МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ЧЕЧЕНСКОЙ РЕСПУБЛИКИ

Государственное бюджетное профессиональное образовательное учреждение
«Чеченский государственный педагогический колледж»

Дипломная работа допущена к защите
«___»_____20_____г.
Заместитель директора по учебной работе
_____Я.М. Басаев

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Дипломная работа

по специальности 09.02.07 Информационные системы программирование

«Разработка системы защиты с использованием биометрических данных, на предприятии»

Выполнила студентка группы 18-ИСиП-2д
очной формы обучения
_____ Делаева Раяна Исмаиловна
(подпись) *(Ф.И.О.)*

Руководитель дипломной работы

_____ Абкаров Ансар Хамзатович
(подпись) *(Ф.И.О.)*

Оценка за защиту «_____» _____

Грозный, 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы. Тема посвящена исследованию и анализу новых структур и математических моделей представления биометрических данных, созданию алгоритмов биометрической верификации и идентификации личности, основанных на современных моделях описания и анализа отпечатков пальцев, а также разработке защищенной системы биометрической аутентификации личности. К современным методам аутентификации относится проверка подлинности на основе биометрических показателей. При биометрической аутентификации, секретными данными пользователя могут служить, как глазная сетчатка, так и отпечаток пальца. Эти биометрические образы являются уникальными для каждого пользователя, что обеспечивает высокий уровень защиты доступа к информации. Согласно предварительно установленным протоколам, биометрические образцы пользователя регистрируются в базе данных.

Традиционные процедуры проверки соответствия осуществляются с помощью информации, которую знает человек (пароль), и / или физических компонентов (например, идентификационные брелоки или смарт-карты). При этом ввод пароля в общем случае является более медленной процедурой по сравнению с установлением личности по смарт-карте. Кроме того, пароль при определенном стечении обстоятельств может стать известным посторонним лицам, а также может быть угадан злоумышленником в случае его простоты, или наоборот, забыт зарегистрированным пользователем в случае его чрезмерной сложности и / или длины.

Идентификация человека по его биометрическим параметрам имеет очевидное преимущество по сравнению с традиционными методами.

Объект исследования: современные методы биометрической аутентификации человека.

Предмет исследования: использование биометрии для аутентификации личности человека по лицу, глазам и отпечатку пальцев, его применение в организации.

Целью исследования является совершенствование представления биометрических данных посредством рассмотрения новых информационных структур, создания на их основе математических моделей представления отпечатков пальцев в биометрических системах с последующей разработкой алгоритмических методов, применяемых в информационных процессах верификации и идентификации личности по отпечаткам пальцев, а также исследование возможности создания защищенной системы аутентификации личности на основе биометрического личностного шифрования с улучшенными характеристиками в качестве альтернативы традиционным средствам аутентификации пользователей в информационных системах, таким как пароли и токены, показать особенности применения биометрии для аутентификации человека на предприятии, на основе теоретического материала.

Помимо усиления безопасности, биометрические системы аутентификации повышают удобство пользователя, устраняя необходимость генерировать и помнить пароли. Кроме того, биометрия:

- один из немногих методов, которые могут использоваться для отрицательного распознавания, когда система определяет, является ли человек тем, кем он отказывает себя признавать;

- предотвращение несанкционированного доступа к ПДн, их утечки и (или) передачи лицам, не имеющим права доступа к такой информации;

- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- обеспечение возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие действий нарушителей;

- осуществление контроля над обеспечением уровня защищенности ПДн.

Для достижения поставленной цели в работе сформулированы и решаются следующие задачи.

– Разработка новых информационных структур представлений отпечатка пальца и основанных на них математических моделей отпечатков пальцев, создание методов верификации и идентификации личности по отпечаткам пальцев на основе новых информационных структур и математических моделей отпечатков пальцев.

– Теоретическая оценка сложности алгоритмов верификации и идентификации с целью оценки возможностей применения с позиции скорости новых алгоритмов верификации и идентификации личности по отпечаткам пальцев в качестве компонент реальных биометрических систем.

– Проведение экспериментальных исследований, оценка вероятности ошибок первого и второго рода, сравнение с существующими алгоритмами верификации и идентификации.

– Исследование возможности практического создания защищенной системы биометрической аутентификации.

– Анализ безопасности полученной защищенной системы биометрической аутентификации.

Метод исследования. В работе применялись методы теории графов, теории вероятностей и математической статистики, теории информации, теории алгоритмов и вычислительной сложности, комбинаторики и защиты информации

ГЛАВА 1. СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

1.1 Анализ обрабатываемой информации и классификация ИСПДн

Под системой контроля и управлением доступа обычно понимают совокупность программно - технических и организационно-методических средств, с помощью которых решается задача контроля и управления помещением предприятия и отдельными помещениями, а также оперативный контроль за передвижением персонала и времени его нахождения на территории предприятия. Исполнительным устройством системы управления доступом может быть замок, электромеханическая защелка, турникет, шлагбаум, электронная проходная. СКУД может быть интегрирована в другие системы безопасности. Грамотная интеграция СКУД в систему видеонаблюдения позволяет полностью контролировать ситуацию на объекте. В случае возникновения чрезвычайной ситуации подобная охранная система позволяет быстро обнаружить нарушителя. Возможна интеграция СКУД в систему охранно-пожарной сигнализации, что позволяет разблокировать двери, турникеты, электронные проходные, включать сирену в случае пожара.[1]

В соответствии с Руководящим документом 78.36.003-2002 «Инженерно-техническая укреплённость. Технические системы охраны. Требования и нормативы проектирования по защите объектов от преступных посягательств» Система контроля и управления доступом (СКУД) предназначена для:

- обеспечения санкционированного входа в здание и в зоны ограниченного доступа и выход из них путем идентификации личности по комбинации различных признаков: вещественный код (Виганда-карточки, ключи touch-memory и другие устройства), запоминаемый код (клавиатуры,

[1] Баймакова, И.А. Обеспечение защиты персональных данных: методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев, А. Х Хыдыров. - М.: 1С-Паблишинг, 2017. - 216 с.

кодонаборные панели и другие устройства), биометрические признаки (отпечатки пальцев, сетчатка глаз и другие признаки);

- предотвращения несанкционированного прохода в помещения и зоны ограниченного доступа объекта.

Система контроля и управления доступом машиностроительного завода построена на основе программно-аппаратного комплекса «Интеллект» российской компании ITV. В состав данной системы входят:

- контроллеры,
- персональные идентификаторы,
- считыватели персональных идентификаторов,
- исполнительные механизмы,
- автоматизированные рабочие места (АРМ),
- программное обеспечение, ведущее базу данных и производящее обработку поступающей информации.
- Локальная вычислительная сеть (ЛВС) СКУД

Посредством локальной вычислительной сети обеспечивается объединение автоматизированных рабочих мест (АРМ) и серверов.

ЛВС СКУД обеспечивает объединение АРМ и сервера для циркуляции информации между центральной проходной, проходной №2, бюро пропусков, серверной и корпусами предприятия. Связь обеспечивается через коммутаторы в корпусах с помощью оптоволоконного кабеля, между проходными, бюро пропусков, корпусами с помощью витой пары. ЛВС СКУД не связана с общей локальной сетью завода с целью повышения безопасности, нет выхода в интернет.[2]

К автоматизированным рабочим местам относятся:

- АРМ администратора безопасности (одно рабочее место);

Он необходим для настройки параметров системы и определения сценариев поведения систем в зависимости от возможных ситуаций. Также

[2] Белкин, П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов/ П.Ю. Белкин, О.О. Михальский, А.С. Першаков. –М.: Радио связь, 2020.-215 с.

определяются права доступа к ресурсам системы операторов и пользователей и т.д. АРМ состоит из системного блока, монитора, клавиатуры, мыши, и источника бесперебойного питания.

- АРМ бюро пропусков (2 рабочих места).

Происходит работа с базой данных работающих, командированных и посетителей: оформление постоянных, временных и разовых пропусков, внесение и корректировка их персональных данных. Оснащается оборудованием по изготовлению пропусков: принтер, цифровая фотокамера.

