими контроллерами BioSmart, так и контроллерами BioSmart-Prox для работы с бесконтактными картами. Программное обеспечение BioSmartNet-Work и Work-Time позволяет организовать отдельные рабочие места для регистрации пользователей, мониторингу событий в системе (проходная), а также получение отчетов по рабочему времени [21].

На рисунке 1.2 представлена СКУД Biosmart на среднем предприятии (численность до 500 человек).

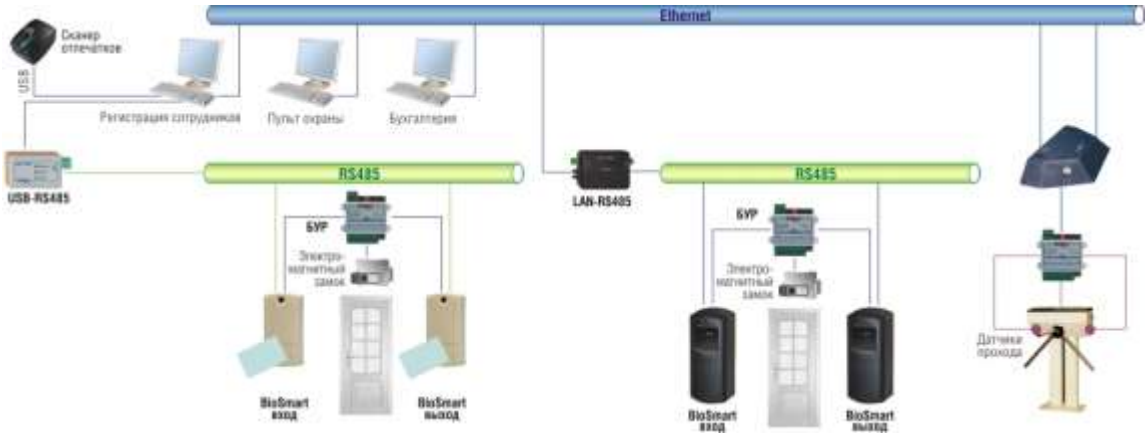

Рисунок 1.2 – СКУД Biosmart на среднем предприятии

При организации контроля доступа и учета рабочего времени при значительной удаленности управляющего ПК или сервера от точек прохода, где применение локальной сети Ethernet или сети Интернет становиться невозможным, можно воспользоваться каналом связи GRPS сотовой сети. Контроллеры Biosmart подключаются при помощи преобразователя GRPS-485, загрузка данных отпечатков и журналов событий производится по GRPS каналу, обеспечивая быструю и недорогую передачу данных на сервер. Количество удаленных точек может быть неограниченным. Для организации контроля за сохранностью оборудования предусмотрены датчики вскрытия корпуса и датчики разряда аккумулятора, при срабатывании которых незамедлительно высылается SMS сообщение на любые 5 телефонных номеров [16].

На рисунке 1.3 представлен Контроль доступа и учет рабочего времени для удаленных объектов.

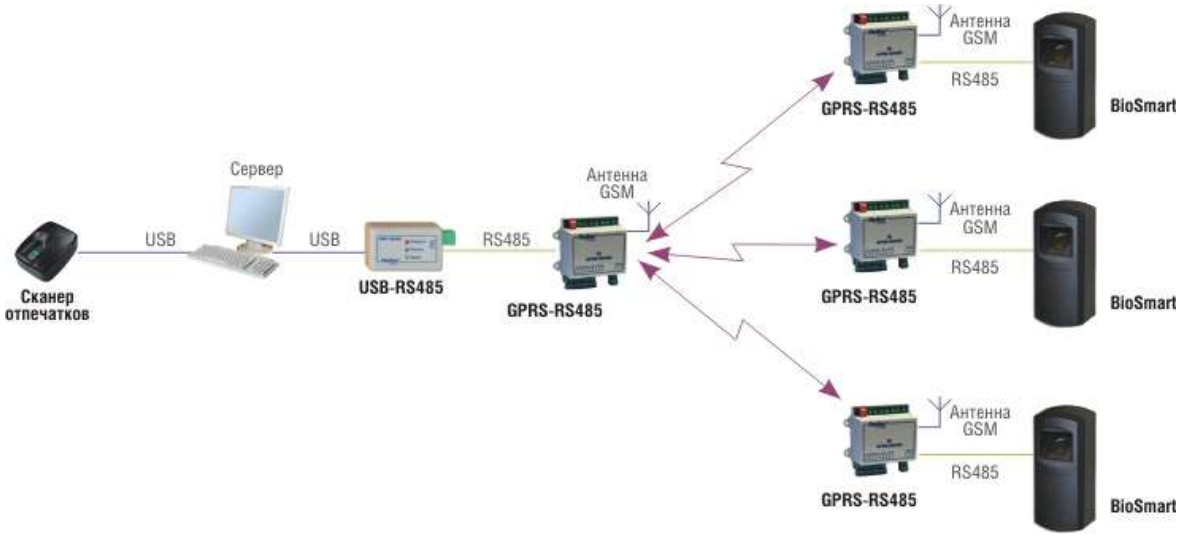

Рисунок 1.3 – Контроль доступа и учет рабочего времени.

1.4 Общая характеристика ГК «НГ-Сервис»

ГК «НГ-Сервис» - компания с высокопрофессиональным персоналом численностью более 400 человек. В группе компаний более 15 подразделений.

Осуществляет следующие виды деятельности:

- оптовая торговля автотранспортными средствами;
- розничная торговля автотранспортными средствами;
- торговля автотранспортными средствами через агентов;
- техническое обслуживание и ремонт легковых автомобилей;
- техническое обслуживание и ремонт прочих автотранспортных средств;
- розничная торговля автомобильными деталями, узлами и принадлежностями через агентов;
- оптовая торговля моторным топливом, в том числе авиационным бензином;
- оптовая торговля лесоматериалами;
- оптовая торговля лакокрасочными материалами;
- оптовая торговля ручными инструментами;
- оптовая торговля синтетическими смолами и пластмассами в первичных формах;
- оптовая торговля эксплуатационными материалами и принадлежностями машин и оборудованием;
- оптовая торговля тракторами;
- деятельность автомобильного грузового транспорта;
- хранение и складирование прочих грузов;
- организация перевозок грузов.
- покупка и продажа собственного недвижимового имущества;
- лизинг;
- коммерческая и посредническая деятельность;
- внешнеэкономическая деятельность.

На предприятии осуществляется учет результатов своей деятельности. Бухгалтерский, оперативный и статистический учет и отчетность ведутся в порядке, установленном действующим законодательством [30].

Ценный конечный продукт отдела информационных технологий:

– бесперебойно функционирующие информационные системы и ИТ-оборудование, обеспечивающие устойчивую и качественную работу ГК "НГ-Сервис";

– инновационные ИТ-решения, предоставляющие конкурентные преимущества, выводящие ГК "НГ-сервис" на новый уровень развития и увеличивающие доход компании.

Внешняя среда в целом неблагоприятна, однако, она дает возможность реализовать стратегию дифференциации:

– предложения отличных от конкурентов услуг и продуктов;

– повышения лояльности клиентов;

– уникальные для рынка региона средства коммуникаций с клиентами.

Внутренняя среда требует изменений, при этом следует основные усилия направить на:

– построение системы менеджмента качества по стандарту ИСО 9000;

– повышение эффективности бизнес-процессов;

– повышение прибыльности бизнеса за счет оптимизации операционной деятельности.

