

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

**ЗАДАНИЕ
НА ВЫПОЛНЕНИЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

СамГТУ 100301.043.014.01 ТЗ

Обучающемуся Самойловой Дарье Владимировне, 4 курс, ИАИТ, 2 группа
(фамилия, имя, отчество, курс, факультет, группа)

Тема Обеспечение безопасности данных методом их подмены
(полное название темы квалификационной работы, в соответствии с приказом об утверждении тем ВКР)

Исходные данные (или цель работы) Разработка комплекса мер, обеспечивающего безопасность информации, методом ее подмены
(наименование объекта исследования; производительность или нагрузка, режим работы; вид сырья или материал изделия; требования к продукту, изделию или процессу; особые условия функционирования или эксплуатации объекта в части требований к безопасности эксплуатации, экологической и экономической целесообразности, оптимальным энергозатратам и т.д.)

Перечень подлежащих исследованию, разработке, проектированию вопросов:

Наименование вопроса	Результаты освоения ОПОП
1. Постановка цели и задач для ВКР	ОК-1, ОК-3, ОК-6
2. Аналитический обзор угроз информационной безопасности и методов защиты от них	ОПК-1, ОК-7, ОК-8
3. Определение объекта и способа его защиты	ОПК-4, ПК-5, ПК-1
4. Разработка структуры комплекса мер, обеспечивающего защиту информации методом подмены	ПК-6, ОК-5, ОПК-2, ПК-2, ОК-2
5. Определение требований к разрабатываемому комплексу мер	ОПК-7, ПК-3, ПК-8
6. Разработка алгоритмов функционирования программы, реализующей метод подмены данных	ОПК-3, ОК-8, ОК-9, ПК-4
7. Оценка экономической эффективности разработки	ОК-4, ОПК-5
8. Изучение охраны труда и безопасности жизнедеятельности при разработке	ОПК-8, ОПК-9, ПК-7
(аналитический обзор литературных источников, постановка задачи исследования, разработки, проектирования; содержание процедуры исследования, разработки, проектирования; обсуждение результатов; дополнительные вопросы, подлежащие разработке; заключение и др.)	из ОПОП прилагается перечень запланированных образовательной программой результатов обучения (профессиональные компетенции, указываются шифры компетенций, через запятую в каждой графе)

Перечень презентационного материала:

1. Плакат «Классификация угроз информационной безопасности и методы защиты от них»
2. Плакат «Категории персональных данных и маскирование, как способ защиты»
3. Плакат «Организационная структура ПАО «Страховая компания «Спутник»
4. Плакат «Структура комплекса мер по защите персональных данных и необходимые требования»

5. Плакат «Алгоритмы функционирования программы, реализующей метод подмены данных»
6. Плакат «Примеры функционирования метода подмены информации»
7. Плакат «Оценка экономической эффективности разработки»

Нормоконтролер:

старший преподаватель, Н.В. Андреева
(должность, ф.и.о. нормоконтролера)

Дата выдачи задания:

« » _____ 20__ г.

Задание согласовано и принято к исполнению.

Руководитель

Н.Е. Карпова
(И. О. фамилия,
к.т.н., доцент
(должность, уч. степень, уч. звание)

(подпись, дата)

Студент

Д.В. Самойлова
(И. О. фамилия)
ИАИТ, 2 группа
(институт, группа)

(подпись, дата)

Тема утверждена приказом по СамГТУ № _____ от " ____ " _____ 20__ г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

Календарный план
выполнения выпускной квалификационной работы

Обучающегося Самойловой Дарьи Владимировны, 4 курс, ИАИТ, 2 группа
(фамилия, имя, отчество, курс, институт, группа)

Тема Обеспечение безопасности данных методом их подмены

(полное название темы квалификационной работы, в соответствии с приказом об утверждении тематики ВКР)

	Этапы выполнения ВКР	Дата (срок) выполнения		Отметка о выполнении
		план	факт	
	Разработка структуры ВКР. Проведение литературного обзора			
	Сбор фактического материала (лабораторные, исследовательские работы и др.)			
	Подготовка рукописи ВКР			
	Доработка текста ВКР в соответствии с замечаниями научного руководителя			
	Предварительная защита квалификационной работы на кафедре			
	Ознакомление с отзывом научного руководителя			
	Подготовка доклада и презентационного материала			

Студент Д.В. Самойлова

Руководитель к.т.н., доцент Н.Е. Карпова

Заведующий кафедрой П.О. Скобелев

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой _____ Скобелев П.О.

«___» _____ 20 г.

Выпускная квалификационная работа

СамГТУ 100301.043.014.02 ПЗ

Тема: _____ Обеспечение безопасности данных методом их подмены
(полное название темы квалификационной работы, в соответствии с приказом об утверждении
тем ВКР)

Обучающийся _____ Самойлова Дарья Владимировна, 4 курс, ИАИТ, 2 группа
(фамилия, имя, отчество, курс, факультет, группа)

Руководитель работы _____ к.т.н., доцент Н.Е. Карпова
(должность, подпись, дата, фамилия, инициалы)

Нормоконтролер _____ старший преподаватель Н.В. Андреева
(подпись, дата, фамилия, инициалы)

Консультант _____ старший преподаватель Н.В. Андреева
(подпись, дата, фамилия, инициалы)

Консультант _____ д.т.н., профессор Н.Г. Яговкин
(подпись, дата, фамилия, инициалы)

Самара 2021г.

РЕФЕРАТ

Пояснительная записка содержит 81 лист, 21 рисунок, 1 таблицу, 7 листов графического материала формата А1.

Целью данной выпускной квалификационной работы является разработка комплекса мер, обеспечивающего безопасность персональных данных, методом подмены информации.

Исходные данные: информационная система, пользователи информационной системы с разграниченными правами доступа, не защищенные персональные данные, хранящиеся в таблицах формата `xlsx`, угроза несанкционированного доступа.

В ходе выполнения выпускной квалификационной работы был реализован комплекс мер по защите информации, обеспечивающий защиту информации, методом ее подмены, а именно: проведен аналитический обзор угроз информационной безопасности и методов защиты от них, определен объект защиты и способ его защиты, разработан комплекс мер по защите информации, обеспечивающий защиту информации, произведена оценка экономической эффективности и рассмотрен вопрос безопасности жизнедеятельности.

При оценке экономической эффективности разработанного комплекса мер был рассчитан полный срок возмещения инвестиционных вложений.

Разработка комплекса мер, обеспечивающего защиту персональных данных, методом подмены информации проводилась в соответствии с требованиями по охране труда и безопасности жизнедеятельности на предприятии.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
ГЛАВА 1. АНАЛИТИЧЕСКИЙ ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ЗАЩИТЫ ОТ НИХ	7
1.1 Угрозы информационной безопасности	7
1.2 Источники угроз информационной безопасности	10
1.3 Методы защиты информационной безопасности	14
ГЛАВА 2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ОБЪЕКТ ЗАЩИТЫ	19
2.1 Основные понятия и виды персональных данных	19
2.2 Обработка персональных данных.....	23
ГЛАВА 3. МАСКИРОВАНИЕ ДАННЫХ, КАК СПОСОБ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	26
3.1 Понятие маскирования данных	26
3.2 Методы маскирования данных	27
ГЛАВА 4. РАЗРАБОТКА КОМПЛЕКСА МЕР, ОБЕСПЕЧИВАЮЩЕГО ЗАЩИТУ ИНФОРМАЦИИ, МЕТОДОМ ЕЕ ПОДМЕНЫ	34
4.1 Организационная структура ПАО «Страховая компания «Спутник». 34	
4.2 Требования к разрабатываемому комплексу мер	39
4.3 Структура комплекса мер, обеспечивающего защиту информации, методом ее подмены	42
4.4 Разработка алгоритмов функционирования программы, реализующей метод подмены информации	45
ГЛАВА 5. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ	57
5.1 Маркетинговый анализ	57

5.2	Расчёт затрат на разработку комплекса мер	58
5.3	Расчет экономической эффективности проекта	63
5.4	Заключение	68
ГЛАВА 6. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ И ОХРАНА ТРУДА.....		69
6.1	Проектирование производственной среды	69
6.2	Проектирование рабочего места.....	70
6.3	Выбор оборудования	73
6.4	Проектирование схемы подключения оборудования	74
ЗАКЛЮЧЕНИЕ.....		76
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ.....		77

ВВЕДЕНИЕ

В современном мире информационные технологии развиваются стремительными темпами, увеличивается количество и важность информации. Множество компаний каждый день хранит и обрабатывает данные различных видов, которые несут большую значимость для организации. В связи с этим на данный момент первостепенной задачей является обеспечение информационной безопасности. Для ее реализации: издаются новые указы, постановления, стандарты, разрабатываются различные системы и комплексы мер, которые позволяют избежать затрат, связанных с утечкой информации и ее распространением, а также обеспечить безопасность данных, их сохранность и целостность.

Большой значимостью на сегодняшний момент обладает информация, содержащая в себе сведения о жизни человека, то есть его персональные данные. Новые технологии, с одной стороны, существенно упростили сбор, обработку, хранение, передачу данных, а с другой - создали очевидные угрозы их незаконного оборота, что ведет к нарушениям прав личности.

Актуальность темы данной выпускной квалификационной работы определяется особой ценностью такой информации, как персональные данные человека, а также тем, что выбранный метод защиты конфиденциальных данных помогает обеспечивать безопасность данных, находящихся в не защищаемых файлах в ситуации, когда доступ к системе был скомпрометирован.

Цель выпускной квалификационной работы – разработка комплекса мер, обеспечивающего безопасность персональных данных, методом подмены информации.

Для реализации поставленной цели необходимо решить следующие задачи:

1. Провести аналитический обзор угроз информационной безопасности и методов защиты
2. Определение организационной структуры предприятия, а так же существующих на предприятии угроз и методов защиты
3. Разработать комплекс мер для обеспечения защиты информации
4. Провести оценку экономической эффективности разработанного комплекса мер
5. Обеспечить безопасность жизнедеятельности и охраны труда при разработке соответствующего комплекса мер

В рамках исследования выпускной квалификационной работы осуществляется защита персональных данных сотрудников организации ПАО «Страховая компания «Спутник», которые хранятся и обрабатываются в не защищенных файлах.

ГЛАВА 1. АНАЛИТИЧЕСКИЙ ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ЗАЩИТЫ ОТ НИХ

1.1 Угрозы информационной безопасности

В настоящее время невозможно представить жизнь человека без информационных технологий. Компьютеры находятся практически в каждой области человеческой деятельности, с их помощью возможно обеспечить хранение, обработку и передачу информации. Однако с увеличением степени информатизации возрастают риски снижения безопасности, доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

В соответствии с ГОСТ Р 50922-2006 «Угроза безопасности информации» представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Для того чтобы правильно определить возможные угрозы, в первую очередь, необходимо определить защищаемые объекты. К таким объектам могут относиться как материальные, так и абстрактные ресурсы, например, документы и другие носители информации, помещения, оборудование системы, а также сотрудники и клиенты. Важным этапом является рассмотрение и классификация угроз, которые могут повлиять на работу системы и организации в целом, а, порой, и привести к негативным последствиям. Такие угрозы можно разделить на следующие классы [9]:

- 1) По характеру нарушения:
 - Нарушение конфиденциальности данных;
 - Нарушение работоспособности ЭВМ;
 - Незаконное вмешательство в функционирование ЭВМ и т.д.

- 2) По тяжести нарушения:
 - Незначительные ошибки;
 - Мелкое хулиганство;
 - Серьезные преступления;
 - Природные и техногенные катастрофы.
- 3) По предвидению последствий нарушителем:
 - Намеренные нарушения;
 - Ненамеренные нарушения.
- 4) По мотивации:
 - Злонамеренные нарушения;
 - Незлонамеренные нарушения.
- 5) По месту возникновения:
 - Внешние угрозы;
 - Внутренние угрозы.
- 6) По законченности:
 - Реализованные;
 - Нереализованные.
- 7) По объекту воздействия:
 - Угрозы, нацеленные на всю информационную систему;
 - Угрозы, нацеленные на отдельные компоненты ИС.
- 8) По причине возникновения:
 - Угрозы, возникшие из-за недостаточности средств технической защиты;

- Угрозы, возникшие из-за недостаточности организационных мер.

9) По каналу проникновения:

- Угрозы, проникающие через уязвимости ПО, бесконтрольные съемные носители;

- Угрозы, проникающие через бреши в системах авторизации, недостатки систем хранения документов и т.д.

10) По виду реализации угрозы:

- Вредоносные программы, спам-письма, программные закладки, хакерские атаки;

- Уязвимые процедуры авторизации и другие регламенты информационной безопасности;

- Стихийные бедствия.

11) По происхождению:

- Антропогенные;

- Техногенные;

- Природные.

12) По размеру ущерба:

- Незначительные;

- Значительные;

- Критичные.

1.2 Источники угроз информационной безопасности

Еще одним важным этапом в построении систем информационной безопасности является рассмотрение источников угроз. Источники угроз для нарушения безопасности могут использовать различные уязвимости системы. В качестве таких источников могут выступать как субъекты (люди), так и объективные проявления, которые при этом могут находиться, как внутри компании, так и за ее пределами [16].

Деление источников на субъективные и объективные оправдано, исходя из того, что субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами. А объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могут быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы [14]:

- 1) Обусловленные действиями субъекта (антропогенные источники угроз);
- 2) Обусловленные техническими средствами (техногенные источники угрозы);
- 3) Обусловленные стихийными источниками.

Антропогенные источники угроз. [14]

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорить о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- 1) криминальные структуры;
- 2) потенциальные преступники и хакеры;
- 3) недобросовестные партнеры;
- 4) технический персонал поставщиков телематических услуг;
- 5) представители надзорных организаций и аварийных служб;
- 6) представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со

спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- 1) основной персонал (пользователи, программисты, разработчики);
- 2) представители службы защиты информации;
- 3) вспомогательный персонал (уборщики, охрана);
- 4) технический персонал (жизнеобеспечение, эксплуатация).

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Техногенные источники угроз. [14]

Данная группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними:

- 1) средства связи;
- 2) сети инженерных коммуникации (водоснабжения, канализации);
- 3) некачественные технические средства обработки информации;
- 4) некачественные программные средства обработки информации;
- 5) вспомогательные средства (охраны, сигнализации, телефонии);
- 6) другие технические средства, применяемые в учреждении.

Стихийные источники угроз. [14]

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:

- 1) пожары;
- 2) землетрясения;

- 3) наводнения;
- 4) ураганы;
- 5) различные непредвиденные обстоятельства;
- 6) необъяснимые явления;
- 7) другие форс-мажорные обстоятельства.

1.3 Методы защиты информационной безопасности

Для того, чтобы минимизировать риск несанкционированного доступа к охраняемой информации необходимо:

1. Обеспечить физическую безопасность.

Методы предотвращения угроз шпионажа и диверсий реализуют традиционный подход к обеспечению ИБ объектов. При защите процессов переработки информации в КС от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются КС.[11]

Применение системы охраны объекта основывается на следующих положениях:

Объект, на котором производятся работы с ценной конфиденциальной информацией, имеет, как правило, несколько рубежей защиты [11]:

1. контролируемая территория;
2. здание;
3. помещение;
4. устройство, носитель информации;
5. программа;
6. информационные ресурсы.