- АРМы контролеров проходных (2 рабочих места - центральная заводская проходная, 1 рабочее место - вторая проходная);

Производится контроль прохода работающих через точки доступа проходных (заводских и цеховых). При этом контролером осуществляется фотоидентификации (сравнение с фотографией владельца пропуска, появляющейся из базы данных при считывании пропуска) персонала, проходящего через проходную. При отрицательном результате фотоидентификации проход персонала через проходную может быть заблокирован контролером АРМ.

- АРМ корпусов находятся в коммуникационных помещениях. (5 рабочих мест);

Производится контроль прохода с помощью контроллера. Также производится видеозапись. Видеоархив хранится на видеосерверах.

На АРМ установлена операционная система Windows XP Professional, Windows 7 Professional. На сервере установлена операционная система Microsoft Windows 2003 Server.

В состав СКУД, в соответствии с задачами дипломного проекта, должны входить биометрические идентификаторы. Они необходимы для упорядочения допуска людей в режимные помещения и позволяют достичь таких целей, как:

- обеспечение санкционированного прохода сотрудников;

- предотвращение бесконтрольного проникновения лиц, не имеющих разрешение на проход;

Выбор и внедрение биометрических идентификаторов описаны в конструкторской и технологической частях данного дипломного проекта.

Анализ обрабатываемой информации и классификация ИСПДн

В СКУД циркулирует информация (идентификационный признак), на основе которой происходит идентификация пользователей СКУД. На основе федерального закона №152-ФЗ «О персональных данных» данная информация относится к персональным данным. Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Необходимо отметить, что до внедрения биометрических идентификаторов, ИСПДн СКУД ОАО «ММЗ» классифицировалась по классу К3. Определим, какая информация циркулирует в ИСПДн, включая биометрические данные. На основе этого проведем классификацию данной системы.[3]

В соответствии с приказом от 13 февраля 2008 года «Об утверждении порядка проведения классификации информационных систем персональных данных», персональные данные разделяются на четыре основные категории:

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни; *

- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

[3] Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин., Е.В.Куренков, А.В. Лысов. -СПб.: Полигон, 2020. –886 с.

- категория 4 - обезличенные и (или) общедоступные персональные данные.

В ИСПДн СКУД машиностроительного завода обрабатываются ПДн 2 категории:

- Ф.И.О.;

- паспортные данные;

- занимаемая должность;

- биометрические данные;

- фотография.

Для классификации ИСПДн СКУД ОАО «ММЗ», в соответствие с ФЗ №152, кроме категории ПДн необходимо проанализировать следующие исходные данные:

- объём обрабатываемых ПД (количество субъектов, персональные данные которых обрабатываются в ИС);

- заданные владельцем информационной системы характеристики безопасности персональных данных, обрабатываемых в ИС;

- структура информационной системы;

- наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена;

- режим обработки ПД;

- режим разграничения прав доступа пользователей информационной системы;

- местонахождение технических средств ИС.

В ИСПДн СКУД машиностроительного завода одновременно обрабатываются персональные данные около 5000 субъектов персональных данных, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию. ИСПДн представляет собой комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа, не имеющий подключения к сетям международного

информационного обмена. В ИСПДн используется многопользовательский режим обработки персональных данных с разграничением прав доступа. Следовательно, ИСПДн СКУД машиностроительного завода можно присвоить класс К2.[4]

1.2 Классификация АС

С целью повышения безопасности информации необходимо использовать комплексную защиту, которая включает в себя средства от НСД. Для того, чтобы внедрить программно-аппаратные средства от НСД необходимо определить класс АС.

На основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

В СКУД имеются различные категории пользователей и обслуживающего персонала, которые обладают разными полномочиями по доступу к АРМ, обрабатывающим ПДн.

Доступ к информационным ресурсам, содержащим ПДн, осуществляется сервер согласно таблице разграничения прав доступа для каждого пользователя. Нагляднее всего это демонстрирует матрица доступа.

[4] Ворона, В.А. Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. - М.: Горячая линия - Телеком, 2010. - 272 с.

Следовательно, автоматизированная система обработки конфиденциальной информации «Система контроля и управления доступом» является многопользовательской с разными правами доступа. На основании этого АС «СКУД» можно присвоить класс 1Г.

Модель нарушителя

Модель нарушителя представляет собой некое описание типов злоумышленников, которые намеренно или случайно, действием или бездействием способны нанести ущерб информационной системе.

Определим нарушителей для ИСПДн СКУД ОАО «ММЗ» в соответствие с документом «Базовая модель угроз безопасности ПДн» от 15.02.2008 года.

Нарушители по данному документу классифицируются на внешних и внутренних. Внутреннего нарушителя в свою очередь можно разделить на несколько групп:

1. Лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступ к ПДн.
2. Зарегистрированный пользователь информационных ресурсов, имеющий ограниченные права доступа к ПДн ИСПДн с рабочего места
3. Пользователь информационных ресурсов, осуществляющие удаленный доступ к ПДн по ЛВС.
4. Зарегистрированный пользователь с полномочиями системного администратора ИСПДн.
5. Зарегистрированный пользователь с полномочиями администратора безопасности ИСПДн.
6. Программисты - разработчики прикладного ПО и лица, обеспечивающие его сопровождение в ИСПДн.
7. Программисты - разработчики прикладного ПО и лица, обеспечивающие поставку, сопровождение в ИСПДн.
8. Другие категории лиц в соответствии с оргштатной структурой ИСПДн.

Внешними нарушителями в нашей системе могут быть:

- криминальные структуры;

- внешние субъекты (физические лица);

- конкуренты (конкурирующие организации);

- недобросовестные партнеры.

К внутренним нарушителям можно отнести: программистов, обслуживающих ПО СКУД «Интеллект»; работников бюро пропусков, которые непосредственно вводят ПДн в СКУД; работников охраны, имеющие доступ к ПДн на КПП, администратора сети, обслуживающий нормальное функционирование ЛВС; другие работники, имеющие доступ в КЗ, но не имеющие доступ к ПДн.[5]

Определим к какой категории каждый нарушитель относится.

Работники, имеющие доступ в КЗ, но не имеющие доступ к ПДн. Данный нарушитель может производить съем информации с помощью ПЭМИН. Данного нарушителя не берем во внимание, так как предотвращение съема информации по ПЭМИН является темой отдельно дипломного проекта.

Охрана и администратор сети относятся к первой категории и имеют санкционированный доступ к ИСПДн, но не имеют доступа к ПДн.

Лицо этой категории, может:

- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

- располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;

- располагать именами и вести выявление паролей зарегистрированных пользователей;

---

[5] Расчет естественного освещения: Методические указания к выполнению практических работ и дипломного проектирования для студентов всех специальностей очной и заочной формы обучения. - Изд. 4-е, переработанное. /Сост. Т.Н. Мазуркина, О.А. Глухов, Н.А. Филина. - Йошкар-Ола: МарГТУ, 2019 г. - 52 с.

Работники бюро пропускного режима относятся ко второй категории. Это зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

Программисты - пятая категория (зарегистрированные пользователи с полномочиями системного администратора ИСПДн).

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

Из вышеизложенного следует, что нарушитель ИСПДн СКУД ОАО «ММЗ» относится к 5 категории.

Возможные угрозы в ИСПДн.[6]

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Существует методика по определению угроз информационной безопасности и построения частной модели угроз. Она описана в документе ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена 14 февраля 2008 г. Актуальной считается только та угроза, которая может быть реализована с информационной системе и представляет опасность для защищаемых сведений. Поэтому в модели угроз опишем только те, которые относятся к нашей информационной системе и являются актуальными. Угрозы безопасности и определение их актуальности описаны в таблице 1.