На рисунке 1.4 - представлена структура опорной сети передачи данных ГК НГ сервис:

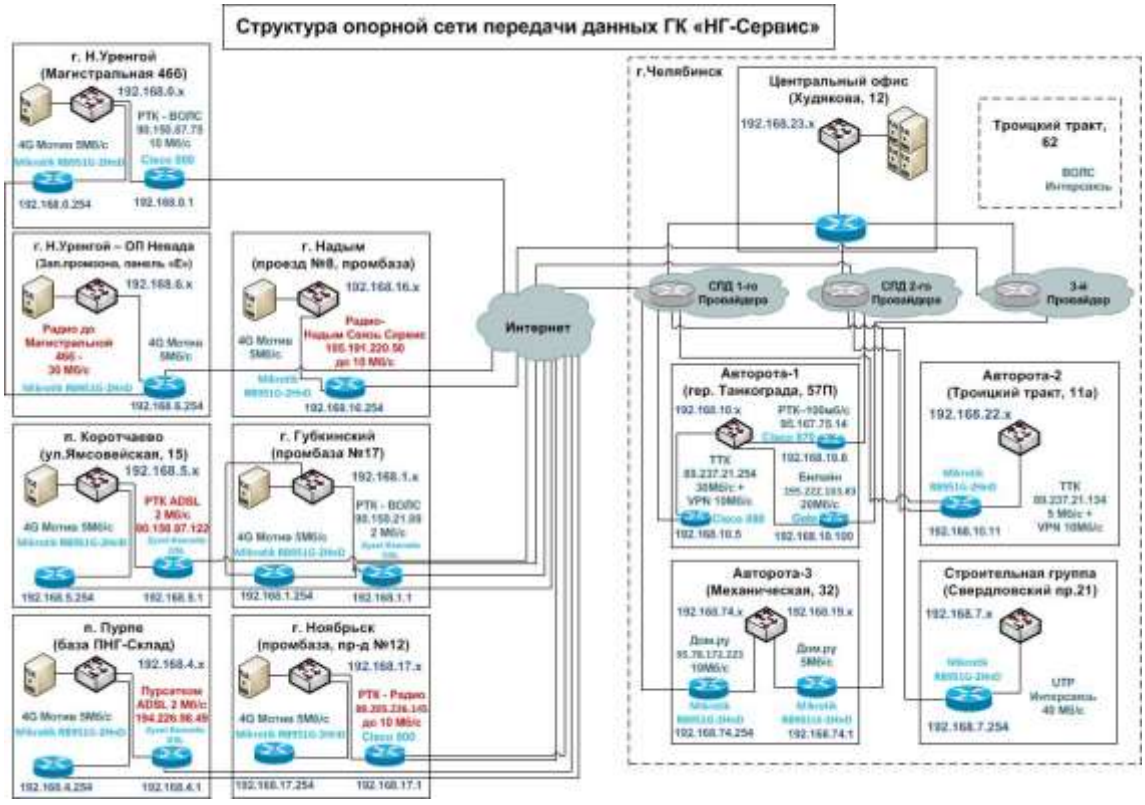

Рисунок 1.4 – Структура опорной сети передачи данных ГК «НГ-Сервис»

Текущие состояния и изменение Инфраструктуры:

Система учета рабочего времени:

Подключены к системе и установлены биометрические считыватели:

- Обособленное подразделение (ОП) Коротчаево;
- ОП Губкинский;
- ОП Надым;
- Система видеонаблюдения:
- ОП Н.Уренгой – установлен сервер видеонаблюдения и новые IP камеры;
- Сервисный центр Полярник – заменен видеорегистратор и устанавливаются новые камеры;
- Дилерский центр УАЗ – заменен видеорегистратор и устанавливаются новые камеры;

Резервное копирование и восстановление данных модернизация сервера хранения резервных копий.

Существующая ИТ-инфраструктура обеспечивает необходимый уровень автоматизации для решения текущих задач, однако для повышения производительности труда требуется модернизация еще около 18 % рабочих мест.

ИТ-инфраструктура имеет ряд уязвимостей для функционирования бизнеса:

- низкий уровень резервирования не позволяет оперативно проводить замену неисправного оборудования и приводит к простоям;
- отсутствие системы резервирования электропитания и кондиционирования приводит к остановке работы подразделений в случае отключения/ повреждения внешних сетей электропитания.

Краткосрочные и долгосрочные цели модернизации процесса ГК «НГ-Сервис»:

- локальная вычислительная сеть в каждом ОП;
- описание работы телефонии;
- календарь регламентных процедур;
- база знаний (описание повторяющихся процедур и известных инцидентов):
- штатная процедура приема/увольнения сотрудника;
- инструкции для пользователей по работе с компьютером, программами (интернет, почта, spark и др.), оборудованием (принтеры, телефоны) и расходными материалами.

2 ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКИХ СИСТЕМ BIOSMART НА ПРЕДПРИЯТИИ

2.1 Технические характеристики системы BioSmart

Системы контроля доступа к информации BioSmart базируются на регистрации такого индивидуального признака человека, как отпечаток пальца руки. Записываемый в виде контрольного образа трехмерный отпечаток пальца сканируется оптической системой, анализируется, оцифровывается, хранится в памяти терминала или в памяти управляющего компьютера и используется для проверки каждого, кто выдает себя за авторизованного пользователя. При этом в памяти устройства не содержится реальных отпечатков пальцев.

Типичное время занесения в память одного контрольного отпечатка пальца составляет 30с. Каждый занесенный в память терминала авторизованный пользователь набирает PIN-код на клавиатуре терминала BioSmart и проходит стадию проверки идентичности, занимающую приблизительно 0,5-2с. Под одним PIN-кодом обычно хранится образец отпечатка одного пальца, но в некоторых случаях возможна аутентификация по отпечаткам трех пальцев. При совпадении предъявляемого и контрольного отпечатков терминал подает сигнал на исполнительное устройство: шлюз и т.д [29]..

Характеристики работы BioSmart:

- работа в среде Windows;
- управление информационными файлами;
- совместимость формата файлов баз данных пользователей и событий с MicrosoftAccess;
- запись всех файлов временных событий в формате ASCII;
- наличие постоянного окна сообщений о событиях в системе;
- контроль исполнительных устройств;
- активация/деактивация пользователей;
- многоуровневая авторизация;
- наличие временных зон;
- список пользователей на каждую дверь;
- ведение журналов сообщений по событиям в системе с установкой фильтров [15].

Разработчиком терминала BioSmart, является фирма Прософт-Биометрикс. Она так же разработала программное обеспечение BSManager, которое, в свою

очередь, контролирует доступ к рабочим станциям и серверам Windows NT, а также к соответствующим ресурсам, защищаемым парольной системой Windows NT. При этом у системного администратора остается возможность использовать свой обычный (не BIO-ключ) пароль, зарегистрированный в Windows NT.

Далее рассмотрим технические особенности BioSmart:

- LCD дисплей 3.5”;
- встроенная кодонаборная панель;
- встроенный считыватель карт;
- возможность работы в режиме серверной идентификации;
- возможность регистрации отпечатков и пластиковых карт с экрана терминала;
- возможность конфигурирования устройства с экрана терминала;
- USB порт для конфигурирования устройства;
- возможность загрузки собственного фонового рисунка экрана;
- WEB интерфейс для конфигурирования параметров;
- поддержка POE.

Опциональные дополнения:

- встроенный считыватель пластиковых карт стандарта Mifare;
- встроенный считыватель пластиковых карт стандарта HID iClass;
- встроенный считыватель пластиковых карт стандарта HID Prox;
- встроенный считыватель пластиковых карт стандарта Legic[28].

Технические характеристики BioSmart «Биометрического консолера» (оптический считыватель) и ПК (контрольный считыватель):

- разрешение рабочей поверхности 508 dpi;
- размеры рабочей поверхности сканирования 16×24 мм;
- размер отсканированного изображения 480x320 мм;
- температурный диапазон от 0 до +55 °C;
- напряжение питания через USB порт DC 4.45.25;
- вес 80 г;
- скорость передачи данных 6 Мбит/сек;

2.2 Внедрение биометрической системы учета рабочего времени на предприятие ГК «НГ-Сервис»

Обычно организации внедряли системы учета рабочего времени с помощью пластиковых карт, однако данная система не защищена от обмана: когда,

например, работники передают карты друг другу для симуляции своего нахождения на рабочем месте, при эксплуатации таких систем постоянно приходится сталкиваться с тем, что карты теряются, ломаются или просто забываются. Каждый подобный инцидент оборачивается потерей эффективного рабочего времени и/или необходимостью перевыпуска карты.

Важная роль в достижении эффективной работы предприятия, принадлежит внедрению биометрической системы учета рабочего времени сотрудников. BioSmart позволит предприятию организовать: систему контроля и управления доступом, предотвратить несанкционированный доступ в центральный офис и подразделения [26].

Биометрические системы лишены перечисленных недостатков. Работник не может передать, потерять или забыть дома свои отпечатки пальцев. От возможной «порчи» отпечатков (порезов, ожогов) система защищена тем, что в ее базу можно заложить несколько отпечатков пальца одного человека.