От шпионажа и диверсий необходимо защищать первые четыре рубежа и обслуживающий персонал.

Система охраны объекта (СОО) КС создается с целью предотвращения несанкционированного проникновения на территорию и в помещения объекта посторонних лиц, обслуживающего персонала и пользователей.

Состав системы охраны зависит от охраняемого объекта. В общем случае СОО КС должна включать в себя:

- инженерные конструкции;
- охранную сигнализацию;
- средства наблюдения;
- подсистему доступа на объект;
- дежурную смену охраны.

Для противодействия наблюдению злоумышленником, находящимся на объекте, необходимо, чтобы [11]:

- двери помещений были закрытыми;
 - расположение столов и мониторов ЭВМ исключало возможность наблюдения документов или выдаваемой информации на соседнем столе или мониторе;
 - стенды с конфиденциальной информацией имели шторы.
- Противодействие подслушиванию осуществляется при помощи методов, которые подразделяются на два класса:
- методы защиты речевой информации при передаче ее по каналам связи;
 - методы защиты от прослушивания акустических сигналов в помещениях.

Защита акустических сигналов в помещениях КС является важным направлением противодействия подслушиванию. Существует несколько методов защиты от прослушивания акустических сигналов [11]:

- звукоизоляция и звукопоглощение акустического сигнала;
- зашумление помещений или твердой среды для маскировки акустических сигналов;
- защита от несанкционированной записи речевой информации на диктофон;
- обнаружение и изъятие закладных устройств.

2. Обеспечить внешнюю безопасность. Первым «защитником сети», выступает межсетевой экран, обеспечивающий защиту от несанкционированного удалённого доступа. Сеть можно разделить на подсети для ограничения серверов от пользователей. Использование фильтрующего маршрутизатора, который фильтрует исходящие и входящие потоки. Все устройства подключение к сети будут иметь доступ в интернет, а обратно доступ к устройствам из Интернета блокируется.

3. Далее необходимо разграничить права доступа администратора и пользователей.

- Доступ к серверам не должен иметь рядовой пользователь;
- Доступ управления конфигурацией компьютеров должен иметь только администратор;
- Доступ к сетевым ресурсам должны иметь каждый там, где ему это необходимо для выполнения должностных обязанностей;
- Трафик всех сотрудников должен фильтроваться, и в этом поможет прокси-сервер;
- Каждый пользователь должен устанавливать сложный пароль, и не должен не кому его передавать. Даже IT специалисты его не знают.

4. Антивирусная защита является главным рубежом защиты корпоративной сети от внешних атак. Комплексная антивирусная защита минимизирует проникновения в сеть вирусов. В первую очередь необходимо защитить сервера, рабочие станции, шлюзы и систему корпоративной почты.

5. Соблюдение организационных мер. Все сотрудники компании, вне зависимости от должности должны понимать и главное соблюдать правила информационной безопасности. Любые посторонние файлы, скаченные из сети или из почты могут быть опасны и нести в себе угрозу, а так же внешние накопители информации, которые не относятся к рабочему процессу.

При построении конкретных систем компьютерной безопасности необходимо руководствоваться основными принципами организации защиты: системностью, комплексностью, непрерывностью защиты, разумной достаточностью, гибкостью управления и применения, открытостью алгоритмов и механизмов защиты и простотой применения защитных мер и средств [10], а также придерживаться рекомендаций, полученных на основе опыта предыдущих разработок.

Основными известными универсальными защитными механизмами являются [8]:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) и авторизация субъектов доступа;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;
- криптографическое закрытие, контроль целостности и аутентичности данных, хранимых в АС и передаваемых по каналам связи;
- контроль целостности ресурсов системы.

Эти универсальные механизмы защиты обладают своими достоинствами и недостатками и могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты.[8]

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.[8]

ГЛАВА 2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ОБЪЕКТ ЗАЩИТЫ

2.1 Основные понятия и виды персональных данных

В данной дипломной работе в качестве объекта защиты были выбраны персональные данные, так как если персональные данные используются произвольно и становятся доступными лицам, которым они не должны быть известны, гражданам наносится моральный вред и материальный ущерб. На текущий момент, характеризуемый быстрым развитием информационных процессов и технологий, на первый план встает вопрос защиты персональных данных при их накоплении, обработке и передаче с использованием средств информатизации. Таким образом, можно сделать вывод, что создание методов защиты персональных данных является актуальным.

В Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных» персональные данные – это информация, относящаяся к физическому лицу, т.е. фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы физического лица.

В состав персональных данных также подлежат включению такие сведения, связанные с поступлением на работу (службу), ее прохождением и увольнением; данные о супруге, детях и иных членах семьи обладателя, данные, позволяющие определить место жительства, почтовый адрес, телефон и иные индивидуальные средства коммуникации гражданского служащего, а также его супруги (ее супруга), детей и иных членов его семьи, данные, позволяющие определить местонахождение объектов недвижимости, принадлежащих гражданскому служащему на праве собственности или находящихся в его пользовании, сведения о доходах, имуществе и обязательствах имущественного характера, сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, сведения, ставшие известными работнику

органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, владение языками (родной язык, русский язык, другой язык или другие языки), образование общее (начальное общее, основное общее, среднее (полное) общее) и профессиональное (начальное профессиональное, среднее профессиональное, высшее профессиональное, послевузовское профессиональное), жилищные условия (тип жилого помещения, время постройки дома, размер общей и жилой площади, количество жилых комнат, виды благоустройства жилого помещения), источники средств к существованию (доход от трудовой деятельности или иного занятия, пенсия, в том числе пенсия по инвалидности, стипендия, пособие, другой вид государственного обеспечения, иной источник средств к существованию).

Персональные данные относятся к категории конфиденциальной информации, предполагающей отсутствие свободного доступа к ней и наличие эффективной системы ее защиты. Включение персональных данных в разряд конфиденциальных сведений направлено на предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в личную жизнь гражданина.

На сегодняшний день законодательство определяет различные категории персональных данных. К ним могут относиться общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах персональных данных (далее ИСПДн), биометрические ПДн и другие. Рассмотрим их более подробно.

1. Общедоступные ПДн

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования

соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

2. Специальные категории ПДн

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. [1] Их обработка допускается только в следующих случаях[1]:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

3. Категории персональных данных, обрабатываемых в ИСПДн

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет следующие категории персональных данных, которые обрабатываются в ИСПДн [2]:

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 ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 - персональные данные, позволяющие идентифицировать субъекта ПДн.

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

4. Биометрические персональные данные

Биометрические персональные данные - это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные

обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Исходя из определения биометрических ПДн, к ним относятся фотографии и видеозображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения - в системах видеонаблюдения и т.п.

2.2 Обработка персональных данных

При передаче, получении и обработке персональных данных необходимо соблюдать все существующие требования в существующем законодательстве.

В российском законодательстве определяются основные принципы обработки персональных данных. К ним относятся [1]:

- оператор персональных данных определяет цели их обработки в соответствии со своими полномочиями.
- объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки.

- недопустимо объединять созданные для разных целей персональные данные (например, в одну базу данных).

- персональные данные подлежат уничтожению по достижении целей (утраты необходимости в) их обработки.

Большое значение в Законе уделено условиям обработки персональных данных. Существует два вида обработки персональных данных: автоматизированный и неавтоматизированный. Так, обработка персональных данных может осуществляться оператором только с письменного согласия субъектов ПДн. Рассмотрим случаи, когда не требуется согласие субъекта ПДн на обработку сведений о нем:

- обработка персональных данных осуществляется на основании других федеральных законов, например, некоторыми Федеральными законами предусматриваются случаи обязательного предоставления субъектом ПДн своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

- оператор и субъект ПДн связаны договором на выполнение действий, которые требуют обработки персональных данных этого субъекта, например, договор, по которому туристическая фирма (оператор) имеет право использовать персональные данные субъекта для бронирования гостиницы;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение его согласия невозможно, например, госпитализация человека при несчастном случае;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;

- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

ГЛАВА 3. МАСКИРОВАНИЕ ДАННЫХ, КАК СПОСОБ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Понятие маскирования данных

Маскирование данных – это технология, позволяющая предотвратить неправомерное использование критичных данных с помощью предоставления пользователям неверных/фиктивных данных, но выглядящих правдоподобно (далее – реалистичных), вместо реальных данных.

Цель состоит в том, чтобы защитить конфиденциальные данные, предоставляя при этом функциональную альтернативу.

Процессы маскирования данных изменяют значения данных, используя тот же формат. Цель состоит в том, чтобы создать версию, которую нельзя расшифровать или реконструировать [17].

При выборе решения по маскированию данных необходимо руководствоваться спецификой решаемой задачи и следующим общим принципом: Если необходимо оградить сотрудников от лишней информации, содержащейся в ответах на запросы к базе данных, подбирайте решение из спектра инструментов динамического маскирования. Если стоит задача регулярно создавать копию реальной базы данных и отдавать ее разработчикам, своим сотрудникам или на аутсорсинг, надо подбирать решение для статического маскирования или разрабатывать скрипты. Самое главное — убедиться, что создаваемая копия структурно не отличается от исходной, а данные после маскировки, хоть и являются ложными, но по форме не отличаются от исходных и позволяют полноценно с ними работать.

Существует несколько причин, по которым маскирование данных важно для многих организаций:

- Маскирование данных устраняет несколько критических угроз - потерю данных, кражу данных, внутренние угрозы или компрометацию

учетной записи, а также небезопасные интерфейсы со сторонними системами.

- Снижает риски данных, связанные с внедрением облака.
- Делает данные бесполезными для злоумышленника, сохраняя при этом многие присущие им функциональные свойства.
- Позволяет обмениваться данными с авторизованными пользователями, такими как тестировщики и разработчики, не раскрывая производственные данные.
- Может использоваться для очистки данных - обычное удаление файлов по-прежнему оставляет следы данных на носителе, в то время как при очистке старые значения заменяются замаскированными.

3.2 Методы маскирования данных

Существуют различные подходы к маскированию. Они могут использовать как разные методы, так и различные схемы хранения данных и пополнения их набора для нужд тестирования. В частности, маскирование можно разделить на ручное и автоматическое, на статическое и динамическое. Тем временем, в качестве алгоритмов маскирования применяются методы псевдонимизации, обфускации и скремблирования. Выбор конкретного метода зависит от целей и особенностей использования маскированных данных. Автоматизированные системы маскирования становятся сегодня все более популярными, потому что они не только гарантируют повсеместные изменения записей, но могут самостоятельно обнаруживать конфиденциальную информацию, а также связанные с ней ключи и обращающиеся к ней приложения.

Самый распространенный вариант технической реализации статического маскирования — специализированные программы на отдельном сервере или виртуальная машина. В настройках указывается сетевой адрес базы данных с критичной информацией и учетные данные для доступа. Для определения полей, в которых хранятся критичные данные, проводится автоматизированный аудит. После этого выбирается метод маскирования. Система выполняет запросы к базе данных и, используя функции СУБД, либо маскирует непосредственно саму базу данных, либо создает копию с измененными данными.

Если компании необходимо передавать готовые копии определенных объемов данных подрядчикам для тестирования или анализа работы определенных приложений, для этого прекрасно подойдут системы создания статических наборов замаскированных данных. Автоматизированные системы могут самостоятельно определить чувствительную информацию в предоставленных БД, ориентируясь на заранее заданные шаблоны и правила. Специальные фрагменты или целые базы данных для неавторизованных пользователей формируются по запросу, и в каждую выгрузку закладывается определенный объем замаскированной информации, которая не соответствует реальным данным, но повторяет их формат.

Статическое маскирование — используется для защиты данных, хранящихся в тестовых средах.

Статическое маскирование — это необратимый процесс замены критичных данных на реалистичные, основанный на заданных правилах, при котором данные преобразуются в одном направлении, а первоначальные данные при этом не могут быть получены, извлечены или восстановлены.

Процесс статического маскирования данных специализированными средствами выглядит так:

- создание копии производственной базы данных сотрудниками с соответствующими правами доступа;
- урезание объёма содержащихся в базе данных сведений по настроенным правилам (при необходимости);
- поиск критичных данных в копии БД на основании заданных шаблонов поиска;
- маскирование найденных критичных данных по настроенным шаблонам и правилам;
- предоставление замаскированной копии базы данных разработчикам/тестировщикам.

Динамическое маскирование – предусматривает подмену критичных данных в режиме реального времени при обращении к производственной базе данных. Реальные данные не покидают базу данных; они заменяются на этапе запроса, например, на полностью реалистичные, без промежуточной записи.

Динамическое маскирование применяется в тех случаях, когда среды тестирования и разработки должны получать доступ к реальным корпоративным данным. Как правило, система динамического маскирования устанавливается в качестве еще одного виртуального сервера и «на лету» маскирует записи, предоставляя подрядчикам доступ к уже искаженным данным. При этом объем базы, и типовые характеристики записей остаются соответствующими реальности. Средства динамического маскирования также позволяют дифференцировать доступ к реальной базе данных и ее «поддельной» копии. То есть пользователи, которым действительно необходимо работать с реальными данными, получают доступ

к фактической БД, а те, у кого нет доступа, будут видеть поддельную базу данных, причем каждый — свою собственную.

Динамическое маскирование можно настроить для отдельных полей базы данных, чтобы скрыть конфиденциальные данные в результирующих наборах запросов. При использовании динамического маскирования данные в базе данных не изменяются. Данный тип маскирования легко использовать с существующими приложениями, так как правила маскирования применяются к результатам запроса.

Назначение динамического маскирования данных — ограничение раскрытия конфиденциальных данных, при котором пользователи, у которых нет доступа к данным, не смогут их просматривать. Динамическое маскирование данных не сможет помешать пользователям подключиться к базе данных напрямую и выполнить запросы для получения фрагментов конфиденциальных данных.

Методы маскирования данных [15].

Существует пять вариантов маскирования. Требования к маскированию определяют, какая из этих функций маскирования будет использоваться. Рассмотрим более подробное описание:

1. Замена

Замена является одним из самых эффективных способов маскировки, позволяющим сохранить исходный внешний вид данных. Например, если исходная таблица базы данных содержит записи с информацией о клиентах, то реальные имена и фамилии можно заменить именами и фамилиями, взятыми из специально созданного подготовленного файла. Так, на первом этапе маскировки все имена клиентов могут заменяться произвольными мужскими именами, на втором этапе можно произвести вставку женских имён в ячейки, соответствующие клиентам-женщинам с помощью

фильтрации списка клиента по ячейке с указанием пола. Применение подобного подхода к маскировке позволяет обеспечить должную анонимность записей и сохранить половое соотношение клиентов в замаскированной таблице. Важно, что база данных при этом выглядит реалистично, а факт маскировки информации не является очевидным.

Метод замены можно применять для полей базы данных, содержащих данные различного рода: например, телефонные номера, почтовые индексы, номера платёжных карт, страховых свидетельств и т. д. Важно, что в случае с номерами пластиковых карт, фиктивные номера должны успешно проходить проверку по алгоритму Луна.

В большинстве случаев файлы с фиктивными данными должны быть достаточно обширными, чтобы обеспечивать как можно большее количество вариаций, и при этом допускать возможность самостоятельного составления наборов данных для замены. Эти критерии являются ключевыми при выборе программного решения для маскировки данных.