Таблица 1

угрозы безопасности	степень опасности Y1	вероятность реализации Y2	коэффициент реализуемости	возможность реализации	степень актуальности
1. утечка акустической (речевой) информации - перехват информации, содержащейся непосредственно в произносимой реи;	Н	2	06	средняя	неактуальная
2. утечка	Н	2	0,6	средняя	неактуальная

[6] Торокин, А.А. Инженерно-техническая защита информации: Учебное пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. - М.: Гелиос АРВ, 2018. - 960 с.

акустической (речевой) информации - перехват информации, воспроизводимой акустическими средствами АС;					
3. утечка видовой информации - просмотр информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения, входящих в состав АС;	Н	2	0,6	средняя	неактуальная
4. перехват информации с использованием специальных электронных устройств съема информации внедренных в ОТСС;		0	0,5	средняя	неактуальная
5. перехват информации с использованием специальных электронных устройств съема информации внедренных в ВТСС;	Н	0	0,5	средняя	неактуальная
6. перехват информации с использованием специальных электронных устройств съема информации внедренных в помещения;	Н	0	0,5	средняя	неактуальная
7. утечка информации по каналу ПЭМИН - перехват ПЭМИ ТС обработки информации;	Н	0	0,75	высокая	актуальная

8. утечка информации по каналу ПЭМИН - наводки на ВТСС;	Н	0	0,75	высокая	актуальная
9. утечка информации по каналу ПЭМИН - наводки на линии, инженерные конструкции, выходящие за пределы КЗ;	Н	5	0,75	высокая	актуальная
10. НСД к информации, обрабатываемой в АРМ - действия нарушителей при непосредственном доступе к АС;	Н	5	0,75	высокая	актуальная
11. НСД к информации, обрабатываемой в АРМ, по средствам внедрения аппаратных закладок;	Н	5	0,5	высокая	актуальная
12. Угрозы, реализуемые в ходе загрузки ОС и направленные на перехват паролей и идентификаторов, модификацию базовой системы ввода / вывода (BIOS), перехват управления загрузкой;	Н	5	0,5	высокая	актуальная
13. Угрозы, реализуемые после загрузки ОС и направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.)	Н	5	0,75	высокая	актуальная

ОС или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)					
14. Внедрение вредоносных программ;	Н	5	0,75	высокая	актуальная
15. угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;	Н	2	0,6	средняя	неактуальная
16. угрозы выявления паролей;	Н	2	0,6	средняя	неактуальная
17. угрозы удаленного запуска приложений;	Н	2	0,6	средняя	неактуальная
18. угрозы внедрения по сети вредоносных программ.	Н	2	0,6	средняя	неактуальная

Для того чтобы произвести анализ рисков (таблица 4), необходимо проанализировать виды угроз, описанные в таблице.

Расчет риска происходит по следующей схеме:

Риск = Величина потерь * Вероятность реализации угрозы

Величина потерь - неотрицательное число. В таблице 2 представлена шкала для определения возможного ущерба. А шкала для определения вероятности угроз в таблице 3.

Таблица 2

Величина потерь	Описание ущерба от реализации угрозы
0	Реализации угрозы приведет к ничтожному ущербу

1	Основная деятельность не будет затронута. Финансовых потерь не будет, возможные последствия учтены в бюджете или предприняты меры по переносу риска
2	Деятельность организации прервется на некоторое время. Будут затронуты внутренние функции организации, превышен бюджет, потеряны возможности получить прибыль
3	Будут затронуты внешние функции организации, нанесен большой финансовый ущерб. Возможна утрата части партнерских связей
4	На восстановление требуются крупные финансовые вложения, деятельность прерывается на длительный срок, возможна смена руководства
5	Деятельность прекращается, невосполнимый ущерб

Таблица 3

Вероятность реализации угрозы	Средняя частота появления
0	Данный вид атаки отсутствует вообще
1	Реже, чем 1 раз в год
2	Около 1 раза в год
3	Около 1 раза в месяц
4	Около 1 раза в неделю
5	Ежедневно

Таблица 4

Описание угрозы	Ущерб	Вероятность	Риск

1. утечка информации по каналу ПЭМИН - перехват ПЭМИ ТС обработки информации;	1	2	2
2. утечка информации по каналу ПЭМИН - наводки на ВТСС;	1	2	2
3. утечка информации по каналу ПЭМИН - наводки на линии, инженерные конструкции, выходящие за пределы КЗ;	1	2	2
4. НСД к информации, обрабатываемой в АРМ - действия нарушителей при непосредственном доступе к АС;	2	5	10
5. Угрозы, реализуемые в ходе загрузки ОС и направленные на перехват паролей и идентификаторов, модификацию базовой системы ввода / вывода (BIOS), перехват управления загрузкой;	2	5	10
6. Угрозы, реализуемые после загрузки ОС и направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) ОС или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	2	5	10
7. Внедрение вредоносных программ;	2	5	10
Итого:	46		

Суммарный риск подсчитывается как сумма максимальных величин риска для каждой угрозы.

Максимальный риск - это риск, который понесет организация при осуществлении всех угроз. Максимальный риск рассчитывается как произведение суммарной цены всех угроз (11) на максимальную величину возможности реализации угрозы (5). Максимальный риск составляет 55 ед.

Соответственно, среднее значение частоты осуществления угроз можно определить, как частное от суммарного риска и суммарной цены всех

угроз. Среднее значение частоты возникновения угроз Рср=55/46=1,2. т.е., исходя из методики и шкалы, различные угрозы осуществляются около одного раза в год.[7]

Для снижения рисков, во-первых, предлагается введение организационно-правовых мер. Однако одних организационно-правовых мер для обеспечения защиты информации недостаточно, необходимо также использовать и программно-аппаратные средства защиты.

Понизить вероятность риска, а, следовательно, и уменьшить предполагаемый ущерб, можно потратив некоторую денежную сумму на построение системы защиты.

Комплексная система защиты должна уменьшать вероятность риска таким образом, чтобы затраты на её внедрение и эксплуатацию, не превышали возможного ущерба от угроз на информацию, которую она защищает.

[7] Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов - 3-е изд. / В.И. Ярочкин - М.: Трикста, 2019 г. – 678 с.

ГЛАВА 2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ

2.1 Организационные мероприятия по защите ПДн в ИСПДн СКУД машиностроительного завода

Предмет контракта: выполнение работ по защите биометрических данных в ИСПДн СКУД завода.

Защите подлежат персональные данные в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О защите персональных данных»

Состав работ:

1. Разработка Перечня информационных систем персональных данных (ИСПДн):

- Анализ структуры информационных систем, с целью выделения независимых ИСПДн.

- Сбор необходимых исходных данных для классификации ИСПДн.

2. Разработка Модели Угроз

Разработка модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных СКУД, во исполнение требованиями подпункта «а» пункта 12 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года №781, в соответствии с требованиями методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации:

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК 14 февраля 2008 года.

- «Базовая модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных», утверждена заместителем директора ФСТЭК 15 февраля 2008 года.

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 центра ФСБ №149/5-144 от 21 февраля 2008 года.

3. Классификация ИСПДн

Сбор и анализ исходных данных по ИСПДн СКУД.

Определение категории обрабатываемых в информационной системе персональных данных и других необходимых критериев для классификации ИСПДн, в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. №55/86/20.

По результатам анализа, на основе модели угроз безопасности персональных данных определение класса специальных информационных систем и подготовка актов классификации систем.

4. Внедрение биометрических считывателей для режимных помещений в СКУД, с целью дополнительного контроля санкционированного допуска и предотвращение несанкционированного прохода.

5. Разработка положения об обработке и защите персональных данных.

Положение об обработке и защите персональных данных должно быть разработано в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах

персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года №781, а также в соответствие с требованиями методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

6. Сбор и анализ имеющихся и используемых СЗИ, в том числе СКЗИ. Определение класса СВТ в соответствие с регламентирующими документами Федеральной службы по техническому и экспортному контролю Российской Федерации.

7. Разработка и сравнительный анализ вариантов реализации системы защиты персональных данных.

На основе результатов работ будет принято решение о необходимости, варианте и порядке реализации системы защиты персональных данных для информационной системы персональных данных.