В данный момент ГК «НГ-Сервис» - компания с высокопрофессиональным персоналом численностью более 400 человек. В группе компаний более 15 подразделений.

Цель отдела технической поддержки:

- внедрение системы контроля и управления доступом;
- разработка, производство и внедрение средств обеспечения информационной безопасности;
- разработка, производство и внедрение комплексных решений для идентификации пользователей финансовых, платежных и других систем массового обслуживания;
- разработка математических алгоритмов для распознавания личности;
- разработка, производство и внедрение систем учета рабочего времени сотрудников на предприятии;
- открытая интеграция производимых систем с продуктами сторонних производителей, предназначенных для обеспечения комплексной безопасности зданий и сооружений.

Основными функциями учета рабочего времени сотрудников являются:

- автоматизированный учет времени прихода и ухода сотрудников;
- ведение табеля рабочего времени по форме Т-13;
- создание отчетов о наличии или отсутствии сотрудника на рабочем месте, об опозданиях и ранних уходах;

– создание и ведение базы данных сотрудников (электронная картотека);

– Импорт данных в программу MicrosoftExcel;

– 1С-Бухгалтерия версии 7.7, 8.1, 8.2 и так далее [25].

ГК «НГ-Сервис» имеет разветвленную сеть офисов и представительств, поэтому в ходе внедрения выяснилось, что биометрические устройства - единственный абсолютно надежный вариант контроля. Организация установила у себя систему учета рабочего времени BioSmart для того, чтобы контролировать работу сотрудников подразделений в других городах. Так как сотрудники находились на значительном расстоянии от руководства, они оставались абсолютно неконтролируемыми.

Принцип работы системы прост: сканер отпечатков пальцев установлен на входе в здание, система управляет дверными замками, обеспечивая доступ на территорию предприятия только зарегистрированных сотрудников. Придя на работу, сотрудник прикладывает палец к сканеру, то же самое он делает, уходя на перерыв или по окончании рабочего дня. Распознав сотрудника, система заносит информацию о его передвижениях в «журнал событий» СКУД BioSmart (ошибки, подтасовки и злоупотребления исключены). СКУД BioSmart передает информацию на общий сервер в режиме реального времени. Это позволяет кадровому специалисту постоянно иметь актуальную информацию о нахождении сотрудников на рабочих местах. Для связи датчиков с головным компьютером используются беспроводные каналы связи - выделенные линии Ethernet, уже существующие на предприятии [10].

Использование BioSmart позволило:

– уменьшить количество персонала за счет сокращения охраны на проходной и нормировщика, который производит подсчеты отработанных часов;

– получать достоверные данные о времени входа и выхода работников;

– производить автоматический ввод данных в табель рабочего учета;

– повысить производственную эффективность за счет улучшения дисциплины и отсутствия работников в рабочие периоды.

Минусами биометрического учета являются:

– налаженность данного метода, установка, дальнейшее обслуживание, и управление должно быть высокопрофессиональным;

– высокая стоимость оборудования.

Решение о вводе биометрического учета рабочих часов должно иметь обоснования не только в виде приказа руководства. Перед внедрением

терминалов было получено письменное согласие от каждого трудящегося на предприятии. Федеральный закон № 128 указывает на то, что сдача отпечатков — мера добровольная, и принудить к этому человека никто не имеет права.

На основании написанных согласований был издан приказ по организации, в котором указаны:

- основание внедрения новшества;
- дата начала нового учета;
- распоряжения в бухгалтерию о новых правилах при расчете зарплаты;
- распоряжение об обязательности ознакомления каждого сотрудника под роспись;
- возложение ответственности за контроль.

К приказу прилагается полный перечень сотрудников, в котором каждый из них поставил личную подпись.

С внедрением биометрического контроля точно известно, кто хронически опаздывает, кто склонен уходить раньше или работает сверх нормы. Система гарантирует точность информации, не привлекая другие ресурсы бизнеса.

Терминал BioSmart способен хранить огромную базу, содержащую досье на каждого работника компании. Досье включает в себя время прихода и ухода, количество и частоту опозданий, число отгулов, больничных, график командировок, а также другие данные, необходимые для знания всего, чтобы лучше узнать подчиненного.

С внедрением данного комплекса получены положительные эффекты:

- из-за технической простоты обслуживания биометрической информации учет ведется быстрее;
- вся информация находится в одном месте, поэтому для составления отчета нет необходимости синхронизировать разные программы;
- мгновенное получение ответа на запрос, касающийся кого-либо из персонала;
- программное обеспечение адаптационно к любому компьютеру, данные в удобном формате (например, с расширениями xls, pdf), что позволяет быстро составить отчет, графики, схемы, легко и быстро найти требуемую информацию, осуществить обмен сведениями с другими программными продуктами, например, с 1С7 или 1С8 [18].

2.3 Техническое решение

В каждом подразделении предприятия ГК «НГ-Серис» установлен персональный компьютер с монитором, через которые выводится подробная информация о сотруднике, поднесшем идентификационную карту или палец к считывателю «ВХОД» или «ВЫХОД». Система оснащена источниками бесперебойного питания, позволяющими осуществлять беспрерывный учет сотрудников при полном отсутствии электроэнергии до двух часов.

Структурная схема учета рабочего времени ГК «НГ-Сервис» (рис. 2.1) иллюстрирует основное оборудование установленных систем видеонаблюдения и контроля.

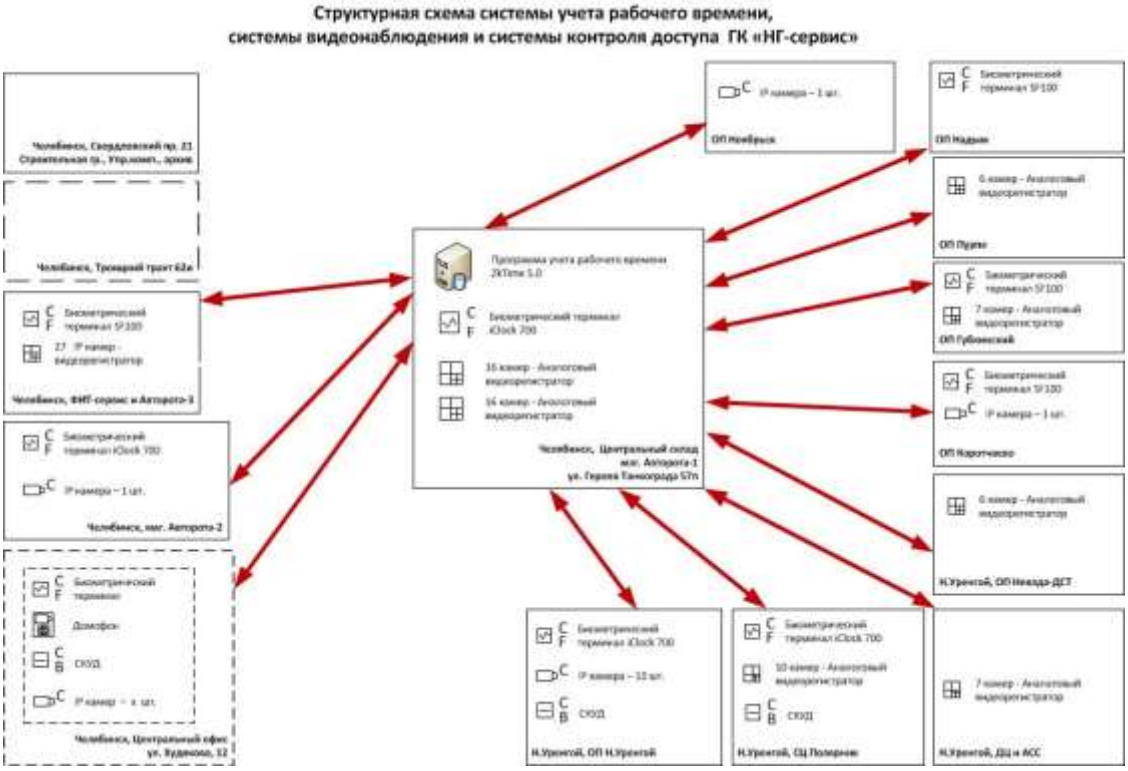

Рисунок 2.1 – структурная схема системы учета рабочего времени, системы видеонаблюдения, системы контроля доступа ГК «НГ-сервис»

В специальном помещении оборудована комната для фотографирования сотрудников и выпуска карт доступа.