2. Перемешивание

Перемешивание - очень распространённый способ маскировки данных. Он схож с методом замены, рассмотренным выше, но при перемешивании данные для замены берутся из той же колонки таблицы, что и исходные данные. Попросту говоря, данные в колонке перемешиваются случайным образом.

Метод перемешивания является отличным дополнением к другим методам маскировки данных и в определённых случаях позволяет получить некоторые преимущества.

3. Дисперсия числовых значений

Метод дисперсии разброса применяется при работе с полями БД, содержащими финансовую информацию и даты. Этот метод заключается в

отклонении замаскированного числового значения от исходного на определённую величину.

4. Шифрование

Шифрование - это наиболее сложный способ маскировки данных. Алгоритм шифрования обычно предполагает наличие "ключа", необходимого для дешифровки и просмотра исходных данных.

На первый взгляд, шифрование - это идеальное решение проблемы ограничения доступа к информации, но на практике "ключ" может быть передан сотруднику, не имеющему достаточных прав на просмотр данных, и это сводит на нет все усилия по маскировке.

Шифрование также может сопровождаться преобразованием исходных данных в бинарный вид, что способно вызвать проблемы в работе приложений. Для выявления и устранения конфликтов внутри приложений необходимо проводить тестирование с передачей исходной информации тестировщикам, а это, в свою очередь, предполагает проверку задействованных в тестировании IT-специалистов службой безопасности. Прекрасная, в теории, идея при реализации на практике вызывает массу сложностей: шифрование отнимает много времени на тестирование и устранение выявленных недостатков.

5. Редактирование/Обнуление

Иногда используется упрощённый метод маскировки данных, заключающийся в замене символов в записи БД нулями или произвольными символами например, астерисками или "X". Очевидно, что этот способ позволяет лишь скрыть, а не замаскировать исходное значение. Практически во всех случаях подобный подход снижает степень целостности данных, поскольку вызывает проблемы с валидацией данных приложениями. Кроме

того, "неестественные" значения в записях БД явно свидетельствуют о том, что к таблице применена маскировка.

Чаще всего этот способ маскировки применяется в процессе работы с платёжными картами.

ГЛАВА 4. РАЗРАБОТКА КОМПЛЕКСА МЕР, ОБЕСПЕЧИВАЮЩЕГО ЗАЩИТУ ИНФОРМАЦИИ, МЕТОДОМ ЕЕ ПОДМЕНЫ

4.1 Организационная структура ПАО «Страховая компания «Спутник».

ПАО «Страховая компания «Спутник» оказывает услуги в сфере страхования.

Общество осуществляет обработку персональных данных на основании: Федерального Закона Российской Федерации № 152 «О персональных данных» от 27 июля 2016 года;

- Налогового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Трудового кодекса Российской Федерации;
- Закона Российской Федерации № 4015-1 «Об организации страхового дела в Российской Федерации» от 27.11.1992 года;
- Устава Общества;
- Лицензий Общества;
- Договоров страхования и иных договоров, а так же трудовых договоров, заключенных с субъектами персональных данных;
- Письменного согласия субъектов персональных данных на обработку их персональных данных.

Для осуществления своей деятельности ПАО «Страховая компания «Спутник» производит обработку персональных данных сотрудников, клиентов и связанных с ними лиц.

В ПАО «Страховая компания «Спутник» не производится обработка персональных данных не совместимая с целями обеспечения его видов деятельности. По окончании обработки персональных данных, они хранятся

в организации не менее пяти лет, после чего уничтожаются или обезличиваются.

При обработке персональных данных компанией обеспечиваются их точность, достаточность и актуальность по отношению к целям обработки. В частности, при каждом обращении проводится обновление и верификация его персональных данных.

Для хранения, обработки персональных данных клиентов в компании разработана «Политика в отношении обработки персональных данных публичного акционерного общества «страховая компания «Спутник», в которой прописаны основные положения, принципы и условия хранения и обработки персональных данных, права и обязанности операторов и субъектов ПДн, а также меры, по защите ПДн.

В данной «Политике в отношении обработки персональных данных ...» разработана модель угроз безопасности персональных данных при их обработке в информационной системе, по результатам которой было установлено следующее:

1. Структура информационной системы – локальная, включающая автоматизированные рабочие места и серверы, имеющие подключение к сетям связи общего пользования и (или) сетям международного обмена (информационно-телекоммуникационной сети «Интернет»).

2. Режим обработки персональных данных в информационной системе - многопользовательский.

3. Угрозы информационной системы:

а) Угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями оператора используемой

информационной системы, посредством которой в т.ч., обрабатываются персональные данные, при создании, эксплуатации, техническом обслуживании и (или) ремонте, модернизации, снятия с эксплуатации такой информационной системы;

b) Угроза воздействия вредоносного кода, внешнего по отношению к используемой информационной системе, где в т.ч. обрабатываются персональные данные;

c) Угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;

d) Угроза несанкционированного доступа к съемным носителям персональных данных;

e) Угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;

f) Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями оператора информационной системы, при помощи уязвимостей в организации защиты персональных данных;

g) Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями оператора информационной системы, при помощи уязвимостей в программном обеспечении информационной системы персональных данных;

h) Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями оператора информационной системы, при помощи уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

i) Угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями оператора информационной

системы, при помощи уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;

ж) Информационная система компании включает следующие подсистемы и файлы, участвующие в обработке ПД:

к) Подсистема для ведения бухгалтерского и налогового учёта, оперативного учёта деятельности организации на основе программной платформы 1С.

л) Подсистема управленческого учета, посредством которой автоматизируется оформление организуемых кооперативом операций финансовой взаимопомощи, формируются базы данных, используемые в целях статистического учета и анализа.

м) Файлы Excel, содержащие персональные данные сотрудников, состоящие из: ФИО, номер контактного телефона, пол, адрес проживания и регистрации, а также сведения о семейном положении, образовании, фотографическое изображение, занимаемая должность.

4. Меры по защите информации:

1) Производится охрана периметра организации;

2) Ведется видеонаблюдение;

3) Используются сертифицированные средства защиты информации в составе системы защиты персональных данных;

4) Назначены уполномоченные сотрудники, ответственные за обеспечение безопасности информации;

5) Осуществляется контроль соблюдения требований обеспечения безопасности информации;

6) Ограничен состав работников, обрабатывающих персональные данные и установлены правила доступа к персональным данным;

7) Определены места хранения материальных носителей, содержащих персональные данные;

- 8) Ограничен доступ в помещения, в которых хранятся материальные носители, содержащие персональные данные;
- 9) Ведётся список сотрудников, обладающих доступом к материальным носителям, содержащим персональные данные;
- 10) Проведены мероприятия по технической защите персональных данных;
- 11) Применяется межсетевое экранирование;
- 12) Ведётся обнаружение вторжений в корпоративную сеть Общества, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- 13) Производится резервное копирование информации;
- 14) Производится обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- 15) Осуществляется регистрация и учёт действий пользователей информационных систем персональных данных;
- 16) Используются антивирусные средства и средства восстановления;
- 17) Осуществляется аутентификация пользователей при запуске рабочего компьютера;
- 18) Обеспечивается учёт и хранения материальных носителей персональных данных и установлен порядок обращения с ними, направленный на предотвращение их хищения, подмены, несанкционированного копирования и уничтожения;
- 19) Проводится проверка готовности и эффективности использования средств защиты информации;
- 20) Реализована парольная защита доступа пользователей к информационной системе персональных данных;
- 21) Реализовано разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации;

22) Применяются средства контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;

23) В необходимых случаях применяются средства криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи;

24) Осуществляется централизованное управление системой защиты персональных данных.

На рисунке 4.1 представлена структура информационной сети ПАО «Страховая компания «Спутник».

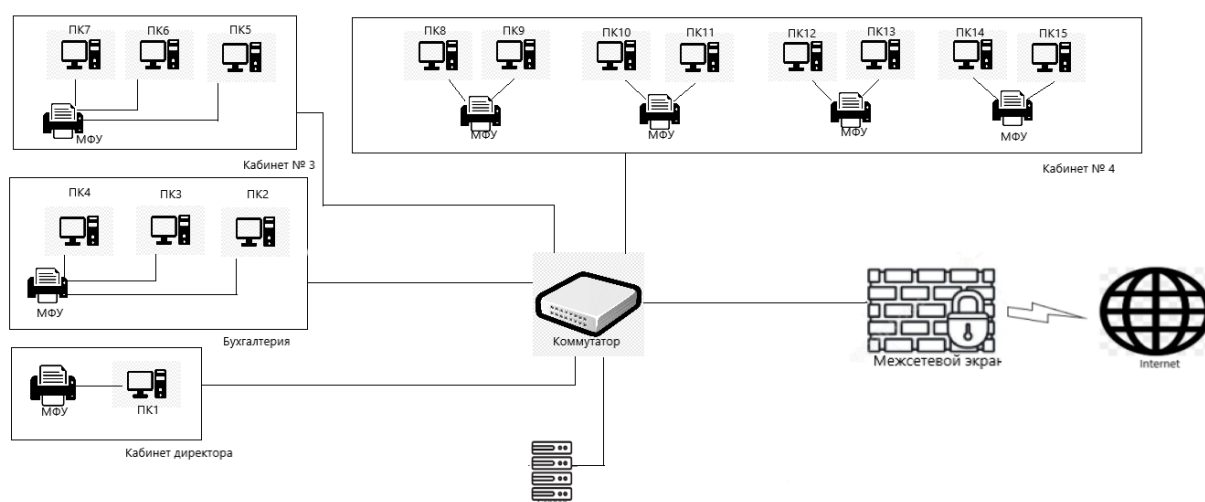


Рисунок 4.1 – Структура информационной сети

4.2 Требования к разрабатываемому комплексу мер

Для применения и правильного функционирования созданного комплекса мер по защите ПДн сотрудников организации ПАО «Страховая компания «Спутник» необходимо составить ряд требований.

Разработанный комплекс мер по защите персональных данных Сотрудников организации ПАО «Страховая компания «Спутник» должен

соответствовать требованиям, установленных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

В рамках разработки данного комплекса мер необходимым является составлением ряда требований, которым должен соответствовать каждый его сегмент.

1. Требования, относящиеся к организационным мерам, по защите ПДн.

- Для работы с персональными данными необходимым является получение согласия субъекта персональных данных на их обработку и хранение. Данное согласие необходимо подписать при трудоустройстве на рабочее место.

- Необходимо проводить инструктаж по работе с персональными данными. Ознакомление сотрудников с нормативами осуществляется в порядке ознакомления с «Политикой в отношении обработки персональных данных ...».

- Проводить проверки, связанные с обработкой персональных данных

- Так же необходимо установить порядок уничтожения информации, содержащей персональные данные сотрудника, при отзыве разрешения на обработку персональных данных, а также при увольнении сотрудника. Утверждение порядка уничтожения информации проводится в соответствии с порядком, установленным в «Политике в отношении обработки персональных данных ...» для ПДн, относящихся к клиентам организации.

2. Требования для маскирования персональных данных.

- При реализации процесса маскировки необходимо учитывать, что результат преобразования не должен быть обратимым в том смысле, что у лиц, не имеющих доступа к ключевой информации, не должно быть возможности восстановить оригинальный текст.

- Результаты маскирования должны относиться к тем же базовым типам данных, что и исходные данные.
- Маскированные данные должны иметь такую же структуру, что и исходные данные.
- Применимость алгоритма маскирования ко всему множеству данных
- Маскирование должно быть автоматизированным, легко повторяемым процессом.

3. Требования необходимые для использования технологии перечисление на основании доступа (ABE).

Для управления технологией необходимо наличие профессиональной или корпоративной версии Windows, а также наличие ОС Windows Server 2008 или выше.

4. Для применения метода подмены информации необходимо:

- объединение двух файлов, поэтому, при создании замаскированных данных, подмененные данные должны находиться в файле с таким же расширением, что и файл, содержащий настоящие ПДн субъектов.

- идентификации пользователя при взаимодействии с запрашиваемым файлом пароль от системы разграничения прав доступа не должен совпадать с паролем от необходимого файла. Пароль создается системе отдельно в соответствии со следующими правилами:

1. Пароль должен содержать в себе: латинские буквы, цифры и символы.
2. В системе не должно быть совпадающих паролей у пользователей
3. Замена пароля производится не реже 1 раза в месяц.

4.3 Структура комплекса мер, обеспечивающего защиту информации, методом ее подмены

Информационная система организации содержит большое количество записей о сотрудниках, находящихся незащищенных файлах системы. Доступ к этим данным имеет большое количество пользователей, поэтому для обеспечения безопасности ПДн субъектов необходимо разработать комплекс мер, мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

Данный комплекс мер необходимо внести в существующую «Политику в отношении обработки персональных данных ...».

В рамках созданного комплекса мер также выполняются требования законодательства РФ, касающиеся обработки, хранения и передачи персональных данных субъектов.

Для разработки комплекса мер по защите персональных данных необходимо:

1. Разработка перечня сведений данных, которые относятся к конфиденциальной, незащищенной информации;
2. Разработка модели угроз, а также модели нарушителя.
3. Разграничение доступа к конфиденциальной информации.
4. Осуществление технических и программных мер по защите конфиденциальной информации.

В первую очередь, для обеспечения защиты данных, необходимо составить перечень сведений, которые необходимо отнести к информации, имеющей конфиденциальный характер.

Перечень сведений, носящих конфиденциальный характер:

1. Фамилия, имя отчество сотрудника фирмы;
2. Дата рождения;
3. Адрес проживания;
4. Адрес регистрации;
5. Контактный номер телефона.

Следующим этапом необходимо определить угрозы безопасности данных, а также разработать модель нарушителя.

Основной угрозой для безопасности персональных данных сотрудника является угроза несанкционированного доступа неавторизованных пользователей, с целью кражи, модификации или удаления данных.

В качестве нарушителя вероятнее всего будет выступать физические лица, которые можно разделить на две категории:

- 1 категория – лица, не имеющие доступа к информационной системе;
- 2 категория – лица, получившие доступ к информационной системе.

Все потенциальные нарушители являются внешними, осуществляющими атаки вне границ организации.

В качестве внешнего нарушителя будем рассматривать:

1. Бывших сотрудников компании;
2. Посторонних лиц, пытающихся получить доступ к информационной сети;
3. Представители преступных организаций.

Внешний нарушитель может осуществлять такие действия как:

1. Получение доступа к информационной сети;
2. Попытка копирования, удаления или модификации персональных данных.

Следующим этапом в обеспечении защиты конфиденциальных сведений является разграничение доступа к информации. Данный этап в выбранной организации уже осуществлен. В рамках разграничения доступа к информации, в информационной сети были определены пользователи сети, а также действия, которые пользователи могут осуществлять в рамках выполнения служебных обязанностей.

Осуществление технических и программных мер по защите конфиденциальных сведений является важным этапом. В ПАО «Страховая компания «Спутник» на данный момент уже установлены необходимые средства защиты информации.

Однако существуют данные находящиеся в незащищенных файлах, для которых также необходимо обеспечить должную защиту. В качестве способа защиты выступает метод подмены данных.