безопасность биометрический информационный предприятие

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 бессмысленными.

С одной стороны, организационные мероприятия должны быть направлены на обеспечение правильности функционирования механизмов защиты, и выполняться администратором безопасности системы. С другой стороны, 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.[8]

К организационным мерам можно отнести такие, как:

- идентификация пользователей ИС по паролю;

- регистрация входа \ выхода пользователей в ИС;

[8] Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов - 3-е изд. / В.И. Ярочкин - М.: Трикста, 2019 г. - 544 с.

- 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, 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 администратора (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 ПДн;

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

В организации должны быть разработаны такие документы, как:

- положение о работе с персональными данными;

- инструкция администратора 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 (Приложение №8):

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

- порядок передачи персональных данных третьим лицом;

- гарантии конфиденциальности персональных данных.

В инструкции администратора 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 администратора по контролю за деятельностью пользователей ИСПДн, в частности, разработка и внедрение системы паролей доступа пользователей, организация разграничения доступа пользователей к техническим средствам защиты ИСПДн и информационным ресурсам ИСПДн, выявление допущенных пользователями нарушений инструкций и приостановление / прекращение их доступа в ИСПДн;

- 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 ИСПДн;

- ответственность за несоблюдение установленных правил работы в ИСПДн.

Такие документы, как положение о парольной защите, положение об антивирусной защите и регламент проведения проверок безопасности ИСПДн носят технический характер и составляются в соответствии необходимым уровнем обеспечения безопасности ИСПДн, обусловленного ее классом.

2.2 Физические мероприятия по защите информации в ИСПДн

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 - это очевидный, но в тоже время очень важный аспект безопасности, поскольку физическая незащищенность сервера ведет к большому риску, который может выразиться в неавторизованном доступе к нему и его порче, что повлияет на целостность сервера, всей сети и ее ресурсов.

В первую очередь надо подготовить помещение, где будут стоять серверы. Обязательное правило: сервер должен находиться в отдельной комнате, доступ в которую имеет строго ограниченный круг лиц. 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, а с другой стороны являться неприметной для злоумышленника, существенно не отличаясь от остальных дверей.

Всё оборудование в серверной 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.

Разумным шагом станет отключение неиспользуемых дисководов, параллельных и последовательных портов сервера. Его корпус желательно опечатать. Все это осложнит кражу или подмену информации даже в том случае, если злоумышленник каким-то образом проникнет в серверную комнату. Не стоит пренебрегать и такими тривиальными мерами защиты, как железные решетки и двери, кодовые замки и камеры видеонаблюдения, которые будут постоянно вести запись всего, что происходит в ключевых помещениях офиса.

Защита помещений

Основным моментом физической 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. Методом противодействия может служить сопровождение человека от вахты до того места, куда он направляется и обратно. Также следует опасаться стажеров и людей, приходящих на собеседование в компанию. На окнах обязательно должны быть жалюзи. На двери необходимо установить кодовые замки. Ключи от помещения с рабочими компьютерами должны выдаваться сотрудникам, согласно утвержденному списку. Данные помещения не должны оставаться незапертыми при отсутствии в них сотрудников даже на короткое время.

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. Но в любом случае, методы защиты архивной копии должны не уступать методам защиты основного источника информации.

Важное правило: резервные копии нельзя хранить в одном помещении с сервером. Часто об этом забывают и в результате, защитившись от информационных атак, фирмы оказываются беззащитными даже перед небольшим пожаром, в котором предусмотрительно сделанные копии гибнут вместе с сервером.

Защита компьютеров от неполадок в электросети

Сейчас, в начале нового века, как и во времена появления лампочки Ильича, главной особенностью сетей электроснабжения является невозможность обеспечения их надежной и стабильной работы.

Поддерживать стандартные параметры напряжения, частоты, высокочастотных шумов и т.д. не удается по многим причинам. Эта проблема актуальна и для самых развитых стран. 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 чувствительной техники. По сообщениям специалистов IBM, в среднем бывает до 120 нарушений электроснабжения в месяц. Ни для кого не секрет, что качество современных силовых сетей далеко от идеального. Даже если нет никаких внешних признаков аномалий, очень часто напряжение в электросети выше или ниже нормы. Нарушения в системе электроснабжения могут нанести ущерб, нанесенный, например, банковской сети или сети научного учреждения, даже трудно подсчитать. Дело не в стоимости оборудования, а в потере ценнейших данных. Для борьбы с этими проблемами разработано специальное оборудование. Поэтому необходимо для каждого компьютера использовать источник бесперебойного питания.

Часто, даже защитив серверы, забывают, что в защите нуждаются и всевозможные провода - кабельная система сети. Причем, нередко приходится опасаться не злоумышленников, а самых обыкновенных уборщиц, которые заслуженно считаются самыми страшными врагами локальных сетей. Лучший вариант защиты кабеля - это короба, но, в принципе, подойдет любой другой способ, 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. Хотя, надо признать, что этот вариант мало распространен и замечен лишь при нарушениях работы крупных фирм - в этих случаях игра с законом стоит свеч. 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, не стоит этим пренебрегать.

2.3 Система охранно-пожарной сигнализации

Охранно-пожарная сигнализация - получение, обработка, передача и представление в заданном виде потребителям при помощи технических средств информации о пожаре или проникновении злоумышленника на охраняемый объект.

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. И чем раньше обнаружится возникающая угроза объекту, тем эффективнее ее можно пресечь. 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: извещатели (датчики), концентраторы, устройства оповещения и реагирования. Извещатели, 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 извещателей 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 охранно-пожарной сигнализации генерируют в охраняемой зоне сигнал и реагируют на изменение его параметров. Пассивные извещатели реагируют на изменение параметров окружающей среды, вызванное вторжением нарушителя или возгоранием.

Каждая охранно-пожарная сигнализация использует охранные и пожарные извещатели, контролирующие различные физические параметры.

Широко используются такие типы охранных извещателей, как инфракрасные пассивные, магнитоконтактные, 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 извещатель 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.[9]

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 извещателя.

Акустические извещатели 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. Извещатель обрабатывает эти 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.

---

[9] Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие/В.А. Глатенко.-ИНТУИТ, 2019.-264 с.

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.

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.

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.

Современная аппаратура охранно-пожарной сигнализации имеет собственную развитую функцию оповещения. Несмотря на то, что системы оповещения о пожаре выделены в самостоятельный класс оборудования, на

базе технических средств пожарной сигнализации достаточно многих производителей можно реализовывать системы оповещения 1 и 2 категории.

Пожарные оповещатели предназначены для оповещения о пожаре с помощью различных звуковых и световых сигналов. Для звуковой сигнализации применяются звуковые сирены различных типов. Для световой сигнализации применяются различные световые оповещатели, выполненные на основе ламп накаливания, светодиодов и импульсных газоразрядных источников света.

На предприятии существует система охранно-пожарной сигнализации, управляемая при помощи пультов охранной сигнализации С-2000. В качестве магнитоконтактных извещателей используются «С2000-СМК». Рассмотрим ОПС бюро пропусков, кабинет администратора безопасности СКУД и серверная. Извещатели «С2000-СМК» устанавливаются на всех дверях для защиты от незаконного проникновения в помещения. В нерабочее время необходим охранный объемный оптико-электронный адресный извещатель «С2000-ИК исп. 02». Он установлен во всех помещениях.

В бюро пропусков имеют доступ все посетители, поэтому обеспечивается дополнительная защита данного помещения. Для этого на окна установлены «С2000-СТ» для обнаружения разбития стекла.

ГЛАВА 3. БИОМЕТРИЧЕСКИЕ ИДЕНТИФИКАТОРЫ С СКУД

3.1 Обзор рынка биометрических считывателей

Многолетний мировой опыт применения метода идентификации по отпечаткам пальцев и интенсивные разработки в области создания различных электронных датчиков, проводимые в последнее время, привели к тому, что в настоящее время этот метод рассматривается как достаточно надежный и относительно недорогой способ идентификации личности.