Станция администрирования СКУД представляет собой персональный компьютер с доступом в заводскую сеть [23].

В Таблице 2.1 представляется спецификация оборудования и программного обеспечения

Таблица 2.1

№п/п	Наименование	Количество
1	Стандартное оборудование	
1.1	PCHPIntelCore 2 DuoT(4×4) E6420-2.13 (1066) (4)/1024/160-SATA/	7
1.2	Монитор L171p Black 17», 0,264, TCO-03, 1280×1024, 76Hz	7
1.3	Сетевой фильтр	7
1.4	APC Smart-UPS 5000VA 3750W	4
1.5	ИБП Smart-UPS 1000VA USB w/PowerChute+	6
1.6	Switch D-Link DGS-1008D 8port 10/100/1000Mbps Autosensing, Unmanaged, desktop	7
1.7	ТриподVelbon CX -460 для фотоаппарата	2
1.8	Фотоаппарат CANON S5 (с двумя комплектами зарядных устройств)	2
2	Специальное оборудование	
2.1	Proximity карты для регистрации в системе и для прохода через турникеты (тонкие)	1500
2.2	Считыватель	9

2.4	Мост microlan-ethernet	6
2.5	Контроллер управления турникетом (контроллер считывателя карт).	8
2.6	Принтер SP35 для Proximity карт цветной	2
2.7	Расходные материалы для принтера из расчета на 1 карту	1500
2.8	Роторный турникет ОМА-16.581 с увеличенной высотой до 1500 мм	4
3	Программное обеспечение	
3.1	Программное обеспечение «Система учета рабочего времени и Пропускная система»	3
4	Работы	
4.1	Шефмонтаж системы (совместно с представителями)	2
4.2	Сервисное обслуживание в течение 1 года	1

В работе разработано следующее руководство пользователя СКУД с описанием терминологии и этапов функционирования системы:

Система контроля доступа и учета рабочего времени предназначена для контроля перемещений персонала, как по охраняемой территории, так и при пересечении ее границы.

Каждый пользователь снабжается личной идентификационной картой, а на входах и выходах с соответствующей территории (территории предприятия, здания, помещения и т. д.) устанавливаются специальные считыватели – контрольные точки.

На контрольной точке сотрудник предъявляет пропуск (подносит идентификационную карту к соответствующему считывателю). Информация поступает на сервер системы, где фиксируется время входа или выхода сотрудника из помещения или с территории предприятия. Кроме того, информация о пересечения сотрудником контрольной точки и его фотоизображение поступает на пульт охраны для визуального контроля.

На основании полученной информации на сервере системы формируются отчеты о времени нахождения сотрудника в том или ином здании, помещении или на территории предприятия и отчеты о рабочем времени.

Пропуск – индивидуальная идентификационная карта, выданная сотруднику предприятия и зарегистрированная в системе.

Контрольная точка – вход в помещение или выход из помещения, оборудованный считывателем идентификационных карт.

Несоответствие событий – несоответствия событий устанавливаются на основании набора предыдущих событий и подразделяются на:

– неожиданный вход – сотрудник должен находиться в определенном помещении, но в системе регистрируется событие о том, что он вошел в другое помещение. Например, сотрудник не зарегистрировался при выходе из территории и снова заходит на территорию предприятия – двойной Вход. Причина – сотрудник не раз регистрировался в предыдущем помещении;

– неожиданный выход – сотрудник должен находиться в определенном помещении, но в системе регистрируется событие, что он вышел из другого помещения, в котором не должен был находиться. Например, сотрудник не зарегистрировался при входе на территорию предприятия и выходит из территории предприятия. Причина – сотрудник не зарегистрировался при входе в помещение;

– незавершенный промежуток времени (при определенных условиях) – если сотрудник находится в помещении, то промежуток времени с момента последнего события до текущего момента считается незавершенным. Как только будет зарегистрировано какое-либо событие, система получает достаточно информации для определения, существует ли несоответствие, или несоответствий нет. Причина – сотрудник не разрегистрировался при выходе с территории предприятия.

Формы отчетности в программном обеспечении СКУД BioSmart: данные о рабочем времени сотрудников автоматически заносятся, например, в бухгалтерские базы данных и используются для начисления зарплаты или

наложения взысканий. Для удобства бухгалтерии или кадровой службы вся информация может передаваться непосредственно в программы MS Excel, 1С-Бухгалтерия. В программном обеспечении BioSmart предусмотрен раздел «Мастер составления отчетов». С его помощью можно создать форму отчетности удобную для кадровика, руководителя. Например, можно автоматически формировать отчеты о рабочем времени, об опозданиях, ранних уходах, больничных, о текущем присутствии сотрудников на рабочих местах.

3 РАБОТА СИСТЕМЫ BIOSMART НА ПРЕДПРИЯТИИ

3.1 СКУД BioSmart. Алгоритм работы.

На предприятии устанавливается система СКУД BioSmart, производитель ПРОСОФТ БИОМЕТРИКС, город Екатеринбург.

СКУД BioSmart отвечает всем современным требованиям, предъявляемым к таким системам, включающим высокий уровень безопасности, обеспечение контроля посещаемости и трудовой дисциплины, интеграцию с системами сторонних производителей. СКУД BioSmart адаптирован к российским условиям (температурный диапазон работы от -40°С до +50°С), алгоритмы обработки шаблонов отпечатков пальцев соответствуют ГОСТ-Р ИСО/МЭК 19794/2 2005, возможность идентификации до 30 тыс. отпечатков пальцев в серверном режиме, запатентованная аппаратная защита от муляжей.

Терминал предназначен для учета рабочего времени сотрудников посредством идентификации их по отпечаткам пальцев.

Максимальное количество отпечатков пальцев – 4500.

Максимальное количество событий 100000.

Описание обобщённой схемы СКУД и её параметров установленной на предприятии ГК «НГ-Сервис».

Система контроля доступа содержит 4 основных элемента:

- идентификатор пользователя (отпечаток пальца);
- устройство идентификации;
- управляющий контроллер и исполнительные устройства.

Обобщённая схема СКУД показана на рис. 3.1.

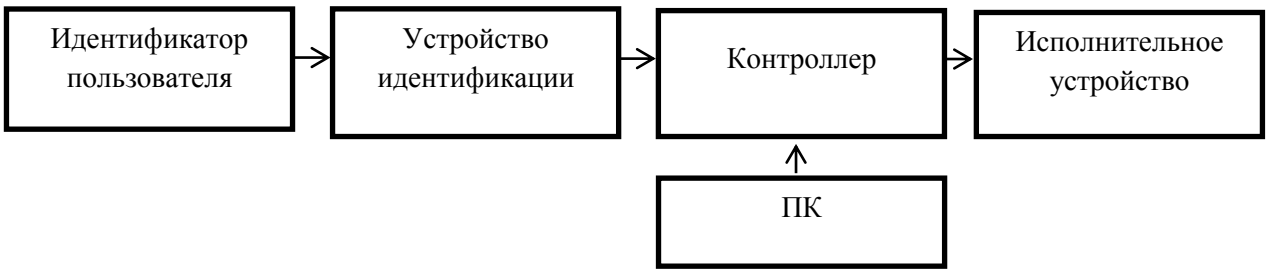

Рисунок 3.1 – Обобщенная схема СКУД

СКУД BioSmart организована как сетевая распределённая система с разграничением прав доступа пользователей.

Задачи СКУД BioSmart:

1. Создание двух взаимозависимых точек прохода на базе стандартных дверей.

2. Обеспечение входа и выхода постоянного персонала в автоматическом режиме с минимальной задержкой.

3. Проход по временным и разовым пропускам только после получения подтверждения от оператора (охранника).

4. Регистрация в архиве системы всех событий.

3.2 Организационные мероприятия по защите персональных данных в СКУД ГК «НГ-Сервис»

В первую очередь необходима разработка организационных мер защиты информации. При отсутствии надлежащей организации работы, отсутствии системы контроля и надзора за деятельностью сотрудников, все технические средства могут оказаться не дееспособными.

Организационные мероприятия должны быть направлены на обеспечение правильности функционирования механизмов защиты, и выполняться администратором безопасности системы, так же руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил[3].