При выборе способа защиты конфиденциальной информации учитывались такие моменты как:

1. Маскирование данных - это эффективный способ защиты конфиденциальной информации от несанкционированного доступа. Он позволяет обеспечить анонимность записей и сохранить половое соотношение клиентов в замаскированной таблице. Важно, что измененные данные при этом выглядят реалистично, а факт маскировки информации не является очевидным.

2. Метод подмены данных эффективен в ситуации, когда злоумышленник заранее получил доступ в информационную систему.

Использование данного метода предусматривает наличие замаскированных данных, а также парольной защиты на файл с конфиденциальными данными.

Так как в компании штатная численность сотрудников составляет 15 человек, то применение метода замены данных будет целесообразно и легким в реализации.

Мероприятия по защите персональных данных методом подмены включают в себя:

- проведение маскировки конфиденциальной информации;
- создание дополнительного файла с подмененными ПДн;
- применение технологии ABE для скрывания файлов недоступных для определенных пользователей;
- идентификация пользователя при работе с защищаемым файлом (создание пароля).

4.4 Разработка алгоритмов функционирования программы реализующей метод подмены информации

В рамках реализации комплекса мер по защите персональных данных сотрудников компании, находящихся в незащищенных файлах типа `xlsx` были разработаны алгоритмы функционирования программы, реализующей метод подмены информации. На рисунке 4.1 представлен алгоритм, отображающий последовательность действий при создании защиты данных, а на рисунке 4.2 отображен алгоритм работы метода подмены информации при попытке взаимодействия с защищаемым файлом.

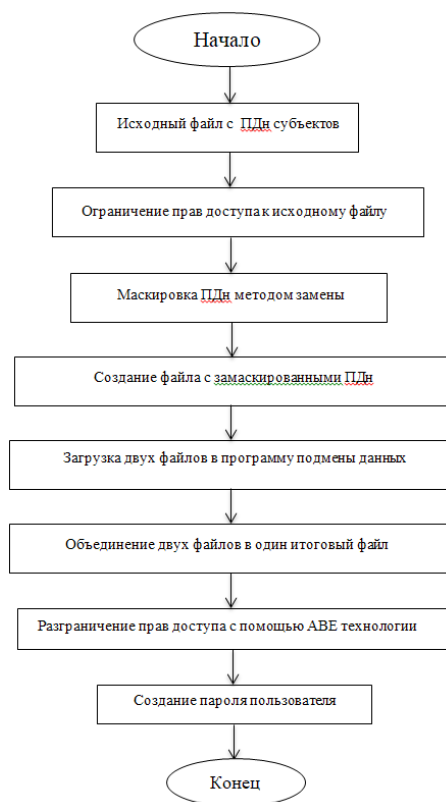


Рисунок 4.1 – Алгоритм последовательности действий при создании защиты данных

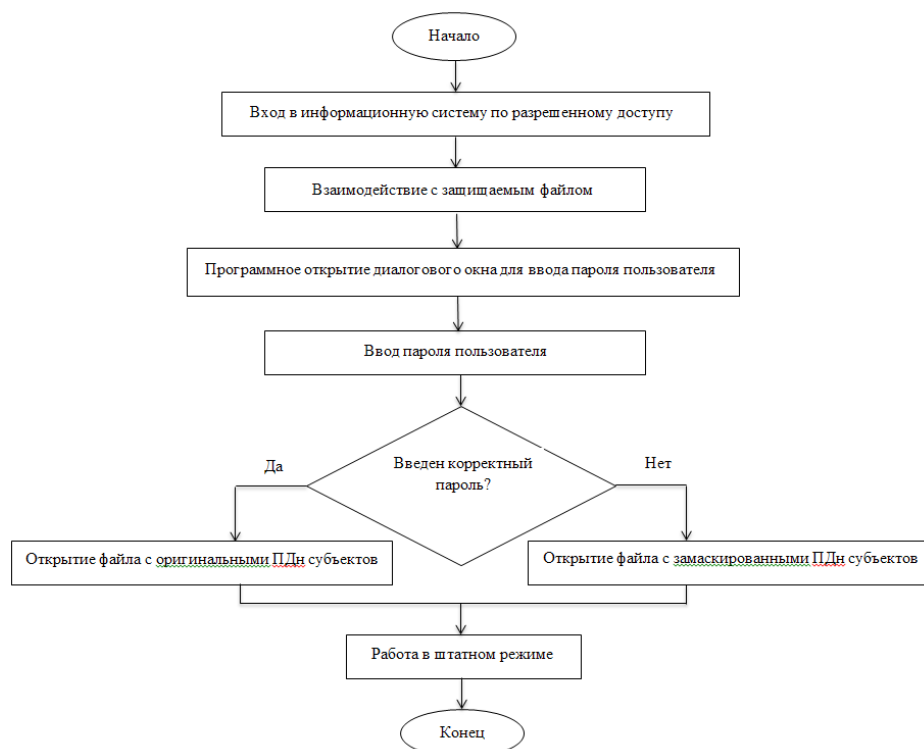


Рисунок 4.2 – Алгоритм работы метода подмены данных

Для подмены данных предварительно были проведены следующие действия:

1. Маскирование персональных данных.

Маскирование данных возможно с применением различных методов, в данном случае был выбран метод замены данных. При использовании маскирования важным критерием является сохранение концепции формата данных, для того, чтобы нарушитель не смог отличить замаскированные данные от подлинных данных.

В выбранной организации ПАО «Страховая компания «Спутник» штатное численность сотрудников равна 15 человек, это означает, что процедуру маскирования данных можно провести вручную. Это позволит компании не тратить денежные средства на установку программного средства.

Маскирование данных выполняется сетевым администратором, используя метод замены.

Этапы маскирования персональных данных:

- а) Для проведения маскировки данных необходимо открыть изначальные персональные данные, для того, чтобы оценить стилистку, формат, в котором находятся персональные данные.

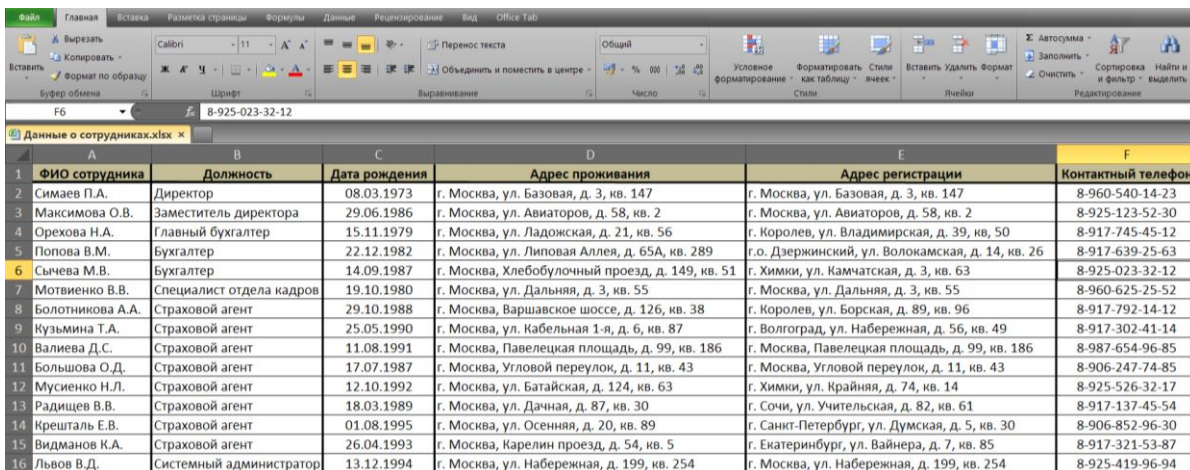
На рисунке 4.3 отображена структура персональных данных сотрудников, на ней видно, что данные находятся в файле формата `xlsx`, а также имеют следующую последовательность:

1. ФИО,
2. Должность
3. Дата рождения
4. Адрес проживания

5. Адрес регистрации
6. Контактный номер телефона

В таблице используется шрифт Calibri, 11. В столбцах 3 и 6 используется выравнивание посередине.

Данный формат необходимо сохранить при создании фиктивного файла.



	A	B	C	D	E	F
	ФИО сотрудника	Должность	Дата рождения	Адрес проживания	Адрес регистрации	Контактный телефон
1	Симаев П.А.	Директор	08.03.1973	г. Москва, ул. Базовая, д. 3, кв. 147	г. Москва, ул. Базовая, д. 3, кв. 147	8-960-540-14-23
2	Максимова О.В.	Заместитель директора	29.06.1986	г. Москва, ул. Авиаторов, д. 58, кв. 2	г. Москва, ул. Авиаторов, д. 58, кв. 2	8-925-123-52-30
3	Орехова Н.А.	Главный бухгалтер	15.11.1979	г. Москва, ул. Ладонская, д. 21, кв. 56	г. Королев, ул. Владимирская, д. 39, кв. 50	8-917-745-45-12
4	Попова В.М.	Бухгалтер	22.12.1982	г. Москва, ул. Липовая Аллея, д. 65А, кв. 289	г.о. Дзержинский, ул. Волокамская, д. 14, кв. 26	8-917-639-25-63
5	Сычева М.В.	Бухгалтер	14.09.1987	г. Москва, Хлебобулочный проезд, д. 149, кв. 51	г. Химки, ул. Камчатская, д. 3, кв. 63	8-925-023-32-12
6	Мотвиенко В.В.	Специалист отдела кадров	19.10.1980	г. Москва, ул. Дальняя, д. 3, кв. 55	г. Москва, ул. Дальняя, д. 3, кв. 55	8-960-625-25-52
7	Болотникова А.А.	Страховой агент	29.10.1988	г. Москва, Варшавское шоссе, д. 126, кв. 38	г. Королев, ул. Борская, д. 89, кв. 96	8-917-792-14-12
8	Кузьмина Т.А.	Страховой агент	25.05.1990	г. Москва, ул. Кабельная 1-я, д. 6, кв. 87	г. Волгоград, ул. Набережная, д. 56, кв. 49	8-917-302-41-14
9	Валиева Д.С.	Страховой агент	11.08.1991	г. Москва, Павелецкая площадь, д. 99, кв. 186	г. Москва, Павелецкая площадь, д. 99, кв. 186	8-987-654-96-85
10	Большова О.Д.	Страховой агент	17.07.1987	г. Москва, Угловой переулок, д. 11, кв. 43	г. Москва, Угловой переулок, д. 11, кв. 43	8-906-247-74-85
11	Мусиенко Н.Л.	Страховой агент	12.10.1992	г. Москва, ул. Батайская, д. 124, кв. 63	г. Химки, ул. Крайняя, д. 74, кв. 14	8-925-526-32-17
12	Радищев В.В.	Страховой агент	18.03.1989	г. Москва, ул. Дачная, д. 87, кв. 30	г. Сочи, ул. Учительская, д. 82, кв. 61	8-917-137-45-54
13	Крешталь Е.В.	Страховой агент	01.08.1995	г. Москва, ул. Осенняя, д. 20, кв. 89	г. Санкт-Петербург, ул. Думская, д. 5, кв. 30	8-906-852-96-30
14	Видманов К.А.	Страховой агент	26.04.1993	г. Москва, Карелин проезд, д. 54, кв. 5	г. Екатеринбург, ул. Вайнера, д. 7, кв. 85	8-917-321-53-87
15	Львов В.Д.	Системный администратор	13.12.1994	г. Москва, ул. Набережная, д. 199, кв. 254	г. Москва, ул. Набережная, д. 199, кв. 254	8-925-419-96-94

Рисунок 4.3 – структура персональных данных сотрудников

б) Создание файла формата xltx, в котором будут храниться замененные данные.

Маскировка будет проводиться для следующих № столбцов: № 1, № 3 - № 6. Столбец № 2 маскировать не обязательно.

Для маскировки столбца № 1 необходимо соблюдать гендерную принадлежность.

Для маскировки столбца № 3 важным является сохранение реальности, то есть дни могут меняться числовых значениях от 1- 30, месяцы от 1-12, а года, в данном случае, будут варьироваться в значениях от 1975 по 1995.

При маскировке столбца № 4 необходимым будет сохранить город проживания, так как ПАО «Страховая компания «Спутник» расположена

в городе Москва, значит, сотрудники данной компании проживают в том же городе.

Для маскировки столбца № 5 города, улицы, дома и номера квартир могут варьироваться. Однако при замене городов ключевым критерием является то, что города должны принадлежать Российской Федерации.

Замена столбца № 6 проводится с сохранением кода операторов, они должны быть реальными, к примеру, код оператора МТС Москвы является 917.

В итоге маскирования получим файл показанный на рисунке 4.4

	A	B	C	D	E	F
	ФИО сотрудника	Должность	Дата рождения	Адрес проживания	Адрес регистрации	Контактный телефон
1	Барabanов В.А.	Директор	18.11.1983	г. Москва, ул. Бажова, д. 52, кв. 21	г. Пенза, ул. Авиационная, д. 43, кв. 78	8-917-345-16-74
2	Моисеева К.А.	Заместитель директора	11.01.1979	г. Москва, ул. Казакова, д. 93, кв. 65	г. Нижний Новгород, ул. Матросова, д. 29, кв. 25	8-905-203-14-02
3	Котова М.Д.	Главный бухгалтер	04.06.1980	г. Москва, ул. Талалихина, д. 297А, кв. 81	г. Москва, ул. Талалихина, д. 297А, кв. 81	8-925-203-54-85
4	Расторгуева И.Л.	Бухгалтер	28.12.1984	г. Москва, ул. Лазо, д. 17, кв. 156	г. Тюмень, ул. Набережная, д. 189, кв. 141	8-960-371-41-75
5	Валуева О.А.	Бухгалтер	15.09.1990	г. Москва, ул. Ротерта, д. 43, кв. 112	г. Омск, ул. Дымная, д. 12, кв. 162	8-917-962-03-01
6	Вдовина Н.О.	Специалист отдела кадров	23.10.1982	г. Москва, ул. Чапаева, д. 2, кв. 36	г. Королев, ул. Рыбная, д. 9, кв. 50	8-925-762-43-91
7	Кириченко Я.Ф.	Страховой агент	08.04.1995	г. Москва, ул. Егорьевская, д. 13, кв. 187	г. Москва, ул. Яблоневая, д. 124, кв. 81	8-925-623-63-13
8	Дмитриева Е.В.	Страховой агент	19.05.1977	г. Москва, ул. Новобутовская, д. 30, кв. 91	г. Брянск, ул. Александровская, д. 17, кв. 11	8-906-814-75-25
9	Ревина Е.А.	Страховой агент	01.02.1980	г. Москва, ул. Гончарная, д. 384, кв. 108	г. Москва, ул. Байкальская, д. 94, кв. 32	8-902-987-63-85
10	Липова К.М.	Страховой агент	24.08.1988	г. Москва, Тихий тупик, д. 5, кв. 18	г. Москва, ул. Красносолнечная, д. 51, кв. 103	8-925-405-81-02
11	Некрасова Л.И.	Страховой агент	30.10.1992	г. Москва, ул. Машкова, д. 251, кв. 36	г. Москва, ул. Луганская, д. 114, кв. 71	8-917-539-98-89
12	Дымов А.Н.	Страховой агент	14.10.1985	г. Москва, ул. Осипенко, д. 141, кв. 90	г. Пермь, ул. Лисовая, д. 30, кв. 79	8-960-370-02-01
13	Савина Е.И.	Страховой агент	09.03.1995	г. Москва, ул. Домодедовская, д. 15, кв. 149	г. Санкт-Петербург, Остропольский переулок, д. 22, кв. 12	8-925-425-65-15
14	Шнайдер Д.В.	Страховой агент	29.07.1984	г. Москва, ул. Ивовая, д. 116, кв. 356	г. Москва, ул. Васильевская, д. 293, кв. 185	8-917-006-36-02
15	Ласкутов К.О.	Системный администратор	06.06.1996	г. Москва, ул. Ягодная, д. 57, кв. 3	г. Москва, ул. Икшинская, д. 41, кв. 218	8-917-731-13-68

Рисунок 4.4 – структура подмененных персональных данных сотрудников

2. На следующем этапе администратору необходимо выгрузить ссылки на оба файла в программу подмены данных.