В системе идентификации по отпечатку пальцев всегда присутствует датчик для снятия отпечатка пальца, база данных, содержащая в каком-либо виде эталонный экземпляр (образец) отпечатка пальца и вычислитель, который работает по определённому алгоритму выделения характерных особенностей отпечатка и записи полученных значений в базу данных, которая может быть, как внутренней, по отношению к вычислителю, так и внешней. Такая система для связи с внешними устройствами может также иметь различные интерфейсы, например, USB, Ethernet, RS-232/485. Эти и другие параметры (например, совместимость со СКУД на предприятии) будут учитываться при выборе биометрического идентификатора для обеспечения контроля доступа в режимные помещения машиностроительного завода.

Биометрический считыватель для СКУД компании Sagem MA500+.

Программируемый считыватель отпечатков пальцев Sagem MA500+ предназначены для контроля доступа в помещения или в сети на основе биометрической идентификации или верификации отпечатков пальцев. Эти устройства имеют встроенную базу данных на 3000 пользователей и осуществляют верификацию и идентификацию в базе на 1000 шаблонов за 0,9 с. Каждый считыватель отпечатков пальцев оснащен оптическим сканером с разрешением 500 точек на дюйм, многоцветным светодиодным индикатором и многотоновым зуммером. MA500+ поддерживают протоколы Wiegand, Clock&Data, RS-422/RS485, TCP/IP и UDP, могут работать автономно или подключаться к контроллеру СКУД, а также получать электропитание от внешнего источника или по сети Ethernet (POE).

Каждый считыватель отпечатков пальцев этой серии оснащен клавиатурой с 12 клавишами для набора PIN-кода и настройки, а также 4 функциональными клавишами, которые предназначены для быстрого вызова предварительно запрограммированных функций. Текущая информация о процессе идентификации / верификации отображается на графическом LCD-дисплее 128x64 пикс.

Удаленное управление считывателем отпечатков, в том числе запрос файла отчета, изменение конфигурационных настроек, обновление ПО считывателя и работа с биометрической БД может осуществляться по TCP/IP или USB. При этом считыватель отпечатков пальцев может работать как автономное устройство или в составе СКУД. В случае работы MA500+ в автономном режиме, управление исполнительным устройством СКУД (электромеханический замок, турникет и др.) осуществляется через релейный выход устройства.

Режимы работы считывателя Sagem MA500+: Идентификация 1:N и Верификация 1:1.

Если MA500+ работает в составе СКУД, то возможны две типовые конфигурации системы:

В первом варианте, для достижения высокого уровня безопасности, вы можете подключить каждый считыватель отпечатков пальцев к контроллеру СКУД, например, через интерфейс Wiegand.

Во втором варианте считыватели MA500+ могут подключаться к ПК не через контроллеры, а напрямую по TCP/IP или через порт USB. Такая конфигурация может использоваться как для СКУД, так и в системах учета рабочего времени.

Благодаря внутреннему ПО, считыватели отпечатков пальцев MA500+ позволяют настраивать уровень надежности идентификации / верификации в зависимости от специфики объекта и задач.

Специализированное ПО MEMS обслуживает считыватели отпечатков пальцев Sagem, установленное на подключенной к сети рабочей станции, позволяет осуществлять назначение временных зон, синхронизацию баз данных считывателей с базой данных сервера, формирование отчетов, а также управление группами считывателей. К этой рабочей станции можно подключить сканер отпечатков пальцев MorphoSmart и устройство печати карт. ПО MEMS поддерживает Microsoft Access и SQL Server, причем при использовании SQL Server возможна работа в режиме «клиент-сервер», что позволяет осуществлять централизованное управление базами данных.

Опционально данный биометрический идентификатор оснащается бесконтактными считывателем карт доступа стандартов Mifare и DESFire.

Биометрический считыватель RWKLB575 HID Global Corporation.

Считыватель RWKLB575 предназначен для аутентификации персонала по отпечаткам пальцев в системах контроля доступа и учета рабочего времени. RWKLB575 считывает любые iCLASS-идентификаторы с объемом памяти 16 Кб и может перезаписывать информацию, хранящуюся в их памяти. Этот биометрический считыватель имеет интерфейсы Wigand, USB, RS-485, выход «открытый коллектор», оснащен постоянным магнитом и совместим со стандартными электрическими коробами. Он надежно

работает от источника постоянного тока 9-12 В при температурах от 0 до +45 градусов Цельсия.

Данный биометрический считыватель относится к линейке оборудования bioCLASS компании HID Global Corporation и представляет собой интегрированное устройство, объединяющее оптический сканер отпечатка пальцев BIO500 и перезаписывающий iCLASS-считыватель RWRL550, оснащенный 12-кнопочной клавиатурой и ЖК-дисплеем. RWKLB575 осуществляет сличение снятого сканером отпечатка пальца предъявителя iCLASS-идентификатора с шаблоном отпечатка, записанным в память этого идентификатора. Для аутентификации в СКУД (системе контроля и управления доступом) сотрудник компании должен поднести идентификатор к считывателю и затем приложить указательный палец на биометрический сканер. Для допуска посетителей и гостей в охраняемое помещение биометрический считыватель может работать и в «гостевом» режиме.

В настоящее время использование отпечатка пальца сотрудника в качестве идентификационного признака признано наиболее надежным для ограничения доступа, поскольку этот параметр отличается минимальной биологической повторяемостью (менее <0,00001%), временной устойчивостью, сложностью подделки и малым «весом» шаблона для записи на идентификатор. Применяемая в RWKLB575 биометрическая технология Identix Incorporated, делает этот биометрический считыватель независимым от мелких повреждений кожи пальцев человека, а также от температуры и влажности воздуха в помещении.

Благодаря схемотехническому решению этот биометрический считыватель с клавиатурой позволяет комбинировать три метода идентификации персонала в СКУД и выбирать один из трех режимов прохода: по iCLASS-идентификатору и PIN-коду (гостевой режим), по iCLASS-идентификатору и отпечатку пальца или по iCLASS-идентификатору, отпечатку пальца и PIN-коду. ЖК-дисплей RWKLB575

отображает последовательность набора команд и правильность ввода PIN-кода, а также точность расположения пальца на биометрическом сканере. Кроме того, биометрический считыватель оснащен трехцветным светодиодным индикатором и многотоновым зуммером, обеспечивающих визуальный и звуковой контроль рабочих состояний считывателя.

Встроенный Wigand-интерфейс позволяет соединять биометрический считыватель HID с контроллерами СКУД большинства известных производителей. Через интерфейс USB считыватель может локально подключаться к компьютеру для перезаписи информации в базу данных, что требуется, например, для учета рабочего времени сотрудников компании. Наличие в RWKLB575 интерфейса RS-485 позволяет создавать последовательную сеть из несколько считывателей, подключаемых к компьютеру через общий контроллер. Построенная по этой схеме биометрическая СКУД, обслуживается одним компьютером и имеет общую базу данных, что особенно удобно для крупных организаций, сотрудники которых имеют доступ только на определенные объекты.

Возможность записи и хранения шаблонов отпечатков пальцев не на считывателе, а на идентификаторе исключает необходимость прокладки дополнительных кабелей для пересылки биометрических шаблонов между считывателем и контроллером, что снижает затраты на монтаж и инсталляцию СКУД. Считыватели в такой сети соединяются между собой кабелем «витая пара», общая длина которого может достигать 1200 м.

Как и большинство считывателей HID, биометрический считыватель RWKLB575 оснащен постоянным магнитом, на базе которого можно создать магнитоконтатный датчик контроля целостности конструкции. Для этого используется магнитоуправляемый элемент - геркон, который монтируется в стену напротив магнита. При несанкционированном вскрытии конструкции биометрического считывателя магнитное поле изменяется, контакты геркона размыкаются и генерируется сигнал тревоги.

Биометрический считыватель ZK Software F702S.