К организационным мерам можно отнести:

- идентификация пользователей по паролю;
- регистрация входа \ выхода пользователей;
- разграничение доступа пользователей к средствам защиты и информационным ресурсам в соответствии с матрицей доступа;
- учет всех материальных носителей информации, регистрация их выдачи;
- физическая охрана ИСПДн (Информационная система персональных данных), контроль доступа в помещение;
- блокирование терминалов пользователей;
- очистка освобождаемых областей оперативной памяти компьютера и внешних накопителей;

– регистрация фактов распечатки документов с указанием даты, времени и имени пользователя;

– наличие службы безопасности, ответственных за ведение, нормальное функционирование и контроль работы средств защиты информации.

Также, к организационным мерам можно отнести отдельные мероприятия на стадии проектирования ИСПДн:

– разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

– определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности;

– разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно распорядительной документации по защите информации (приказов, инструкций и других документов).

В организации разработаны документы и регламенты:

– положение о работе с персональными данными;

– инструкция службы безопасности;

– инструкция пользователя ИСПДн;

– положение о парольной защите;

– положение об антивирусной защите;

– регламент проведения проверок безопасности ИСПДн;

– порядок учета и регистрации магнитных носителей информации.

В Положении о работе с персональными данными отражается:

– порядок получения, обработки, использования и хранения персональных данных;

– порядок передачи персональных данных третьим лицом;

– гарантии конфиденциальности персональных данных.

В инструкции службы безопасности устанавливаются:

– правовая основа деятельности администратора;

– требования к уровню его знаний, квалификации и опыту;

– перечень вверенного ему оборудования и порядок доступа к нему;

– перечень и периодичность плановых мероприятий по контролю осуществления надлежащего функционирования системы защиты ИСПДн;

– полномочия сотрудника по контролю над деятельностью пользователей ИСПДн, в частности, разработка и внедрение системы паролей

доступа пользователей, организация разграничения доступа пользователей к техническим средствам защиты ИСПДн и информационным ресурсам, выявление допущенных пользователями нарушений инструкций и приостановление / прекращение их доступа;

– ответственность за допущенные нарушения.

В инструкции пользователя ИСПДн указываются:

– требования к уровню владения техническими средствами обработки информации;

– полномочия доступа к техническим средствам защиты информации;

– полномочия доступа к информационным ресурсам, периферийным устройствам, материальным носителям информации;

– обязанности по соблюдению правил антивирусной защиты;

– ответственность за несоблюдение установленных правил работы.

На рисунке 3.2 рассмотрена система защиты персональных данных.

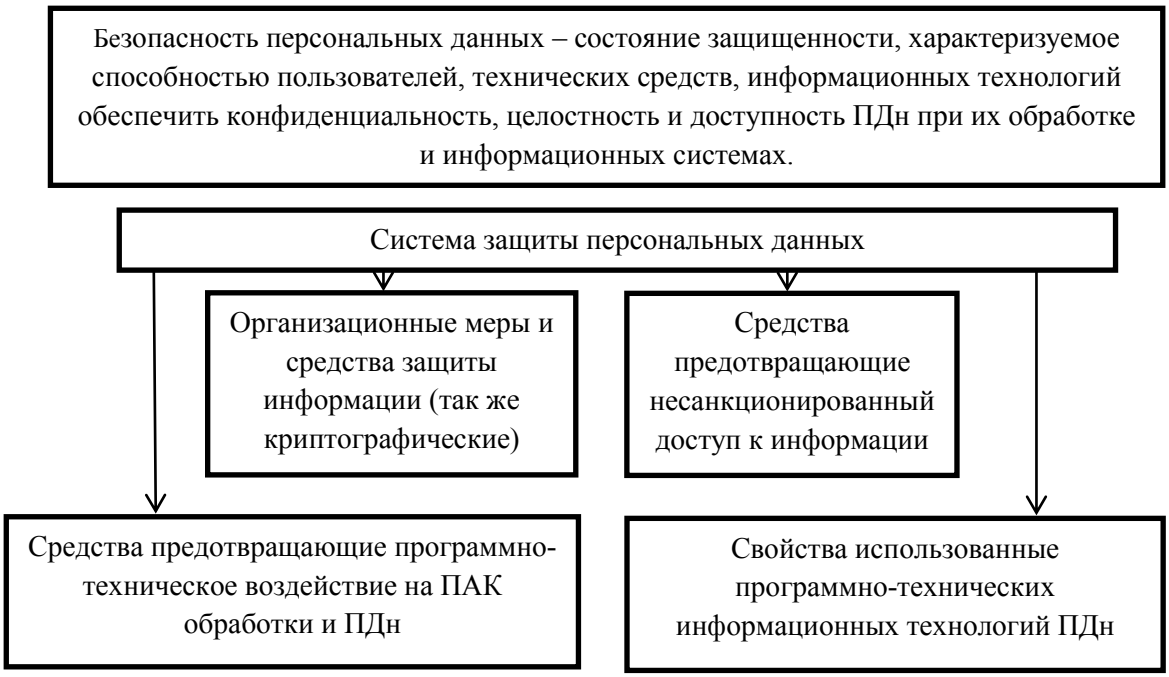

Рисунок 3.2 – Система защиты персональных данных

Мероприятия по защите информации в информационной системе персональных данных.

Физические меры защиты – различные механические, электро – или электронно-механические устройства, предназначение для создания физических препятствий на путях проникновения потенциальных нарушителей к защищаемой

информации, а также техника визуального наблюдения, связи и охранной сигнализации.

Защита серверов.

Физическая безопасность серверов – необходимый аспект безопасности, физическая незащищенность сервера ведет к значительному риску, который может выразиться в неавторизованном доступе к нему и его неисправности, что повлияет на целостность сервера, всей сети и ее ресурсов.

Ключевой этап подготовки помещений, где будут стоять серверы. Сервер должен находиться в отдельной комнате, доступ в которую ограничен. На окнах обязательно должны быть жалюзи. Расположение помещения внутри здания также является важной частью защиты. Доступ в данное помещение осуществляется, конечно же, через дверь, она должна быть единственной, в том понимании, что через нее должен осуществляться единственный доступ в комнату. Дверь должна быть надежно укреплена, оборудована кодовыми замками, рассчитана на преднамеренные попытки взлома, существенно не отличаясь от остальных дверей.

Всё оборудование в серверном помещении должно быть размещено в закрытых шкафах или на открытых стойках, число которых определяется исходя из имеющегося оборудования, его типоразмеров и способов монтажа. Закрытые шкафы позволяют организовать дополнительные ограничения доступа к оборудованию с использованием подсистемы контроля доступа. Однако такие шкафы требуют обеспечения необходимого температурного режима, для чего применяются дополнительные вентиляторы, встраиваемые системы охлаждения и модули отвода горячего воздуха. При распределении оборудования по шкафам или стойкам следует учитывать его совместимость, а также распределение мощности, габариты, массу и оптимальность проведения коммуникаций [27].

Отключение неиспользуемых дисководов будет положительным, параллельных и последовательных портов сервера. Его корпус при возможности опечатать. Все это даст возможность избежать кражи или подмену информации даже в том случае, даже при проникновении в серверную комнату. Можно использовать другие меры защиты, как железные решетки и двери, кодовые замки и камеры видеонаблюдения.

Защита помещений.

Основным моментом защиты является доступность в помещение, в котором находится оборудование, способное помочь проникнуть в сеть.

Для защиты от прямого доступа к оборудованию применяются стандартные методы защиты имущества. А именно, установление соответствующей системы безопасности, включающей в себя замки, сигнализацию, квалифицированную охрану, имеющую доступ только до внешнего периметра комнат. То есть не имеющая прямого доступа к оборудованию, которое охраняет.

В помещениях с рабочими компьютерами высокий уровень защиты, необходимый для серверных комнат, не требуется. Поэтому для них используют немного другие методы. Первым делом необходимо препятствовать проникновению посторонних лиц на территорию компании без необходимости. На окнах обязательно должны быть жалюзи. На двери необходимо установить кодовые замки. Ключи от помещений с рабочими компьютерами должны выдаваться сотрудникам, согласно утвержденному списку. Данные помещения не должны оставаться незапертыми при отсутствии в них сотрудников даже на короткое время[6].