После того, как в программу будут вставлены ссылки на два имеющихся файла, произойдет их соединение, и на выходе мы будем иметь файл, такого же формата, что файлы содержащие данные, то есть формат **xlsx**.

На рисунке 4.5 показано, что для объединения файлов необходимо выбрать соответствующие.

Далее на рисунке 4.6 отображается новый файл. Данный файл хранит в себе ссылки на файл под названием ПДн1.xlsx и ПДн2.xlsx.

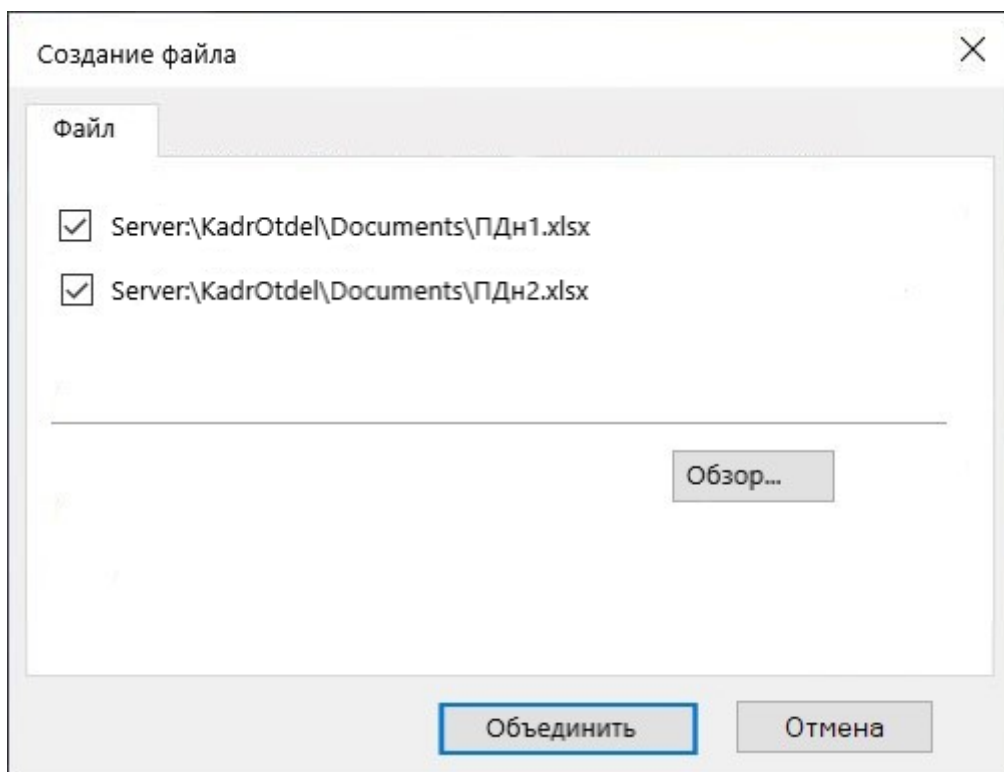


Рисунок 4.5 – Соединение двух файлов

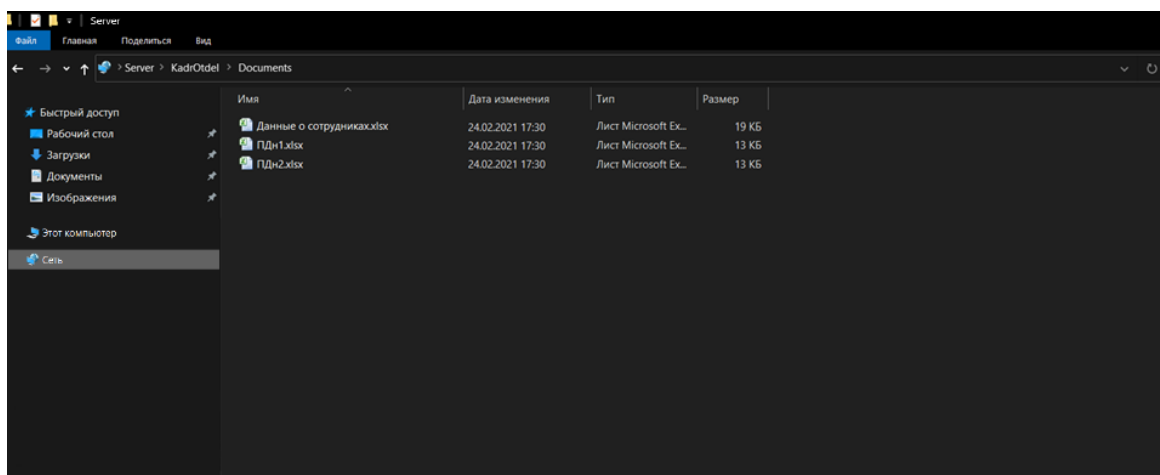


Рисунок 4.6 – Создание нового файла

3. На следующем этапе администратору с помощью технологии перечисление на основании доступа (ABE) необходимо скрыть изначальные файлы ПДн1.xlsx и ПДн2.xlsx. с помощью разграничения прав доступа. Данная технология позволяет скрывать файлы от пользователей, для которых

доступ к данным файлам будет ограничен, то есть пользователю запрещены следующие операции с файлом: чтение, запись, изменение, выполнение.

Функционал технологии ABE позволяет реализовать проверку прав доступа на объекты файловой системы до того, как пользователю отправляется список содержимого папки. Следовательно, в конечный список будут попадать только те объекты, к которым у пользователя есть хотя бы права Чтения, а все недоступные ресурсы просто не отображаются (скрываются).

Системному администратору необходимо провести настройку технологии ABE, так чтобы исходные файлы были видны только для него, а для всех остальных пользователей, файлы были скрыты. На рисунке 4.7 показаны те файлы, которые видны администратору после настройки технологии, а на рисунке 4.8 то, что отображается обычному пользователю.

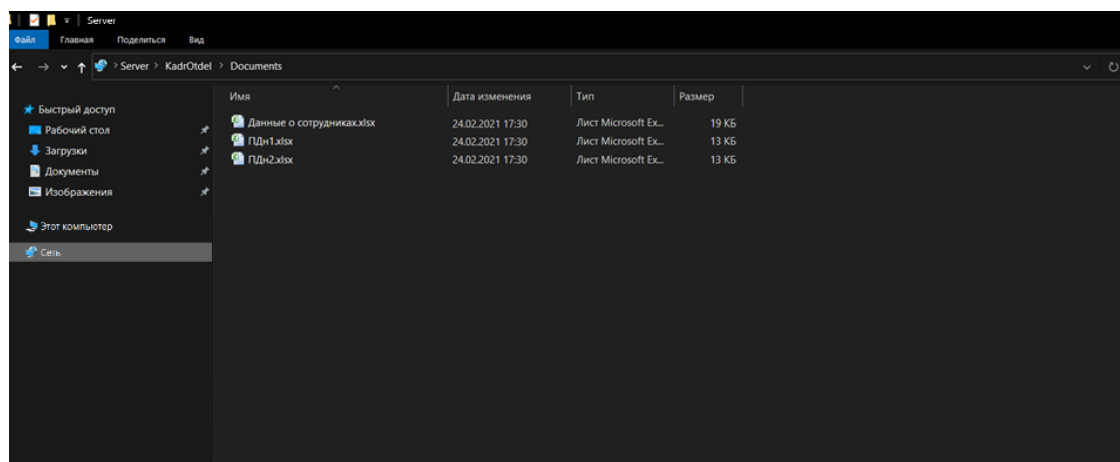


Рисунок 4.7 – Отображаемые файлы для администратора

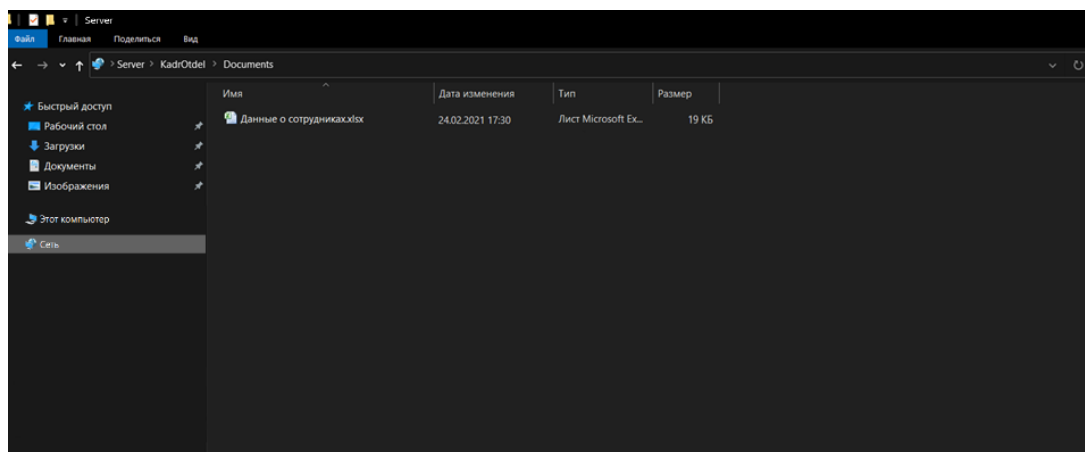


Рисунок 4.8 – Отображаемые файлы для пользователя

4. На данном этапе администратору необходимо в программе подмены данных, создать пароли для пользователей согласно требованиям.

В программе, во всплывающем диалоговом окне администратору необходимо выбрать каждую учетную запись, придумать для нее пароль и сохранить. С помощью создания данного пароля будет в дальнейшем происходить идентификация пользователя. На рисунке 4.9 показано всплывающее диалоговое окно для создания пароля.

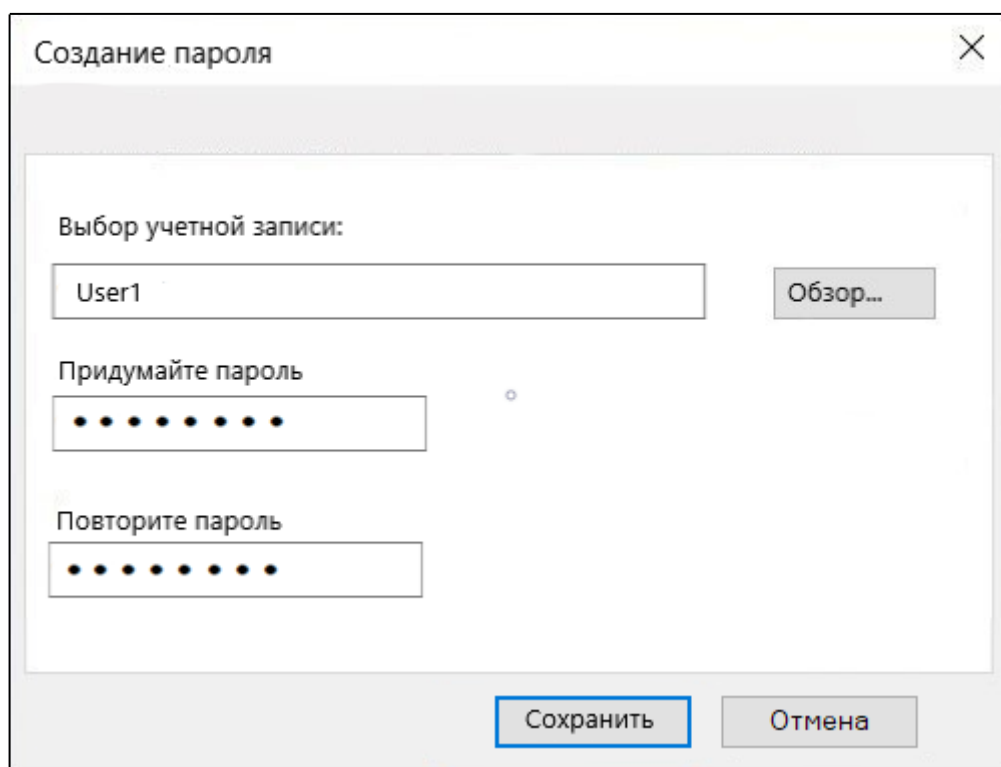


Рисунок 4.9 – Создание пароля для пользователей

Создание паролей для всех пользователей является крайним этапом для обеспечения защиты данных.

Далее будет продемонстрирована работа программы при попытке взаимодействия с файлом.

В первую очередь методы подмены данных является эффективным в том случае, когда доступ к информационной системе был взломан.

Таким образом, если злоумышленник попытается взаимодействовать с файлом, то пароль от файла ему неизвестен, и программа выдаст файл с подмененными ПДн.

Далее будет показано то, как работает данный метод.

На рисунках 4.10– 4.12 отображены взаимодействия с файлом обычного пользователя, которому необходим данный файл для выполнения служебных обязанностей.