Биометрический считыватель F702S предназначен для работы в составе автономной или сетевой системы контроля доступа с программированием с помощью встроенной клавиатуры. При этом централизованная система контроля доступа может быть организована на базе русифицированного ПО, которое входит в комплект поставки считывателя и может поддерживать неограниченное число считывателей по сети Ethernet или по шинам RS-232 и RS-485. Данное ПО позволяет программировать считыватели, вводить пользователей с учетом уровней их доступа, выполнять мониторинг СКУД в режиме реального времени, формировать отчеты и выводить на монитор охраны фотографии.

Считыватель F702S оснащен базой данных на 1500 шаблонов отпечатков пальцев. Он имеет Wiegand-интерфейс, благодаря которому считыватель можно использовать в системах контроля доступа большинства производителей, поддерживающих обмен данными между контроллером и считывателем по протоколу Wiegand. При этом Wiegand формат может произвольно конфигурироваться пользователем с длиной кода от 26 до 64 бит.

В зависимости от конфигурации СКУД биометрический считыватель может работать в режиме идентификация 1:N (только отпечаток пальца) или в режиме верификация 1:1 (ПИН плюс отпечаток пальца или карта плюс отпечаток пальца). Кроме того, F702S поддерживает идентификацию пользователя по ПИН-коду плюс код, по карте плюс код или только по карте. Для реализации определенных режимов верификации или идентификации можно использовать опциональный встроенный считыватель или подключить внешний.

Возможен автономный режим работы считывателя, т.е. без его подключения к сети Ethernet. В этом случае F702S программируется не с помощью ПО, а данные переносятся с помощью USB-накопителя. Бесплатное ПО ZK Software, установленное на подключенной к сети рабочей станции, позволяет осуществлять назначение временных зон, синхронизацию

баз данных считывателей с базой данных сервера, формирование отчетов, а также управление группами считывателей.

Функциональные параметры на биометрические считывателя F702S:

1. ЖК-дисплей с поддержкой русского языка

2. Релейный выход управления замком

3. Датчик вскрытия корпуса

4. Вход для подключения кнопки выхода

5. Вход для подключения датчика положения двери

6. Wiegand вход / выход

7. Общий тревожный выход и выход для подключения дверного звонка

8. 2 функциональные клавиши для выбора типа события для системы учета рабочего времени (приход / уход)

9. Поддержка кода принуждения

10. Опционально: Поддержка кода работ, web-сервер, считыватель карт EM, Mifare, HID.

Биометрический считыватель системы контроля

Считыватели ST-FR020EM выполняют идентификацию персонала по отпечаткам пальцев и по проксимити картам стандарта EM. Эти устройства могут использоваться для организации автономной системы контроля доступа и программироваться локально через систему голосового меню. Кроме того, ST-FR020EM могут работать в составе централизованной сетевой СКУД, при этом их программирование выполняется с помощью специализированного ПО.

Централизованная система контроля доступа может быть организована либо на базе программного обеспечения «Таймекс» с подключением исполнительных устройств непосредственно к данному считывателю, либо путем интеграции ST-FR020EM в любую стороннюю СКУД.

Для интеграции считывателя ST-FR020EM в сторонние системы контроля доступа используется интерфейс Wiegand. При этом пользователь может произвольно конфигурировать выходной Wiegand формат устройства с длиной кода от 26 до 64 бит. Бесплатная версия ПО «Таймекс» обеспечивает программирование считывателей, ввод пользователей с учетом уровней доступа и формирование отчетов.

ST-FR020EM рассчитан на обслуживание до 600 шаблонов отпечатков пальцев. Таким образом, если на каждого человека заносится по 2 шаблона, то общее количество пользователей составит 300. При этом устройство поддерживает такие режимы распознавания пользователя, как идентификация по пальцу или по карте. Наличие у ST-FR020EM Wiegand входа позволяет подключить к нему внешний проксимити считыватель или дополнительный биометрический.

Функциональные возможности:

11. Контроллер с поддержкой всех функций контроля доступа
12. Металлический корпус
13. Высокий уровень погодозащищенности
14. Сенсор со стеклянной призмой
15. Релейный выход управления замком и общий тревожный выход
16. Вход подключения кнопки выхода и вход датчика положения двери, датчик вскрытия
17. Wiegand выход / выход, USB порт (host)
18. Поддержка отпечатка пальца прохода по принуждению
19. Голосовые инструкции на русском языке

3.2. Выбор биометрического считывателя

Исходя из технических характеристик, выполняемых функций и экономической составляющей вопроса из рассматриваемых биометрических считывателей для контроля доступа в режимные помещения был выбран ZK Software F702S с возможностью считывания HID карт.

Биометрический считыватель F702S известного производителя ZK Software обеспечивает ограничение доступа в помещения по отпечаткам пальцев и способен работать как автономно, так и в составе на базе ПО «Интеллект».

Для централизованного конфигурирования биометрических устройств по Ethernet или RS232/485 все считыватели и терминалы ZKSoftware комплектуются русифицированным программным обеспечением. Это ПО позволяет запрограммировать уровни доступа и временные зоны для каждого сотрудника компании, а также использовать в системе контроля доступа режим фотоверификации. Благодаря наличию в программе отчетов по проходам через биометрические считыватели, резервированию БД и менеджменту пользователей (добавление, удаление и редактирование записей), на базе этого ПО можно построить простейшую систему безопасности объекта.

Данный считыватель по сравнению с другими обладает высокой функциональностью по доступной цене (15000 рублей - это почти в три раза меньше, чем аналогичный продукт от компании Sagem). Имеющаяся встроенная база данных на 1500 биометрических шаблонов, достаточна для того чтобы внести необходимое количество пользователей для прохода в режимные помещения. Также необходимо отметить, что F702S единственный работает с HID-картами, которые уже используются на предприятии, что сокращает расходы на приобретение новых видов карт.

F702-S - биометрический терминал контроля производится с применением надежных комплектующих и соблюдением стандартов безопасности. Широко используется для организации систем контроля доступа в офисах, гостиницах, фабриках, заводах, общественных заведениях. Перед продажей изделие подвергается полному и строгому тестированию всех функций.

Терминал доступа имеет возможность подключения кнопки открытия двери, считывателя, электронного замка, звонка, аларма.

Технические характеристики:

1. Аппаратная платформа: ZEM500
2. Операционная система: Linux
3. Количество пользователей: 1500
4. Количество записей: 50000
5. Сенсор: ZK сенсор
6. Зоны контроля доступа: 50 временных зон, 5 групп, 10 комбинаций, Управление праздниками, работа в сети или автономное использование
1. Соединение: TCP/IP, RS232, RS485
2. Дисплей: LCD, 80 символов
3. Питание: 12 В
4. Скорость идентификации: <2 с
5. FRR/FAR: <1%/<0.0001%
6. Вход и Выход: Weigand Подключение терминала к контроллеру, подключение считывателя к терминалу
7. Проводной звонок: Да
8. Температура эксплуатации: 0-45 гр. С, влажность 20-80%

ZK Software F702S встраиваются в уже имеющуюся систему контроля и управления доступом. Всего биометрических идентификаторов необходимо 35 штук, которые устанавливаются на вход в режимные помещения. В отделе испытаний и научно-техническом центре с помощью данных считывателей осуществляется двойное распознавание (карта + отпечаток пальца), в других помещениях только по отпечатку пальца.

3.2 Обзор рынка программно-аппаратных средств защиты от НСД

Одно из приоритетных направлений по улучшению системы защиты информации является установка на компьютеры программно-аппаратных

комплексов защиты от НСД. При выборе средств защиты необходимо обратить внимание на наличие сертификатов ФСТЭК.

Также критерием отбора является наличие у продукта следующих характеристик:

- контроль целостности информации;
- контроль и разграничение доступа;
- наличие подсистемы аудита;
- возможность шифрования трафика сети;
- дополнительная идентификация пользователей;
- затирание остатков информации в системе.

Dallas Lock 7.7

Система Dallas Lock 7.7 представляет собой программное средство защиты от НСД к информации в персональном компьютере с возможностью подключения аппаратных идентификаторов. Система предназначена для защиты компьютера, подключенного к локальной вычислительной сети, от несанкционированного доступа в среде XP/2003/Vista/2008/7.