На системных блоках АРМ проходных и корпусов должны быть отключены все дисководы, параллельные и последовательные порты, корпусы опечатаны.

Защита электронных архивов.

Методом защиты целостности информации, на случай взлома, является создание архивной копии. Частота создания архивной копии определяется важностью и объемами поступления новой информации. Резервные копии не хранить в одном помещении с сервером.

Защита компьютеров от неполадок в электросети.

Поддерживать стандартные параметры напряжения, частоты, высокочастотных шумов и т.д. не удается по многим причинам. Развитие энергетики не успевает за развитием других отраслей промышленности и энергопотреблением. Непредсказуемые всплески и падения напряжения во время включения и выключения мощных потребителей, удары молний, различные аварии - все это приводит к выходу из строя компьютерной и другой техники. Даже если нет никаких внешних признаков неисправностей, периодически напряжение в электросети выше или ниже нормы. Нарушения в системе электроснабжения могут нанести ущерб, нанесенный, например, банковской сети или сети научного учреждения. Поэтому необходимо для каждого компьютера использовать источник бесперебойного питания.

Защита кабельной системы сети.

Так же в защите нуждаются и провода - кабельная система сети. Лучший вариант защиты кабеля - это короба, но подходят различные способы

позволяющий скрыть и надежно закрепить провода. Впрочем, не стоит упускать из вида и возможность подключения к ним извне для перехвата информации или создания помех, например, посредством разряда тока. Рассматриваемая фирма является ведущим производителем в своей области, и хотя серьезных конкурентов у предприятия нет, и случаев попыток перехвата информации посредством наводок замечено не было, тем не менее, следует проявлять осторожность [7].

Система охранно-пожарной сигнализации.

Охранно-пожарная сигнализация - получение, обработка, передача и представление в заданном виде потребителям при помощи технических средств информации о пожаре.

Система охранно-пожарной и тревожной сигнализации представляет собой: совокупность совместно действующих технических средств обнаружения пожара и попытки проникновения нарушителя на охраняемый объект, сбора и предоставления в заданном виде информации о проникновении (попытке проникновения), а также выдачи сигналов тревоги в дежурную часть органов внутренних дел при разбойном нападении на объект в период его работы.

Уровень безопасности в основном зависит от времени реагирования технических средств охраны (ТСО) на возникающую угрозу. Этого можно достичь благодаря правильному выбору и использованию ТСО, а также их оптимальному размещению в охраняемых зонах.

Любая система охранно-пожарной сигнализации (ОПС) может быть разбита на три составляющие: датчики, концентраторы, устройства оповещения и реагирования. Датчики, объединенные в логические группы, именуемые шлейфами, анализируют текущее состояние объекта по различным физическим параметрам и передают полученную информацию на концентратор. Концентратор является ядром системы, он обрабатывает сообщения от всех датчик в и, в случае необходимости какой-либо реакции, выдает информацию на систему оповещения и реагирования.

По принципу формирования информационного сигнала о проникновении на объект или пожаре извещатели охранно-пожарной сигнализации делятся на активные и пассивные. Активные извещатели генерируют в охраняемой зоне сигнал и реагируют на изменение его параметров. Пассивные извещатели реагируют на изменение параметров окружающей среды, вызванное вторжением нарушителя или возгоранием.

Широко используются такие типы охранных извещателей, как инфракрасные пассивные, магнитно-контактные, извещатели разбития стекла,

периметральные активные извещатели, комбинированные активные извещатели. В системах пожарной сигнализации применяются тепловые, дымовые, световые, ионизационные, комбинированные и ручные извещатели.

Извещатели (датчики) являются основным элементом систем ОПС и во многом определяют эффективность их использования. Это устройства, предназначенные для определения наличия угрозы безопасности охраняемого объекта и передачи тревожного сообщения для своевременного реагирования. Извещатели могут классифицироваться по физическому принципу действия. Рассмотрим наиболее распространенные типы извещателей.

Контактные извещатели служат для обнаружения несанкционированного открытия дверей, окон, ворот и т.д. Магнитные извещатели состоят из двух частей: герконового реле (геркона), устанавливаемого на неподвижную часть конструкции, и магнита, устанавливаемого на открывающийся модуль. Когда магнит находится вблизи геркона, его контакты в замкнутом состоянии. По принципу монтажа герконы делятся на накладные, врезные и для монтажа на металлические двери.

Инфракрасные пассивные извещатели служат для обнаружения вторжения нарушителя в контролируемый объем. ИК датчик с помощью пироэлемента преобразуют тепловое излучение в электрический сигнал. В настоящее время используются 2 и 4 площадные пироэлементы. Это позволяет существенно снизить вероятность ложных тревог. Формирование зон обнаружения происходит с помощью зеркал (на отражение) и / или линз (на прохождение) Френеля.

Комбинированные извещатели объединяют в одном корпусе пассивный ИК и радиоволновый детектор, основанный на эффекте Доплера. Это позволяет существенно уменьшить вероятность ложной тревоги: поскольку сигнал тревоги выдается только при одновременном обнаружении нарушения обеими частями оповещения.

Акустические датчики оснащаются высокочувствительным миниатюрным микрофоном, улавливающим звук, издаваемый при разбитии стекла. Эти извещатели крепятся на стену или потолок около окна. При разбитии стекла возникает два типа звуковых колебаний в строго определенной последовательности: сначала ударная волна от колебания всего массива стекла с частотой порядка 100 Гц, а потом волна разрушения стекла с частотой около 5 Кгц, обрабатываются сигналы и принимает решение о наличии проникновения.

Дымовые извещатели предназначены для обнаружения наличия частиц дыма в воздухе. По принципу действия они делятся на два основных типа:

оптоэлектронные и ионизационные. Дымовые извещатели позволяют обнаружить пожар на ранней стадии развития. Это их главное преимущество перед тепловыми извещателями. Поэтому дымовые извещатели сейчас наиболее перспективны для применения на всех видах объектов.

Дымовые извещатели по зоне обнаружения делятся на точечные и линейные. Точечные извещатели имеют чувствительную зону внутри измерительной камеры извещателя. Принцип обнаружения основан на отражении оптического излучения от частиц дыма, попадающих в эту зону.

Линейные дымовые извещатели в качестве чувствительной зоны используют, как правило, луч света длиной до 100 м, который пересекает защищаемое помещение. Обнаружение пожара происходит при ослаблении оптического излучения дымом [20].

Тепловые извещатели служат для обнаружения внутри помещения повышенной температуры. По принципу действия они делятся на термоконтактные и дифференциальные. Дифференциальные извещатели являются восстанавливаемыми и содержат термопару для измерения температуры. Такой извещатель реагирует не только на абсолютное значение температуры, но и на высокую скорость изменения температуры. Тепловые извещатели недостаточно эффективны для раннего обнаружения пожара. Их применение оправдано только для тех объектов, где вероятность повышения температуры более высока, чем появление дыма или открытого пламени, а также там, где условия эксплуатации не позволяют применить извещатели другого типа.

Извещатели пламени реагируют на инфракрасное или ультрафиолетовое излучение открытого пожара. Область их применения достаточно ограничена. В основном это производственные объекты, места хранения ЛВЖ, бензоколонки и т.д.

Особенностью ручных извещателей является то, что в действие их приводит человек, обнаруживший пожар. Этот тип извещателей применяется в местах постоянного присутствия людей, на лестничных пролетах, на путях эвакуации и т.д.

В зависимости от способов выявления тревог и формирования сигналов, извещатели и системы охранно-пожарной сигнализации делятся на неадресные, адресные и адресно-аналоговые. В неадресных системах извещатели имеют фиксированный порог чувствительности, при этом группа извещателей включается в общий шлейф охранно-пожарной сигнализации, в котором в случае срабатывания одного из приборов охранно-пожарной сигнализации формируется

обобщенный сигнал тревоги. Адресные системы отличаются наличием в извещении информации об адресе прибора охранно-пожарной сигнализации, что позволяет определить зону пожара с точностью до места расположения. Адресно-аналоговая охранно-пожарная сигнализация является наиболее информативной и развитой. В такой системе применяются «интеллектуальные» извещатели охранно-пожарной сигнализации, в которых текущие значения контролируемого параметра вместе с адресом передаются прибором по шлейфу охранно-пожарной сигнализации. Такой способ мониторинга используется для раннего обнаружения тревожной ситуации, получения данных о необходимости технического обслуживания приборов вследствие загрязнения или других факторов. Кроме этого, адресно-аналоговые системы позволяют, не прерывая работу охранно-пожарной сигнализации, программно изменять фиксированный порог чувствительности извещателей при необходимости их адаптации к условиям эксплуатации на объекте.