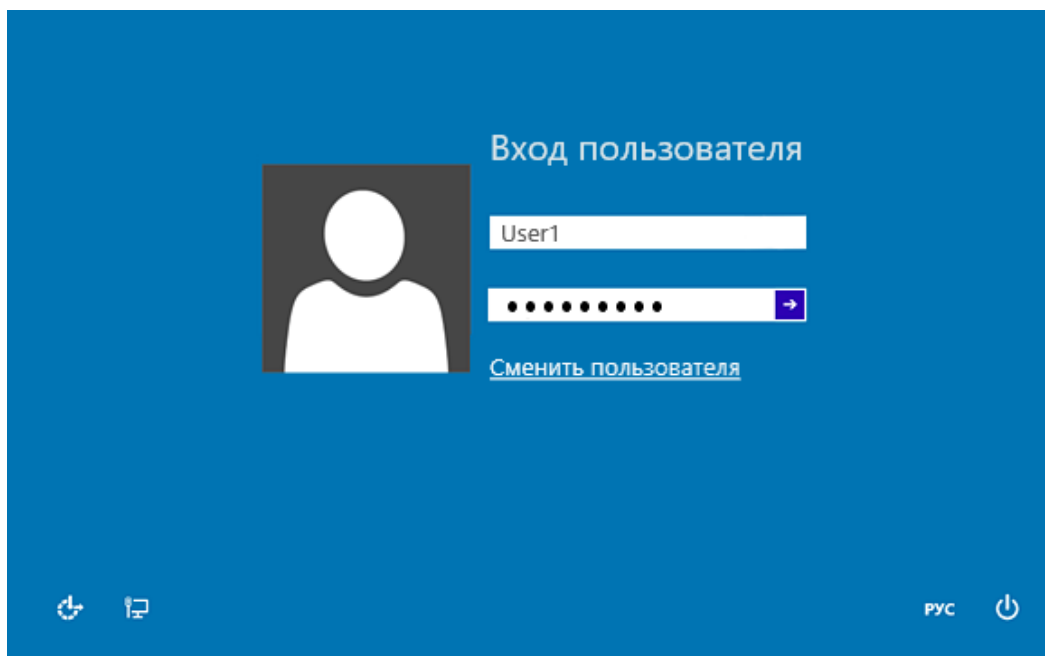


Рисунок 4.10 – Вход пользователя в систему

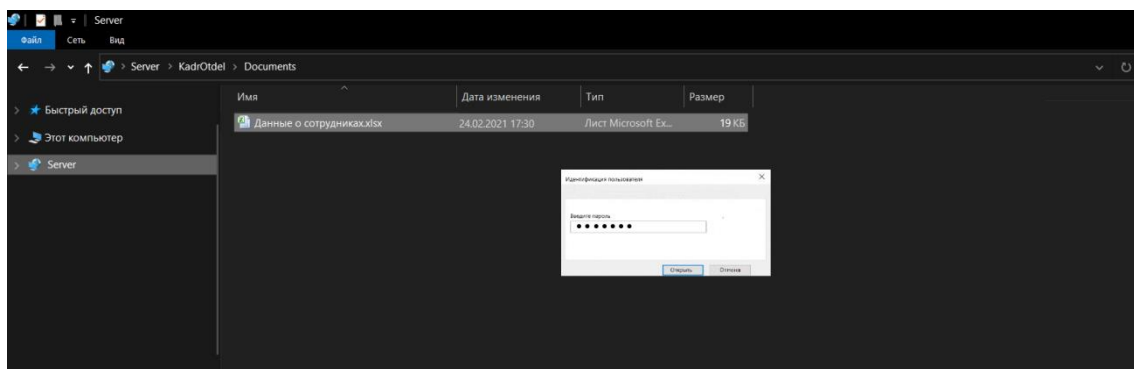


Рисунок 4.11 – Взаимодействие с файлом и ввод верного пароля от файла

А	В	С	Д	Е	Ф
ФИО сотрудника	Должность	Дата рождения	Адрес проживания	Адрес регистрации	Контактный телефон
1	Симаев П.А.	08.03.1973	г. Москва, ул. Базовая, д. 3, кв. 147	г. Москва, ул. Базовая, д. 3, кв. 147	8-960-540-14-23
2	Максимова О.В.	29.06.1986	г. Москва, ул. Авиаторов, д. 58, кв. 2	г. Москва, ул. Авиаторов, д. 58, кв. 2	8-925-123-52-30
3	Орехова Н.А.	15.11.1979	г. Москва, ул. Ладожская, д. 21, кв. 56	г. Королев, ул. Владимирская, д. 39, кв. 50	8-917-745-45-12
4	Попова В.М.	22.12.1982	г. Москва, ул. Липовая Аллея, д. 65А, кв. 289	г.о. Дзержинский, ул. Волокамская, д. 14, кв. 26	8-917-639-25-63
5	Сычева М.В.	14.09.1987	г. Москва, Хлебобулочный проезд, д. 149, кв. 51	г. Химки, ул. Камчатская, д. 3, кв. 63	8-925-023-32-12
6	Мотвиенко В.В.	19.10.1980	г. Москва, ул. Дальняя, д. 3, кв. 55	г. Москва, ул. Дальняя, д. 3, кв. 55	8-960-625-25-52
7	Болотникова А.А.	29.10.1988	г. Москва, Варшавское шоссе, д. 126, кв. 38	г. Королев, ул. Борская, д. 89, кв. 96	8-917-792-14-12
8	Кузьмина Т.А.	25.05.1990	г. Москва, ул. Кабельная 1-я, д. 6, кв. 87	г. Волгоград, ул. Набережная, д. 56, кв. 49	8-917-302-41-14
9	Валиева Д.С.	11.08.1991	г. Москва, Павелецкая площадь, д. 99, кв. 186	г. Москва, Павелецкая площадь, д. 99, кв. 186	8-987-654-96-85
10	Большова О.Д.	17.07.1987	г. Москва, Угловой переулок, д. 11, кв. 43	г. Москва, Угловой переулок, д. 11, кв. 43	8-906-247-74-85
11	Мусиенко Н.Л.	12.10.1992	г. Москва, ул. Батайская, д. 124, кв. 63	г. Химки, ул. Крайняя, д. 74, кв. 14	8-925-526-32-17
12	Радищев В.В.	18.03.1989	г. Москва, ул. Данная, д. 87, кв. 30	г. Сочи, ул. Учительская, д. 82, кв. 61	8-917-137-45-54
13	Крешталев Е.В.	01.08.1995	г. Москва, ул. Осенняя, д. 20, кв. 89	г. Санкт-Петербург, ул. Думская, д. 5, кв. 30	8-906-852-96-30
14	Видманов К.А.	26.04.1993	г. Москва, Карелин проезд, д. 54, кв. 5	г. Екатеринбург, ул. Вайнера, д. 7, кв. 85	8-917-321-53-87
15	Львов В.Д.	13.12.1994	г. Москва, ул. Набережная, д. 199, кв. 254	г. Москва, ул. Набережная, д. 199, кв. 254	8-925-419-96-94

Рисунок 4.12 – Открытие файла с оригинальными данными

Далее работа сотрудника проходит в штатном режиме. Оператор выполняет действия согласно разграничению прав доступа, для всех пользователей в информационной системе, кроме системного администратора и сотрудника кадрового отдела, разрешенным действием является – чтение.

На рисунках 4.13 – 4.15 продемонстрирована работа метода при действиях нарушителя.

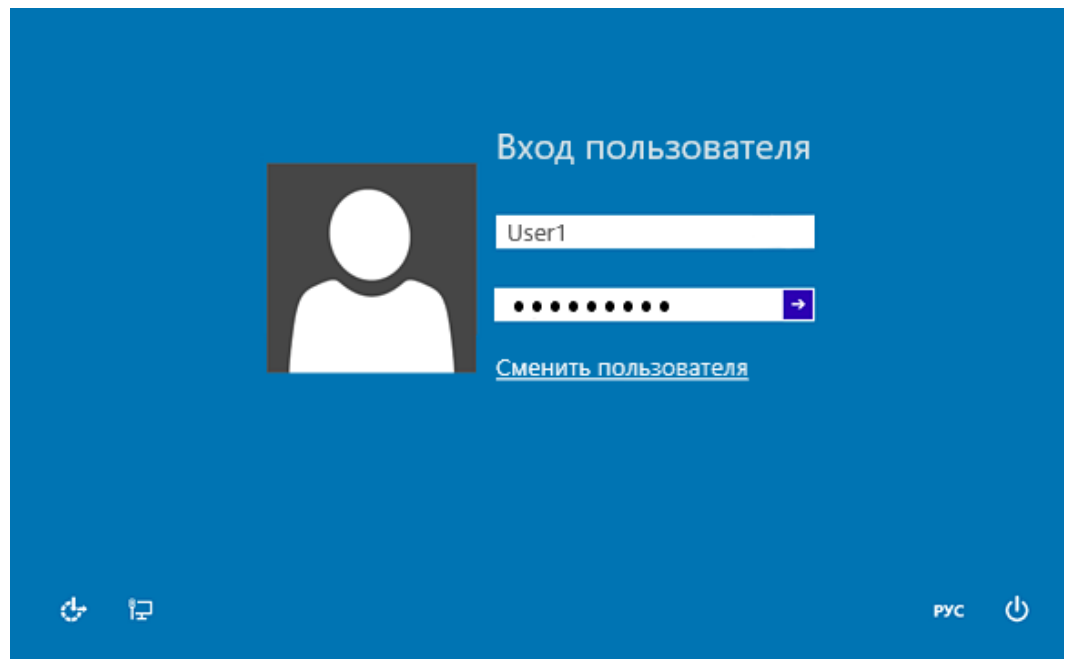


Рисунок 4.13 – Скомпрометированный вход в систему

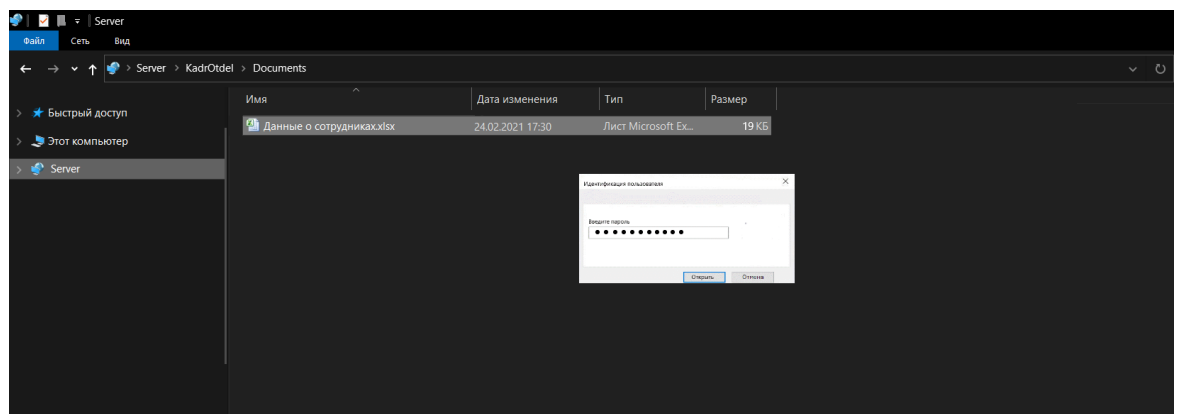


Рисунок 4.14 – Взаимодействие с файлом и ввод неверного пароля от файла

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид Office Tab						
<div> <div> <div>Вырезать</div> <div>Вставить</div> <div>Буфер обмена</div> </div> <div> <div>Копировать</div> <div>Формат по образцу</div> <div>Шрифт</div> </div> <div> <div>Стиль</div> <div>Выравнивание</div> <div>Число</div> </div> <div> <div>Общий</div> <div>Условное форматирование</div> <div>Стили</div> </div> </div>						
F11 8-925-405-81-02						
А	В	С	Д	Е	Ф	
1	ФИО сотрудника	Должность	Дата рождения	Адрес проживания	Адрес регистрации	Контактный телефон
2	Барабанов В.А.	Директор	18.11.1983	г. Москва, ул. Бажова, д. 52, кв. 21	г. Пенза, ул. Авиационная, д. 43, кв. 78	8-917-345-16-74
3	Моисеева К.А.	Заместитель директора	11.01.1979	г. Москва, ул. Казакова, д. 93, кв. 65	г. Нижний Новгород, ул. Матросова, д. 29, кв. 25	8-905-203-14-02
4	Котова М.Д.	Главный бухгалтер	04.06.1980	г. Москва, ул. Талалихина, д. 297А, кв. 81	г. Москва, ул. Талалихина, д. 297А, кв. 81	8-925-203-54-85
5	Расторгуева И.Л.	Бухгалтер	28.12.1984	г. Москва, ул. Лазо, д. 17, кв. 156	г. Тюмень, ул. Набережная, д. 189, кв. 141	8-960-371-41-75
6	Валуева О.А.	Бухгалтер	15.09.1990	г. Москва, ул. Ротерта, д. 43, кв. 112	г. Омск, ул. Дымная, д. 12, кв. 162	8-917-962-03-01
7	Вдовина Н.О.	Специалист отдела кадров	23.10.1982	г. Москва, ул. Чапаева, д. 2, кв. 36	г. Королёв, ул. Рыбная, д. 9, кв. 50	8-925-762-43-91
8	Кириченко Я.Ф.	Страховой агент	08.04.1995	г. Москва, ул. Егорьевская, д. 13, кв. 187	г. Москва, ул. Яблоневая, д. 124, кв. 81	8-925-623-63-13
9	Дмитриева Е.В.	Страховой агент	19.05.1977	г. Москва, ул. Новобутовская, д. 30, кв. 91	г. Брянск, ул. Александровская, д. 17, кв. 11	8-906-814-75-25
10	Резина Е.А.	Страховой агент	01.02.1980	г. Москва, ул. Гончарная, д. 384, кв. 108	г. Москва, ул. Байкальская, д. 94, кв. 32	8-902-987-63-85
11	Липова К.М.	Страховой агент	24.08.1988	г. Москва, Тихий тупик, д. 5, кв. 18	г. Москва, ул. Красносолнечная, д. 51, кв. 103	8-925-405-81-02
12	Некрасова Л.И.	Страховой агент	30.10.1992	г. Москва, ул. Машкова, д. 251, кв. 36	г. Москва, ул. Луганская, д. 114, кв. 71	8-917-539-98-89
13	Дымов А.Н.	Страховой агент	14.10.1985	г. Москва, ул. Осипенко, д. 141, кв. 90	г. Пермь, ул. Лисовая, д. 30, кв. 79	8-960-370-02-01
14	Савина Е.И.	Страховой агент	09.03.1995	г. Москва, ул. Домодедовская, д. 15, кв. 145	г. Санкт-Петербург, Остропольский переулок, д. 22, кв. 12	8-925-425-65-15
15	Шнайдер Д.В.	Страховой агент	29.07.1984	г. Москва, ул. Ивовая, д. 116, кв. 356	г. Москва, ул. Васильевская, д. 293, кв. 185	8-917-006-36-02
16	Ласкутов К.О.	Системный администратор	06.06.1996	г. Москва, ул. Ягодная, д. 57, кв. 3	г. Москва, ул. Икшинская, д. 41, кв. 218	8-917-731-13-68

Рисунок 4.15 – Открытие файла с подмененными файлами

В данном случае можно наблюдать, что нарушитель выполняет все те же действия, что и обычный пользователь, однако при взаимодействии с файлом был введен неверный пароль, в следствие чего, программа открывает файл с подмененными файлами.

Таким образом, мы можем видеть, что файлы защищены от несанкционированного доступа нарушителем.

ГЛАВА 5. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ

5.1 Маркетинговый анализ

В выпускной квалификационной работе проводится разработка комплекса мер, обеспечивающего безопасность персональных данных методом подмены. Данный метод позволяет защитить данные, которые находятся в незащищенных файлах.

Для использования такого комплекса мер необходимо для начала определить защищаемые сведения, а также файлы, в которых они располагаются. Далее необходимо составить алгоритмы работы, на основе которых выполняются необходимые действия. По алгоритму работы проводится маскировка данных, затем разграничиваются права доступа, а после, с помощью написанной программы, выполняется метод подмены.

Изучив методы защиты информации, существующие на рынке, можно сделать вывод, о том, что методов для защиты информации большое количество, однако, методов для защиты информации, находящейся в незащищаемых файлах существует ограниченное количество.

Таким образом, разработанный комплекс мер по защите данных методом подмены, является дополнением к существующим методам защиты информации, находящихся в незащищаемых файлах, не потребует больших затрат на его создание, и выполняет все необходимые для него функции. Это позволяет сделать вывод о его экономической эффективности.

Расчеты по разработке и внедрению данного комплекса мер будет проводить по организации ПАО «Страховая компания «Спутник». Данная компания оказывает услуги в сфере страхования. В информационной сети организации имеются конфиденциальные сведения, находящиеся в незащищаемых файлах формата `xlsx`. Внедрение комплекса мер по защите информации методом ее подмены позволит избежать несанкционированного доступа к ней, даже в том случае, если вход в систему был скомпрометирован.