Dallas Lock 7.7 обеспечивает многоуровневую защиту локальных ресурсов компьютера:

- запрет загрузки компьютера посторонними лицам;
- двухфакторная авторизация по паролю и аппаратным идентификаторам (USB eToken, смарт-карты eToken, Rutoken, Touch Memory);
- разграничение прав пользователей на доступ к локальным и сетевым ресурсам;
- контроль работы пользователей со сменными накопителями;
- мандатный и дискреционный принципы разграничения прав;
- организация замкнутой программной среды;
- аудит действий пользователей;
- контроль целостности ресурсов компьютера;

- очистка остаточной информации;

- возможность автоматической печати штампов (меток конфиденциальности) на всех распечатываемых документах;

- защита содержимого дисков путем прозрачного преобразования;

- удаленное администрирование

- выделенный центр управления, работа в составе домена безопасности (v7.5/7.7);

- возможность установки на портативные компьютеры (Notebook);

- отсутствие обязательной аппаратной части;

- работа на сервере терминального доступа;

- удобные интерфейс, установка и настройка.

СЗИ Dallas Lock 7.7 блокирует доступ посторонних лиц к ресурсам ПК и позволяет разграничить права пользователей и администраторов при работе на компьютере. Контролируются права локальных, сетевых и терминальных пользователей. Разграничения касаются прав доступа к объектам файловой системы, доступа к сети, к сменным накопителям и к аппаратным ресурсам.

Для идентификации пользователей служат индивидуальные пароли и аппаратные идентификаторы Touch Memory, eToken, ruToken (двухфакторная аутентификация). Аппаратная идентификация не является обязательной - система может работать в полностью программном режиме.

Запрос пароля и аппаратных идентификаторов происходит до начала загрузки ОС. Загрузка ОС возможна только после проверки идентификационных данных пользователя в СЗИ. Таким образом обеспечивается доверенная загрузка системы.

Разграничение прав доступа к ресурсам файловой системы реализуется следующими методами:

- Дискреционный - предоставляет доступ к защищаемым объектам файловой системы на основании списков контроля доступа. В соответствии с содержимым списков определяются права доступа для каждого пользователя.

- Мандатный - каждому пользователю присваивается максимальный уровень мандатного доступа. Пользователь получает доступ к объектам, мандатный уровень которых не превышает его текущий уровень.

СЗИ позволяет контролировать целостность файлов, папок и параметров аппаратно-программной среды компьютера. Для контроля целостности используются контрольные суммы, вычисленные по одному из алгоритмов на выбор: CRC32, MD5, ГОСТ Р34.11-94.

Подсистема аудита действий пользователей состоит из шести журналов, в которые заносятся события и результат (с указанием причины, при отказах) попыток входов и выходов пользователей, события доступа к ресурсам файловой системы, события запуска процессов, события печати на локальных и сетевых принтерах, события по администрированию СЗИ. Для облегчения работы с журналами, реализована возможность фильтрации записей по определенным признакам и экспорт журналов в формат MS Excel.

Подсистема очистки остаточной информации гарантирует невозможность восстановления удаленных данных.

Возможно очищение освобождаемого дискового пространства, файла подкачки, освобождаемой памяти и заданных папок при выходе пользователя из системы. Подсистема может работать в автоматическом режиме, когда зачищаются все удаляемые данные, либо данные зачищаются по команде пользователя.

Подсистема перехвата событий печати позволяет на каждом распечатанном с ПК документе добавлять штамп. Формат и поля штампа могут гибко настраиваться.

Для защиты от загрузки компьютера и доступа к информации в обход СЗИ предусмотрена возможность преобразования содержимого диска в «прозрачном» режиме. Информация преобразуется при записи и декодируется при чтении с носителя. При работе процесс преобразования незаметен для пользователя. После преобразования диска получить доступ к хранящейся на нем информации невозможно без пароля для входа в СЗИ.

Режим «прозрачного» преобразования диска защищает информацию, даже если жесткий диск будет подключен к другому компьютеру. Данные могут быть преобразованы по алгоритмам XOR32 или ГОСТ 28147-89.

СЗИ предоставляет возможность преобразования отдельных файлов и / или папок. В качестве ключа преобразования используется пароль и, по желанию пользователя, аппаратный идентификатор. Преобразованные данные хранятся в файле-контейнере, который может использоваться для безопасной передачи данных или хранения информации на отчуждаемом носителе. Доступ к преобразованным данным можно получить с любого компьютера с СЗИ при совпадении пароля и аппаратного идентификатора.

Возможно использование встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего сертифицированного криптопровайдера (например, «КриптоПро»).

Для предотвращения утечки информации через сменные накопители, предусмотрена возможность гибкого разграничения доступа к дискетам, оптическим дискам, USB-Flash - возможно разграничения доступа по типу накопителя, либо к конкретным экземплярам.

Система позволяет настраивать замкнутую программную среду (режим, в котором пользователь может запускать только программы, определенные администратором).

Для осуществления централизованного управления защищенными компьютерами в составе ЛВС, в состав системы входит «Сервер Безопасности» (СБ). СБ Dallas Lock и зарегистрированные на нем компьютеры с Dallas Lock образуют «Домен Безопасности». При использовании СБ возможно централизованное управление учетными записями пользователей, управление политиками безопасности, просмотр и автоматический сбор журналов, назначение прав доступа к ресурсам, управление прозрачным преобразованием и выполнение команд оперативного управления.

С помощью модуля «Менеджер серверов безопасности» возможно объединение нескольких СБ в «Лес Безопасности», с помощью которого осуществляется централизованное управления несколькими Доменами Безопасности (получение журналов, управление политиками и учетными записями пользователей).

Возможна установка СЗИ на портативные компьютеры (ноутбуки).

Существует возможность просматривать экранные снимки удаленных компьютеров. Эти снимки могут быть сохранены в файлы и просмотрены в дальнейшем.

Возможна установка СЗИ на компьютеры, работающие в составе домена (как на клиентские машины, так и на контроллер домена, таким образом с помощью Dallas Lock 7.7 можно защитить всю сеть.

Возможна установка на сервер терминального доступа.

Сертификат соответствия ФСТЭК №2209 удостоверяет, что система защиты информации от несанкционированного доступа Dallas Lock 7.7 является программным средством защиты информации от несанкционированного доступа к информационным ресурсам компьютеров и соответствуют требованиям руководящих документов Гостехкомиссии России по 2-му уровню контроля отсутствия недекларированных возможностей и 3-му классу защищенности от НСД. Версия продукта может использоваться для защиты государственной тайны категории «совершенно секретно» (АС до класса защищенности «1Б» включительно), а также для защиты информации (персональных данных) в ИСПДн до 1 класса включительно.

КСЗИ «ПАНЦИРЬ-К»

Система предназначена для защиты информации, обрабатываемой на автономном компьютере, либо на компьютерах в составе корпоративной сети. КСЗИ служит для эффективного противодействия, как известным, так и потенциально возможным атакам на защищаемые ресурсы, что

обеспечивается устранением архитектурных недостатков защиты современных ОС.

КСЗИ может применяться для защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечивая эффективное противодействие атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве).

КСЗИ также может использоваться для эффективного противодействия вирусным атакам и шпионским программам.

В части дополнительной защиты конфиденциальности информации в КСЗИ реализованы возможности гарантированного удаления остаточной информации и шифрования данных «на лету» (шифрование файлов и дисков, локальных, съемных, сетевых).

Система реализована программно (опционально может использоваться аппаратная компонента защиты), содержит в своем составе клиентскую и серверную части (для реализации АРМа администратора безопасности в составе сети).

Основные механизмы защиты КСЗИ реализованы в виде системных драйверов. Все возможности защиты, предоставляемые КСЗИ, реализованы собственными средствами (не использованы встроенные механизмы ОС).