Концентраторы (контрольные панели) предназначены для сбора и обработки информации о состоянии извещателей и линий передачи (шлейфов). Можно выделить проводные безадресные и адресные концентраторы. В последних информация от датчиков к концентратору поступает в цифровом коде. Это позволяет концентратору контролировать состояние каждого подключенного к общему шлейфу датчика в отдельности. Беспроводные концентраторы получают информацию от датчиков по радиоканалу. Концентраторы выдают соответствующие сигналы на внешние устройства оповещения на основе анализа информации от датчиков.

Линии передач, по которым поступают сигналы от извещателей, представляют физические шлейфы, они в общем случае могут отличаться от логических шлейфов, с которыми оперирует схема обработки сигналов концентратора. Логическим шлейфом (зоной) называется единичный сегмент информационного пространства концентратора: именно его состояние анализируется им в каждый момент времени. Максимальное число зон, которое может контролировать концентратор, составляет: до 30 - для аналоговых и до 100 - для микропроцессорных (цифровых) концентраторов.

3.3 Установка, настройка и подключение BioSmart в подразделении ГК «НГ-Сервис»

С целью выполнения дипломного проекта был проведен анализ и выбор программы BioSmart биометрические системы со сканером отпечатков пальцев. В

данном разделе структурно и пошагово описывается установка, настройка и подключения данной системы, на предприятии ГК «НГ-Сервис» в подразделении г. Челябинска с численностью персонала пятнадцать человек.

В первую очередь необходима установка драйверов для сканера отпечатков пальцев. Для правильной работы сканера «Futronic FS-80» следует установить драйверы этого устройства. Драйверы скачиваются с сайта выбранного и купленного продукта, электронный ресурс: http://www.mgbit.ru/download/download.php или установить с диска. Была выполнена установка драйверов в указанной последовательности:

1. Подключение сканера к USB-порту компьютера.

2. Запуск мастера нового оборудования выбран пункт «Да, Только в этот раз», «Далее».

3. Установление в следующем окне флага «Включать следующие места поиска:» (все остальные флаги сняты), указание пути к каталогу, где находятся драйвер для сканера «Далее».

Драйверы, таким образом, установлены.

Занесение отпечатков в БД при помощи программы «Пропуска».

Для вызова окна «Шаблоны отпечатков» необходимо открыть страницу «Пропуска» в главном окне программы. На странице «Пропуска» следует выделить пользователя и выбрать пункт «Биометрия» в контекстном меню, вызов которого осуществляется щелчком правой кнопки мыши. Присваиваем каждому сотруднику отпечатки пальцев, для удобства два по одному на каждую руку, в программе же на одного пользователя возможно присваивать пять отпечатков.

Выбор шаблонов отпечатков: «Шаблоны отпечатков». На экране появляется окно «Авторизация отпечатка», далее «Контрольная авторизация отпечатка».

После добавления отпечатков сотрудника, произвожу загрузку в контроллер. Для контроля загрузки отпечатков в программе «Пропуска» следует открыть вкладку «Биометрия». На этой вкладке отображается информация о загрузке пропусков с «привязанными» к ним наборами отпечатков.

Настройка контроллера «BioSmart»

Контроллер «BioSmart» поступает не настроенным для работы в составе СКУД «Реверс». Для того чтобы его настроить, устанавливается программа «BioSmart-Studio v.4» устанавливаем инструкцию на сайте, элетронный ресурсы: \http://www.biosmart.ru/support/ftp.htm, либо на диске, поставляемом в комплекте с каждым контроллером «BioSmart»). После установки программы «BioSmart-Studio» и настройки связи с контроллером «BioSmart» (при подключении

используем руководство по эксплуатации на контроллер), необходимо запустить программу «BioSmart-Studio» и перейти к окну свойств контроллера «BioSmart». В окне свойств контроллера необходимо изменить только один параметр: в разделе «Работа со сторонним оборудованием», в строке «Дополнительное оборудование» изменяем значение на «Кронверк». После этого нажать кнопку «Записать», а затем кнопку «ОК», чтобы изменения были записаны в контроллер «BioSmart».

Подключение контроллера «BioSmart». Контроллер «BioSmart» включается в нижнюю магистраль связи RS-485 контроллеров «Реверс С16». Подключение необходимо производить к контактам отмеченным, как БУР+ (соответствуют контактам А на контроллере «Реверс К2» или АА на контроллере «Реверс С16») и БУР- (соответствует контактам В на контроллере «Реверс К2» или ВВ на контроллере «Реверс С16»). Названия контактов и их описания приведены в таблице 3.1.

Таблица 3.1 – Контакты и описание

Наименов. контакта	Обозначение	Описание	Назначение
1	+485	Интерфейс RS-485 +	Используется для подключения в магистраль связи RS-485
2	-485	Интерфейс RS-485 -	Используется для подключения в магистраль связи RS-485
3	+БУР	Интерфейс RS-485 +	Не используется для подключения к СКУД «Реверс»
4	-БУР	Интерфейс RS-485 -	Не используется для подключения к СКУД «Реверс»
5	WO1	D1 для подключения контроллера «BioSmart» к контроллеру «Реверс К2»	Не используется для подключения к СКУД «Реверс»

6	WO0	D0 для подключения контроллера «BioSmart» к контроллеру «Реверс К2»	Не используется для подключения к СКУД «Реверс»
7	WI1	D1 для подключения к контроллеру «BioSmart» считывателя	К данным контактам можно подключать внешний считыватель
8	WI0	+12 В	
11	+12	Общий	К блоку питания 12В
12	-12		

Добавление контроллера «BioSmart» в конфигурацию СКУД «Реверс» осуществляется в программе «Конфигуратор системы», входящей в состав ПО «Реверс». Для добавления контроллера «BioSmart» необходимо выбрать в иерархическом дереве устройств программы «Конфигуратор» контроллер «Реверс С16» и, нажатием правой кнопки мыши, вызвать контекстное меню, в котором выбрать пункт «Добавить». В появившемся окне «Добавление устройства» выбираем пункт «Контроллер «BioSmart».

В следующем окне «Добавление контроллера BioSmart» необходимо установить тип контроллера «Реверс К2» и указать его производственный адрес (он указан как на плате, так и в паспорте контроллера). В нижней части окна нужно выбрать производственный адрес контроллера «BioSmart» (он указан на плате контроллера и в паспорте).

Далее нажмите кнопку «Ввод». К контроллеру «Реверс С16» будут добавлены два устройства контроллер «Реверс К2» (к этому устройству подключаются все периферийные устройства, такие как кнопка ДУ, геркон и замок или турникет) и контроллер «BioSmart» (этот контроллер выполняет роль считывателя и исполнительные устройства к нему не подключаются).

В окне свойств контроллера «BioSmart», на вкладке «Сеть», представлены настройки, позволяющие менять режим работы контроллера (для вызова окна свойств необходимо выбрать контроллер в иерархическом древе или списке устройств, при помощи правой кнопки мыши вызвать контекстное меню и выбрать в нем команду «Свойства»).

Инициализация контроллера – производит удаление отпечатков пальцев из памяти контроллера «BioSmart».

Идентификация по карте ИЛИ отпечатку пальца – проход через ТД, где установлен контроллер «BioSmart», можно осуществлять как по карточке, так и по отпечатку пальца.

Идентификация по карте и отпечатку пальца –проход через ТД, где установлен контроллер «BioSmart», можно осуществлять, только если сначала был предъявлен пропуск, а затем был предъявлен палец.

Устройства биометрического замка монтируются по принципу врезных замочных механизмов.

Этапы монтирования:

– подготовка нескольких отверстий, служащих для взаимодействия различных частей конструкции;

– выполнение высокоточной разметки при помощи двухстороннего трафарета, входящего в комплектацию с замком;

– сборка механизма и подключение врезной части к разъемам внутренней замочной системы при помощи проводки.