5.2 Расчёт затрат на разработку комплекса мер

Сумма затрат на разработку нового продукта складывается из нескольких основных составляющих, в число которых входит проведение предварительных исследований, разработка технического и рабочего проектов структуры комплекса мер, разработки необходимых алгоритмов работы, а также проведения испытаний.

Для рационального проведения расчётов затрат на разработку нового продукта пред производственная стадия разбивается на следующие этапы:

- проведение маркетинговых исследований;
- разработка ТЗ;
- анализ методов, существующих на данный момент времени;
- разработка структуры комплекса мер и необходимых алгоритмов;
- макетирование, проверка на работоспособность;
- разработка ПО или ПМО;
- оснащение технологических процессов;
- приобретение сырья и материалов для осуществления работ;
- оформление сопутствующей документации;
- сдача продукта заказчику или начало работы производства;
- иные этапы при необходимости, обусловленной спецификой работы.

В состав затрат на разработку продукта входят:

- расходы на зарплату исполнителей;
- расходы по арендной плате за помещение;
- расходы на освещение и отопление;
- расходы на оплату машинного времени;
- косвенные расходы.

Расходы по зарплате исполнителям

$$З_{з/и} = З_{осн} * (1 + K_{доп})(1 + K_{с/ф}) \quad (1)$$

где:

$З_{осн}$ - основана зарплата работников, определяемая в зависимости от трудоемкости этапов разработки, квалификации и уровня оплаты.

$$З_{осн} = \sum_{j=1}^m \sum_{i=1}^n З_{ij} \text{час} t_{ij} \quad (2)$$

где:

m – кол-во этапов разработки;

n – кол-во разработчиков, принимающих участие в процессе разработки;

$З_{ij} \text{час}$ – часовая зарплата разработчика;

t_{ij} – затраты времени в часах i -го разработчика на j -ом этапе;

$m=3$

$n=1$

$З_{ij} \text{час} = 500 \text{ руб/час}$

$t_{ij} = 20 \text{ часов}$

Все виды работ выполняются 1 человеком в течение двух рабочих недель, в которые входят 3 этапа проектирования.

Коэффициенты, учитывающие дополнительную заработную плату и отчисления в социальные фонды:

$K_{доп} = 0.08$

$K_{с/ф} = 0.3$

После проведения подсчетов получаем следующие значения:

$$З_{\text{осн}} = 30\,000 \text{ рублей}$$

$$З_{\text{з/и}} = 42\,120 \text{ рублей}$$

Расходы по арендной плате за помещение

Проектирование, расчеты и подготовка документации осуществляются в офисном помещении площадью 15 м².

Расчет затрат на арендную плату вычисляется по следующей формуле:

$$З_{\text{ар}} = (Ц_{\text{ар}} S_{\text{пл}} T_{\text{раз}})/365 \quad (3)$$

где:

$Ц_{\text{ар}}$ - Арендная плата за 1 кв.м. площади в год;

$S_{\text{пл}}$ - арендуемая площадь в кв.м.;

$T_{\text{раз}}$ - время на разработку в календарных днях.

Помещение арендуется на две недели, его стоимость составит 2632 рублей.

Размер необходимой арендуемой площади

$$S_{\text{пл}} = \sum_{j=1}^m n_i q_{\text{чел}} + 5 \quad (4)$$

Так как в работе над проектом будут задействованы 1 человек, необходимая площадь составит 11 м²

Площадь арендованного помещения составляет 15 м², что соответствует необходимым требованиям.

Расходы на освещение и отопление

$$З_{\text{эн}} = P * t_{\text{дн}} * T_{\text{разр.раб.}} * W_{\text{э}} + S_{\text{пл}}(T_{\text{разр}}/365) \quad (5)$$

где:

P – суммарная мощность энергоприемников в помещении (5кВт)

$t_{\text{дн}}$ – продолжительность работы энергоприемников (8 часов)

Тарифы на электроэнергию и тепловую энергию:

$W_{\text{э}} = 4.6$ руб. за 1 кВт/ч

$W_{\text{тепл}} = 417$ руб. за 1 год

Таким образом рассчитаем $З_{\text{э}} = 1840 + 168,885 = 2008,885$ рублей

Расходы на оплату машинного времени

$$З_{\text{маш}} = \sum_{j=1}^{n_{\text{м}}} T_{j\text{э}} * Ц_{\text{маш}} \quad (6)$$

$n_{\text{м}}$ – количество этапов разработки с использованием вычислительной техники.

$T_{j\text{э}}$ – продолжительность этих этапов в часах

$Ц_{\text{маш}}$ – стоимость одного машино-часа работы (110 руб.)

Рассчитаем оплату машинного времени при продолжительности этапов в 40 часов $З_{\text{маш}} = 13\,200$ рублей

Косвенные расходы организации разработчика

$$З_{\text{косв}} = З_{\text{осн}} * K_{\text{косв}} \quad (7)$$

$K_{\text{косв}}$ в нашем случае принимается за 1

Рассчитаем $З_{\text{косв}} = 30\,000 \text{ руб.} * 1 = 30\,000 \text{ руб.}$

Итоговая себестоимость проектирования будет 89 960,885 рублей

Затраты на изготовление проектируемого изделия

Калькуляция себестоимости отображена в таблице 1.

Таблица 1 – Калькуляция себестоимости

	Наименование статей калькуляции	Затраты	
		Руб.	%
1	Тарифная зарплата производственных рабочих	55 000	58,4
2	Премия производственных рабочих	11 000	11,7
3	Итого зарплата производственных рабочих	66 000	
4	Дополнительная зарплата производственных рабочих	6 600	7
5	Отчисление в социальные фонды	18 876	20
6	Прочие производственные расходы	2 744	2.9
7	Итого производственная себестоимость	94 220	100

Общими затратами является сумма, затраченная на производство продукта и его себестоимость. На рисунке 5.1 представлено процентное соотношение себестоимости.



Рисунок 5.1 – Производственная себестоимость

После суммирования всех затраченных ресурсов, получаем результат равный $I = 184\,180,885$ руб.

5.3 Расчет экономической эффективности проекта

Целью этого раздела является определение показателей экономической эффективности затрат на приобретение новых видов информационно - измерительной техники, аппаратных средств защиты информации, средств автоматизации и регулирования производственных процессов, программных продуктов и других разработок. Эти затраты для пользователя носят характер инвестиций – долговременных вложений капитала с целью получения прибыли. Принятие решения инвестиционного характера, как и другой вид управленческой деятельности, основывается на использовании различных методов, позволяющих обоснованно принимать решения в области инвестиционной политики.

Поскольку инвестирование, это долговременный процесс, чаще всего для определения экономической эффективности инвестиций используются методы, основанные на дисконтированных оценках. Дисконтирование применяется для обеспечения сопоставимости затрат и будущих доходов.

Предварительно необходимо провести обоснование пороговой процентной ставки (r), на основе которой рассчитываются коэффициенты дисконтирования K :

$$K=1/(1+r)^t \quad (8)$$

В соответствии с классификацией инвестиционных проектов, устанавливаем пороговую ставку в 15 процентов.

$$r = 15\%$$

$$t=3$$

$$K_1=0,870;$$

$$K_2=0,756;$$

$$K_3=0,658.$$

Расчет чистой дисконтированной стоимости:

Необходимо сопоставить величины исходных инвестиций (И) с общей суммой дисконтированных чистых денежных поступлений (ЧДП), в течение прогнозируемого срока функционирования проекта.

Формула чистой дисконтированной стоимости:

$$\text{ЧДС} = \sum_{i=1}^t (\text{ЧДП}_i / (1 + r)^t) - \text{И} \quad (9)$$

где:

$$\text{ЧДП} = \Delta \text{П}_i - \Delta \text{Э} \quad (10)$$

$$\Delta \text{Э}_i = (\text{Эс} - \Delta \text{Эн}) \quad (11)$$

Эс – эксплуатационные издержки, до внедрения новой программы

Значение Эс = 250 227,13 руб./год. Т.е. это сумма издержек, которые уходили на защиту данных, работу с более дорогостоящей техникой и понесенные убытки.

Эн – эксплуатационные издержки, после внедрения новой программы

$$\text{Эн} = \text{З} + \text{Рт} + \text{М} + \text{А} \quad (12)$$

З – фонд заработной платы обслуживающего персонала

$$\text{З} = 35\,000 \text{ руб.}$$

Рт – затраты на текущий ремонт и межремонтное обслуживание

$$\text{Рт} = \text{Сэл} + \text{Зр} \quad (13)$$

Сэл – стоимость заменяемых в процессе ремонта элементов

$S_{эл} = 10\,000$ руб.

$Зр$ – зарплата ремонтных рабочих

$Зр = 5\,000$ руб.

Рассчитаем: $P_T = 10\,000 + 5000 = 15\,000$ руб.

M – материальные затраты на обслуживание техники

$M = 7600$ руб.

A – амортизационные отчисления

$$A = П * На / 100 \quad (14)$$

При норме амортизационных отчислений 15% и первоначальной стоимости техники и работы составит:

$A = 184\,180,885 * 15 / 100 = 27\,627,13$ руб.

Значение $Э_n = 100\,227,13$ руб./год

Рассчитаем по имеющимся данным величину $\Delta Э_i = 150\,000$ руб.

Тогда соответственно $ЧДП = 150\,000$ руб.

Пороговая ставка r составляет 15%

Рассчитаем $ЧДС$:

$ЧДС = (150\,000 * 0,870 + 150\,000 * 0,756 + 150\,000 * 0,658) - 184\,180,885$
 $= 158\,419,115$ руб.

$ЧДС > 0$, следовательно затраты оправданы.

Расчет внутренней нормы доходности

Находим необходимую процентную ставку, при которой значение ЧДС = 0

Определим ВНД по следующей формуле:

$$\text{ВНД} = \text{ЧДС}_+ * (r_2 - r_1) / (\text{ЧДС}_+ + |\text{ЧДС}_-|) \quad (15)$$

$$r_1 = 20\% = 0.20$$

$$r_2 = 25\% = 0.25$$

При $R_1 = 17\%$ чистая дисконтированная стоимость равна:

$$\text{ЧДС} = (150000 * 0,833 + 150000 * 0,694 + 150000 * 0,579) - 184\,180,885 = 13\,151,1737 \text{ руб.}$$

При $R_2 = 25\%$ чистая дисконтированная стоимость равна:

$$\text{ЧДС} - = (150000 * 0,800 + 150000 * 0,640 + 150000 * 0,512) - 184\,180,885 = -18\,907,285 \text{ руб.}$$

$$\text{ВНД составит} = 0.20 + (13\,151,1737 * (0.25 - 0.20) / (13\,151,1737 + 18\,907,285) = 22.05 \%$$

Полученное ВНД $> r$ (15%) – затраты оправданы.

На рисунке 5.2 представлены графические доказательства расчетов.

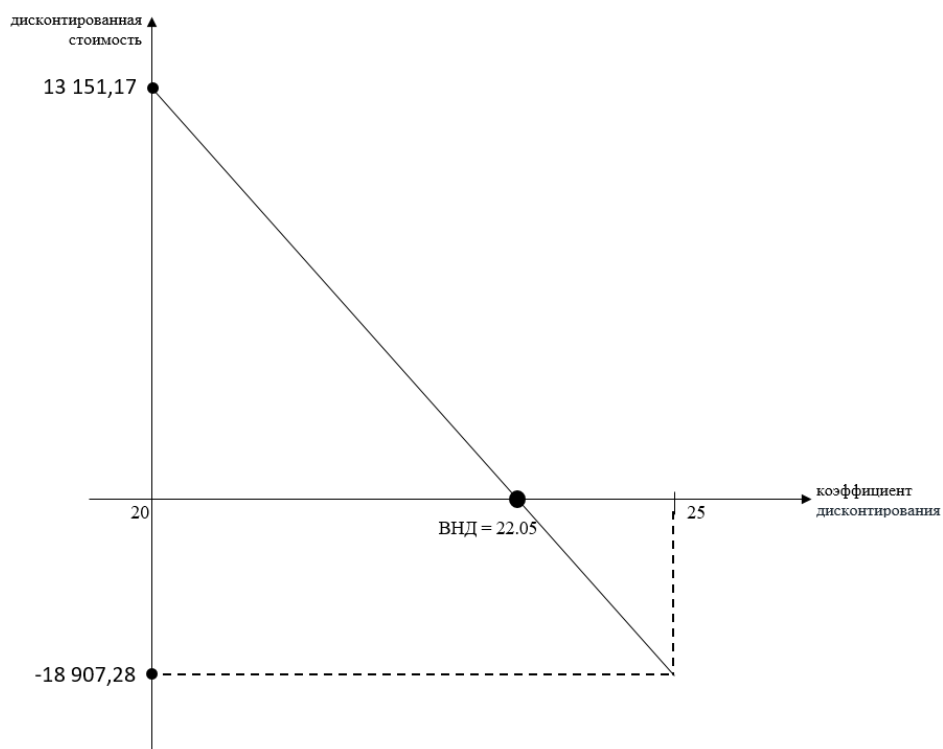


Рисунок 5.2 – Внутренняя норма доходности

Расчет срока полного возмещения инвестиций:

Позволяет определить тот срок, в течение которого инвестиции окупаются

$$\text{СВПИ} = n (+)(И - \sum_{i=1}^n \text{ЧДС}_i) / \text{ЧДС}_{n+1} \quad (16)$$

$$\text{СВПИ} = 2 (+) \frac{(184\,180,885 - 243\,900)}{98\,700} = 1.4 \quad (17)$$

СВПИ при И = 184 180,885 руб. составит 1.4 года

На рисунке 5.3 продемонстрирован срок полного возмещения инвестиций, который составляет около полутора лет.

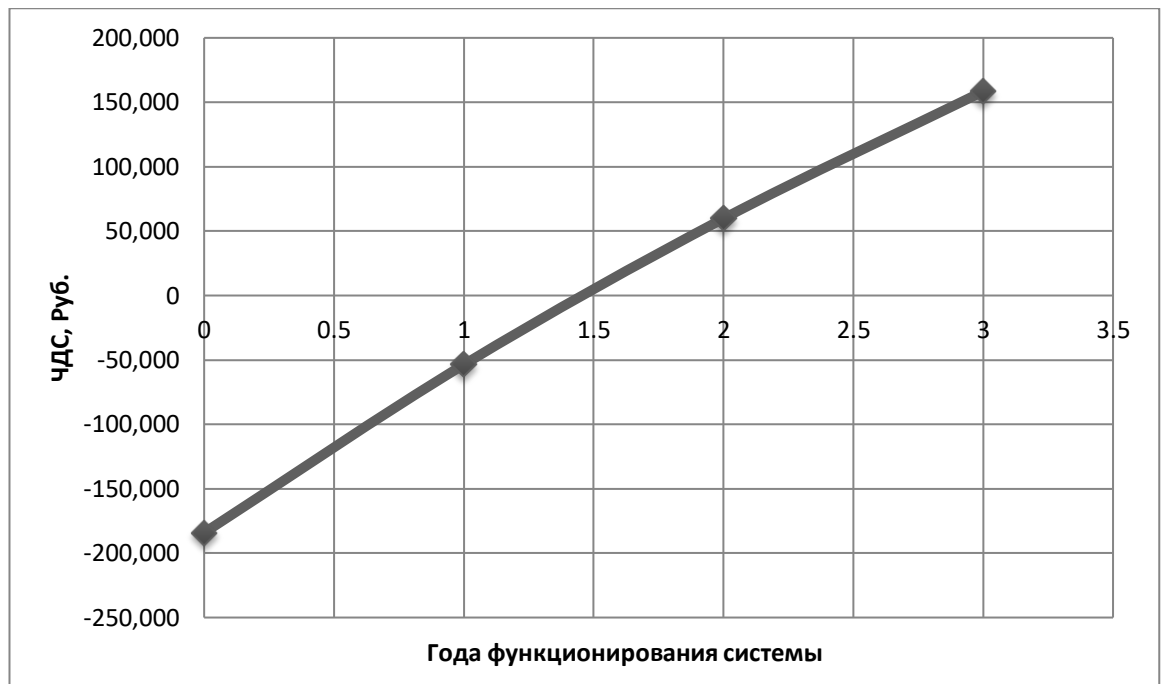


Рисунок 5.3 – Срок полного возмещения инвестиций

5.4 Заключение

В результате проделанной работы, можно сказать, что при ставке 15 % ЧДС составит 54 053,279 рублей, что говорит об экономической эффективности проекта, также срок полного возмещения инвестиционных вложений составляет 1,5 года, ВНД = 22,05 %, что больше 15 %, это свидетельствует об устойчивости проекта.