Основные механизмы защиты, реализованные в КСЗИ «Панцирь-К»:

1. Механизмы разграничения доступа к локальным и разделенным в сети ресурсам - к файловым объектам, к объектам реестра ОС, к внешних накопителям, к принтерам, к сетевым хостам и др.;

2. Механизм включения в разграничительную политику субъекта «процесс», как самостоятельного субъекта доступа к ресурсам, принципиально расширяющий функциональные возможности защиты и противодействующий атакам на расширение привилегий;

3. Механизм управления подключением устройств;

4. Механизм обеспечения замкнутости программной среды, позволяющий локализовать среду исполнения для пользователей, в частности противодействующий запуску троянских и шпионских программ;

5. Механизмы контроля целостности файловых объектов (программ и данных) и контроля корректности функционирования КСЗИ;

6. Механизм авторизации, позволяющий подключать аппаратные средства ввода парольных данных (eToken и др.);

7. Механизм контроля корректности идентификации субъекта доступа к ресурсам (контроль олицетворения);

8. Механизм противодействия ошибкам и закладкам в системном и в прикладном ПО;

9. Механизм шифрования данных, реализующий ключевую политику, обеспечивающую невозможность несанкционированно раскрыть похищенную информацию (в том числе и собственно пользователем, ее обрабатывающим - инсайдером), даже при наличии у похитителя ключа шифрования.

Сертификат ФСТЭК России №1973

КСЗИ «ПАНЦИРЬ-К» для ОС Windows 2000/XP/2003VISTA/2008 /Windows 7 (в т. ч. для 64-х-битных систем), сертифицированная по 5 классу СВТ и 4 уровню контроля НДВ, собственными средствами реализует все технические требования, регламентируемые для АС класса защищенности 1Г), а также для защиты информации (персональных данных) в ИСПДн до 1 класса включительно.

Secret Net 6.5

Secret Net 6 - это комплексное решение, сочетающее в себе необходимые возможности по защите информации, средства централизованного управления, средства оперативного реагирования и возможность мониторинга безопасности информационной системы в реальном времени.

Тесная интеграция защитных механизмов Secret Net с механизмами управления сетевой инфраструктурой, повышает защищенность информационной системы компании в целом.

ЗАКЛЮЧЕНИЕ

Целью представленной дипломной работы являлась разработка комплекса мер по защите биометрических ПДн.

Защита ПДн - весьма сложная, требующая комплексного, системного подхода проблема. В связи с этим было проведено тщательное аналитическое исследование данной предметной области, в ходе которого были выявлены

угрозы ПДн и составлена модель вероятного нарушителя с точки зрения физической и технической защиты ПДн.

На основе проведенного аналитического исследования были предложены решения по оснащению объекта программно-аппаратными средствами защиты ПНд для ИСПДн СКУД организации. Доработана СКУД с помощью биометрических считывателей отпечатков пальцев. В ходе подготовки дипломной работы также были предложены организационные меры обеспечения безопасности ПДн, базирующиеся на пакете разработанных документов для данного предприятия. Также была рассмотрена физическая защита помещений от несанкционированного доступа.

Таким образом, в данной дипломной работе изложен комплекс мер, охватывающий программно-аппаратное и нормативно-правовое обеспечение безопасности ПДн. На основании вышесказанного можно сделать вывод, что поставленные цели, были достигнуты, а задачи выполнены.

В завершение хотелось бы подчеркнуть, что обеспечение безопасности персональных данных является не правом организации, а ее обязанностью, установленной законом «О персональных данных» и регламентированной рядом подзаконных актов. Данный блок нормативных правовых актов призван реализовать конституционные права граждан на неприкосновенность их частной жизни, личную и семейную тайну, закрепленные в ст. 23 Конституции Российской Федерации. Несоблюдение организацией требований по обеспечению безопасности персональных данных может повлечь не только ущерб для самой организации, но, в первую очередь, привести к нарушению конституционных прав граждан, повлечь за собой череду гражданско-правовых исков со стороны физических лиц, чьи права могут оказаться нарушенными, и, даже привлечение к административной или уголовной ответственности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты:

1. ФЗ «О государственной тайне».
2. Федеральный закон от 27.07.2018N 152-ФЗ (ред. от 21.07.2019) «О персональных данных».
3. ФСТЭК, приказ No 17 от 11.02.2017.

4. ГОСТ Р 50922-2018 «Защита информации. Основные термины и определения».

Литература:

5. Поляков А.В. Метод идентификации личности по отпечаткам пальцев на основе сферического локально-чувствительного хэширования // Программная инженерия, 2018, № 5, с. 207-214.

6. Поляков А.В. Биометрическое личностное шифрование // Интеллектуальные системы. Теория и приложения, 2018, том 21, № 1, с. 149-163.

7. Аверченков, В.И. Криптографические методы защиты информации/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак, –Брянск: БГТУ, 2020. –216 с.

8. Аверченков В.И. Организационная защита информации: учеб. Пособие для вузов/В.И. Аверченков, М.Ю.Рытов. –Брянск: БГТУ,2018. –184 с.

9. Баймакова, И.А. Обеспечение защиты персональных данных: методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев, А. Х. Хыдыров. - М.: 1С-Паблишинг, 2017. - 216 с.

10. Белкин, П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов/ П.Ю. Белкин, О.О. Михальский, А.С. Першаков. –М.: Радио связь, 2020. -215 с.

11. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. –СПб.: Изд-во СПбГУЭФ, 2021. –96 с.

12. Болдырев, А.И. Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практ. Пособие/ А. И. Болдырев –М.: НЕЛК, 2019. –137 с.

13. Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин., Е.В.Куренков, А.В. Лысов. -СПб.: Полигон, 2020. –886 с.

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

15. Государственная тайна в Российской Федерации: учеб-методич. пособие/ под ред. М.А.Вуса. –СПб. Изд-во С.-Петерб. ун-та, 2020. –330 с.

16. Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие/В.А. Глатенко.-ИНТУИТ, 2019.-264 с.

17. Расчет естественного освещения: Методические указания к выполнению практических работ и дипломного проектирования для студентов всех специальностей очной и заочной формы обучения. - Изд. 4-е, переработанное. /Сост. Т.Н. Мазуркина, О.А. Глухов, Н.А. Филина. - Йошкар-Ола: МарГТУ, 2019 г. - 52 с.

18. Торокин, А.А. Инженерно-техническая защита информации: Учебное пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. - М.: Гелиос АРВ, 2018. - 960 с.

19. Ушаков, И.П. Организационно-экономическое обоснование курсового и дипломного проектов: учеб. пособие / И.П. Ушаков. - Йошкар-Ола: МарГТУ, 2019. - 87 с.

20. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов - 3-е изд. / В.И. Ярочкин - М.: Трикста, 2019 г. - 213 с.

21. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов - 3-е изд. / В.И. Ярочкин - М.: Трикста, 2019 г. – 678 с.

22. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов - 3-е изд. / В.И. Ярочкин - М.: Трикста, 2019 г. - 544 с.

23. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

24. РД 78.36.006-2005 «Выбор и применение технических средств охраны и средств инженерно-технической укрепленности для оборудования объектов».

25. ГОСТ 12.1.004-91. ССБТ. Пожарная безопасность. Общие требования.

Интернет – ресурсы:

26. Страж NT. Система защита информации. [Электронный ресурс] - Режим доступа: http://www.guardnt.ru/strazh30.html

27. Центр защиты информации. Конфидент. [Электронный ресурс] - Режим доступа: http://www.confident.ru/isc/index.php? id=34

28. ОКБ САПР. ПАК СЗИ НСД Аккорд. [Электронный ресурс] - Режим доступа: http://www.accord.ru/accords.html

29.Сайт «Биометрические системы». − http://www.bio5.ru

2.Сайт «BioLink Solutions». − http://biolinksolutions.com 3.Сайт «Прософт-Биметрикс». − http://www.bio-smart.ru 4.Сайт «Контроль безопасности системы». − http://www.r-control.ru 5.Сайт «Фрилансим». − http://habrahabr.ru