После монтажа биометрического устройства стоит обратить внимание на его настройку. Специалисты рекомендуют программировать в его память максимальное число отпечатков пальцев. Это поможет при непредвиденных ситуациях, ведь иногда сенсор, которым оснащен замок, отказывается распознавать отпечатки пальца.

Высокая стоимость таких устройств обуславливается предоставлением эффективной и современной защиты. Привычные механические замки обходятся гораздо дешевле, однако они несравнимы по параметрам с премиум сегментом. Существует два вида замков:

– биометрические замочные системы с несложной конструкцией и ограниченным функционалом;

– замки с дополнительными возможностями, большим объемом памяти и надежной защитой от механического воздействия

ЗАКЛЮЧЕНИЕ

В ходе внедрения биометрической системы учета рабочего времени на предприятии был выявлен наиболее эффективный и экономически выгодный метод контроля сотрудников путем решения поставленных задач.

Первая задача состояла в определении наиболее эффективного способа системы учета рабочего времени сотрудников.

Для ее решения в работе проведен анализ существующих наиболее распространенных методов учета и контроля, таких, как: назначение ответственного сотрудника, ведение личной отчетности сотрудников, установка систем видеонаблюдения и систем контроля и управления доступом с применением пропусков или сканеров отпечатка пальца (биометрические). Выявлены недостатки некоторых из них (передача/потеря пропускных карточек, невнимательная работа контролирующих сотрудников), неизбежно ведущих к возникновению неблагоприятных ситуаций. Обоснована модернизация методов путем введения биометрических систем.

Для решения второй задачи в работе обоснован выбор наиболее выгодной биометрической системы для предприятия ГК «НГ-Сервис».

Рассмотрены две наиболее актуальные системы система контроля удаленного доступа: Терминал PV-WTC (сканер отпечатка руки) и Терминал BioSmart-WTC2 (сканер отпечатка пальца). Проведенный анализ показал, что биометрическая система учета рабочего времени сотрудников по отпечатку пальца BioSmart-WTC2 имеет более краткий срок окупаемости, так же такая система является автономной после ее внедрения и требует наименьшего внимания сотрудников информационных технологий.

При решении третьей поставленной задачи выявлены недостатки и достоинства метода контроля и учета рабочего времени по результатам внедрения системы:

внедрение системы BioSmart, имело положительный эффект, который позволил организации:

– уменьшить количество персонала за счет сокращения охраны на проходной и нормировщика, который производил подсчеты отработанных часов;

– получать достоверные данные о времени входа и выхода работников;

– производить автоматический ввод данных в табель рабочего учета;

– повысить производственную эффективность за счет улучшения дисциплины и отсутствия работников в рабочие периоды.

Выявлены также возникающие трудности и недостатки биометрического учета:

– налаженность данного метода, установка, дальнейшее обслуживание, и управление должны быть высокопрофессиональными;

– высокая стоимость оборудования.

Для решения четвертой задачи по осуществлению, установке, настройке и монтажа оборудования в работе представлен алгоритм, являющийся наиболее оптимальным. Структурно и пошагово описаны установка, настройка и подключение системы контроля и учета на предприятии ГК «НГ - Сервис». Использование технических разработок обеспечивают высокую надежность системы при достаточной простоте и удобстве ее эксплуатации.

По результатам проведенной работы можно сделать следующий вывод:

В организациях с большим количеством сотрудников, офисов и подразделений, где трудно контролировать рабочее время, для эффективного выполнения этой задачи должен быть введен автоматизированный метод учета рабочего времени. Предложенная в работе система является наиболее эффективной, удобной в эксплуатации и простой во внедрении.

Затраты и экономический эффект системы

Количество сотрудников на предприятии	400
Средняя ЗП одного сотрудника в месяц, руб.	20 000
Неотработанное время сотрудника, минуты в день	5
Неотработанное время всего персонала, часы в день	9
Переплата за неотработанное время сотрудника, руб. в месяц	210,50
Переплата за неотработанное время по предприятию, руб. в месяц	84 200
Стоимость системы BioSmart, руб.	280 800
Итого: срок окупаемости в месяцах	3

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Илясов, Г.Г. Как улучшить финансовое состояние предприятия, финансы / Г.Г. Илясов. – издание 10-ое – 2010. – 72 с.

2 Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов – 3-е изд. / В.И. Ярочкин – М. – Трикста, 2009 г. – 559 с.

3 Ворона, В.А. Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. – М.: Горячая линия – Телеком, 2010. – 272 с.

4 Абрамов, А. М. Системы управления доступом / А.М. Абрамов – М.: «Оберег-РБ», 2015 г. – 112 с.

5 Татарченко Н. В. Биометрическая идентификация в интегрированных системах безопасности / Н. В. Татарченко – Специальная техника, 2013 – 218 с.

6 Морзеев Ю. Современные биометрические решения в системах безопасности / Ю. Морзеев – Компьютер Пресс, 2014. – 418 с.

7 Кухарев А.В. Биометрические системы. Методы и средства идентификации личности человека: Г. А. Кухарев — Москва— Политехника, 2011 г.- 240 с.

8 Кочеткова О. О. Особенности правового регулирования использования биометрических документов в европейском Союзе и Российской Федерации / О. О. Кочеткова — Фундаментальные исследования, 2015г. — 316 с.

9 Маркелов К.М. Идентификация и верификация личности - комплексная биометрическая информационная технология / К.М. Маркелов — InternationalJournalofOpenInformationTechnologies, 2015г. – 603 с.

10 Антосенков Е.М. Анализ фонда рабочего времени на предприятии // Экономист, 2008г. — № 4. — 117 с.

11 Воронцовский А.В. Инвестиции и финансирование. Методы оценки и обоснования // – Издательский дом Санкт-Петербургского государственного университета, 2003г. – 528 с.

12 Биометрические технологии - альтернатива персональным идентификационным номерам и паролям [Электронный ресурс] - Режим доступа: http://www.k2kapital.com/archives/research/rs20000508.html.

13 Виталий Задорожный. Области применения и принципы построения биометрических систем [Электронный ресурс] - Режим доступа: http://www.pcmag.ru/?ID=447314&4Print=1.

14 Система контроля и управления доступом [Электронный ресурс] - Режим доступа: http://www.itv.ru/products/intellect/.

15 Биометрическая идентификация: биометрические считыватели и СКУД Sagem. [Электронный ресурс] - Режим доступа: http://www.sagem-biometrics.ru/news/ma-200.ahtm.

16 Сканеры отпечатков пальцев [Электронный ресурс] - Режим доступа: http://cyberdefend.narod.ru/biometric_devices.htm.

17 Smartec. Контроль доступа. [Электронный ресурс] - Режим доступа: http://smartec-security.ru/news/biometric-reader.htm.

18 Биометрическая идентификация [Электронный ресурс] - Режим доступа: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html.

19 Биометрические системы безопасности [Электронный ресурс] - Режим доступа: http://daily.sec.ru.

20 Современные технологии распознавания личности по отпечатку пальца с использованием емкостных датчиков [Электронный ресурс] - Режим доступа: http://www.radioradar.net/staty/identif_otpech.php.

21 Государство. Бизнес. ИТ. [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/index.php/Продукт%3АСКУД_BioSmart.

22 Босс кадровик [Электронный ресурс] - Режим доступа: http://www.tadviser.ru/index.php/Продукт%3АБОСС.

23 Биометрические технологии [Электронный ресурс] - Режим доступа: https://www.bytemag.ru/articles/detail.php?ID=6675.

24 Учет рабочего времени [Электронный ресурс] – Режим доступа: http://www.bio-smart.ru/solution/typesolution/time_attendance.

25 Биометрическая система контроля и управления доступом СКУД BioSmart [Электронный ресурс] Режим доступа: http://zefz.ru/frontend/web/attaches/files/62/4371/BioSmart-1c.pdf.

26 Анализ систем защиты информации, построенных на принципах биометрии [Электронный ресурс] Режим доступа: https://www.webkursovik.ru/kartgotrab.asp?id=-117889.

27 BioSmart – биометрическая система контроля доступа и рабочего времени [Электронный ресурс] - Режим доступа: http://gciskander.ru/biosmart1/.

28 Система Biosmart [Электронный ресурс] – Режим доступа: https://camafon.ru/skud/biosmart.

29 Регламент № 18 «Об организационной политики ГК «НГ-Сервис».