ГЛАВА 6. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ И ОХРАНА ТРУДА

В настоящем разделе рассмотрен вопрос, касающийся охраны труда работников ПАО «Страховая компания «Спутник», которые в свою очередь обрабатывают персональные данные, используя ПЭВМ.

При организации труда сотрудников компании, работающих на ПЭВМ, важным фактором является обеспечение безопасности организации рабочего места каждого сотрудника. Эффективность работы сотрудника напрямую зависит от условий нахождения за рабочим местом, так как при длительной и монотонной работе за ПЭВМ увеличивается утомляемость и снижается концентрация внимания, что мешает сотруднику компании выполнять свои служебные обязанности.

Для того чтобы избежать вредного воздействия при работе с вычислительной техникой необходимо соблюдать соответствующие меры безопасности, правильно планировать рабочее место и режим работы.

6.1 Проектирование производственной среды

Все помещения ПАО «Страховая компания «Спутник» - сухие помещения с регулярной сухой и влажной уборкой от грязи и пыли. Все помещения являются проветриваемыми и имеют достаточное количество окон.

В каждом из помещений выполняются следующие нормы:

- температура воздуха составляет 22°C;
- относительная влажность 55 %;
- уровень шума не превышает 50дБА;
- наличие искусственного и естественного освещения, не создающее бликов на поверхности экранов мониторов;

- коэффициент естественной освещенности составляет 1,5%.

Все помещения компании, в которых ведется работа с ПЭВМ, принадлежат к категории «В», так как в них имеются горючие и трудногорючие элементы.

В помещениях, согласно требованиям размещены углекислотные огнетушители ОУ – 5. Для помещений компании необходимо 3 огнетушителя, размещенные таким образом, чтобы их верх находился на высоте не более полутора метров от поверхности пола.

6.2 Проектирование рабочего места

Сотрудники компании исполняют служебные обязанности на ПЭВМ с ВДТ на базе плоского жидкокристаллического экрана. Рабочие места сотрудников составляют ...

При размещении рабочих мест учитывались расстояния между рабочими столами с видеомониторами в 2 метра и расстояния между боковыми поверхностями в 1,2 метра.

Для обеспечения комфорта и безопасности сотрудников компании, за исключением руководящего звена компании (директор, заместитель директора, главный бухгалтер) было выбрано офисное кресло фирмы PROFIT. Данный вариант удовлетворяет необходимым требованиям, таким как:

- кресло имеет подъемно-поворотный механизм;
- есть возможность регулировки кресла по высоте;
- спинка кресла регулируется как по высоте, так и по углу наклона;
- глубина сиденья составляет 49 см;
- ширина сиденья составляет 59 см;
- высота кресла составляет 120 (128) см;
- высота сиденья регулируется в пределах от 48 до 55 см;

- поверхность сиденья и спинки кресла полумягкое с нескользящим, слабо электризующимся и воздухопроницаемым покрытием.

Для руководящего звена было выбрано кресло офисное BRABIX PREMIUM. Данный вариант кресла обладает механизмом качания, который позволяет фиксировать сиденье в 5 разных положениях. Так же в кресле расположен механизм позволяющий мягко менять угол наклона спинки.

Характеристики:

- высота кресла минимальная 113 см, максимальная 119 см;
- ширина сиденья равна 57см;
- глубина сиденья равна 48 см;
- ширина спинки сиденья равна 57.5 см;
- высота спинки сиденья равна 65.5 см;
- поверхность сиденья и спинки кресла полумягкое с нескользящим, слабо электризующимся и воздухопроницаемым покрытием.

В качестве рабочего стола сотрудников компании был выбран стол ПРАТО. Данный стол удовлетворяет следующим критериям:

- высота рабочей поверхности 75 см;
- пространство для ног:
 - a) высота – 70 см;
 - b) ширина – 65 см;
 - c) глубина на уровне колен – 55 см;
 - d) глубина на уровне вытянутых ног – 70 см;

Рабочее место сотрудников оборудовано подставкой для ног FELLOWES, которая имеет ширину 30 см, глубину равную 45 см и угол наклона опорной поверхности 15°. Подставка имеет рифленую поверхность и оборудована бортиком по переднему краю высотой 1 см.

Для оборудования рабочего места руководящего звена был выбран стол Born, соответствующий необходимым требованиям, а именно: высота

рабочей поверхности составляет 80 см, пространство для ног обладает следующими параметрами:

- а) высота 75 см;
- б) ширина 70 см;
- с) глубина на уровне колен 60 см;
- д) глубина на уровне вытянутых ног 75 см;

Рабочее место также оборудовано подставкой для ног FELLOWES, которая имеет ширину 30 см, глубину равную 45 см и угол наклона опорной поверхности 15°. Подставка имеет рифленую поверхность и оборудована бортиком по переднему краю высотой 1 см.

Ниже на рисунке 6.1 представлена схема рабочего места сотрудников компании.

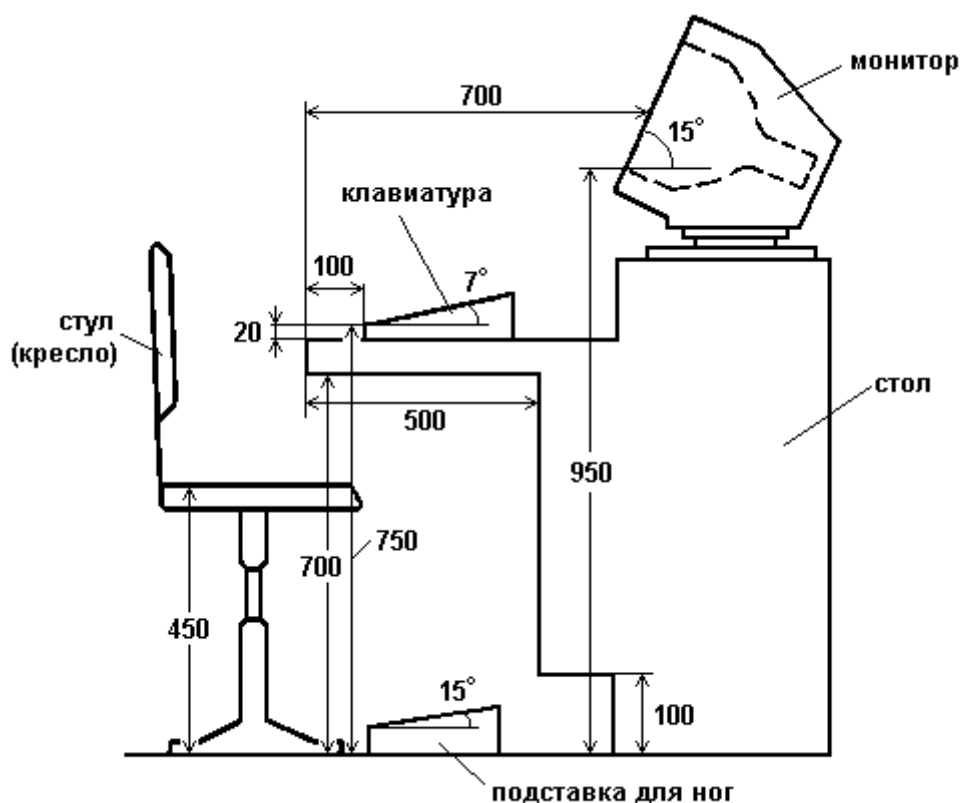


Рисунок 6.1 – Организация рабочего места оператора ПЭВМ

6.3 Выбор оборудования

В выбранной организации сотрудники компании постоянно работают за ПЭВМ, они обрабатывают большой поток информации на протяжении всего рабочего дня. Поэтому для работы необходимо выбрать ПЭВМ с соответствующими характеристиками.

В связи с заданными условиями, в качестве системного блока был выбран IRU Office 120, обладающий следующими характеристиками:

- двухъядерный процессор AMD E1 6010;
- оперативная память DIMM, DDR3 4096 Мб 1600 МГц на 32 Гб;
- SSD для хранения информации на 60Гб;
- графический интегрированный редактор AMD Radeon R2;
- операционная система Windows 10 Professional;
- внутренний блок питания 350 Вт;
- вес корпуса 7 кг.

В ПЭВМ используется жидкокристаллический монитор DELL SE2216H. Монитор имеет эргономичную конструкцию: 21,5-дюймовый экран, регулируемая подставка с возможностью менять угол наклона экрана. Данный тип монитора обладает следующими характеристиками:

- разрешение экрана 1920x1080;
- соотношение сторон экрана 16:9;
- угол наклона экрана $-5^{\circ}/+21^{\circ}$;
- яркость экрана 250 кд/м2;
- угол обзора 178° по горизонтали, 178° по вертикали;
- частота обновления 60 Гц.

Для исполнения служебных обязанностей необходимо использование многофункционального устройства. В качестве МФУ был выбран CANON Maxify MB2140. Данный тип МФУ практически бесшумен, а также быстро и качественно выполняет свои функции.

При работе с ПЭВМ важным фактором является использование источников бесперебойного питания, так как его применение позволит защитить серверное оборудование, периферийную компьютерную и вычислительную технику, которая питается от сети, от резких перепадов напряжения или внезапных отключений электроэнергии, а также предотвратить потерю важных данных. Для выполнения этой цели был выбран ИБП IPPON Back Basic 2200 Euro.

6.4 Проектирование схемы подключения оборудования.

В связи с использованием ПЭВМ, помещения, где размещаются рабочие места сотрудников, по техническим требованиям оборудованы защитным заземлением. Для питания ПЭВМ применена система с глухозаземленной нейтралью трансформатора. Для защиты от статического электричества применено дополнительное заземление корпуса ПЭВМ, проводимое к каждому рабочему месту.

Для проектирования рабочего места были использованы следующие планировки:

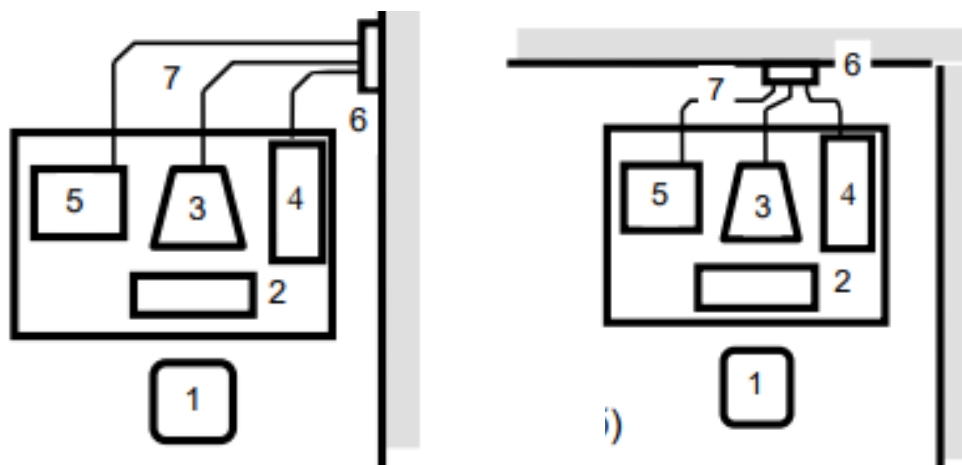


Рисунок 6.2 – Схемы компоновки рабочих мест

Цифрами на рисунке обозначены:

1. Рабочее место сотрудника
2. Клавиатура
3. Дисплей

4. Системный блок ПЭВМ
5. МФУ
6. Розетки питания
7. Сетевые кабели питания ПЭВМ

Разработка рабочего места сотрудников предполагает его размещение в удалении от зоны расположения розеток. При организации рабочего пространства также обеспечивается невозможность прямого доступа к токоведущим частям, что защищает оператора от случайного прикосновения.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы была поставлена цель разработки комплекса мер, обеспечивающего безопасность персональных данных, методом подмены информации.

Для ее реализации были изучены теоретические аспекты по защите персональных данных, организационная структура предприятия, на основе которого осуществляется защита информации, определена целевая угроза для не защищенных сведений, далее составлена структура разрабатываемого комплекса мер и разработаны алгоритмы функционирования используемого метода подмены информации.

В ходе выполнения данной работы также была произведена оценка экономической эффективности проекта, которая показала, что срок возмещения инвестиционных вложений составляет 1,5 года, ЧДС составит 54 053,279 рублей, что говорит об экономической эффективности разработки.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»
2. Совместный приказ ФСТЭК России, ФСБ России и Минкомсвязи России от 31 декабря 2013, N 151/786/461.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
4. ГОСТ Р ИСО/МЭК 1335-1-2006. Информационная технология. Методы и средства обеспечения безопасности.
5. ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации.
6. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.
7. ГОСТ 7.32-2017 СИБИД Отчет о научно-исследовательской работе. Структура и правила оформления.
8. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий – М.: МИФИ, 1995, - 96 с.
9. Галатенко В.А. Основы информационной безопасности: Курс лекций. Учебное пособие — Москва, 2006. - 199 с.
10. Давыдов И.Г. Защита информации в социотехнических системах: Тематические материалы к курсу лекций — Минск, 2007. - 101 с.
11. Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для вузов — М.: Академия, 2008. — 336 с.
12. Поцелуева Л.П. Методические указания по экономическому обоснованию дипломных проектов [Текст]: методические указания / Л.П. Поцелуева. – СамГТУ, 2007. – 23 с.
13. Проектирование рабочего места оператора ПЭВМ [Текст]: методические указания. – СамГТУ, 2016. – 14 с.

14. Вихорев С.В. Классификация угроз информационной безопасности. – [Электр. ресурс]. Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.

15. Казыханов А.А. – Методы маскировки критически важной информации – «Научно-практический электронный журнал Аллея Науки» № 5(21). – 2018. Режим доступа: https://alley-science.ru/domains_data/files/4663May2018.

16. Окатов А.В., Костюнина Т.Н. – Информационная безопасность. – Электронное учебное пособие. Режим доступа: http://eos.ibi.spb.ru/umk/11_11/5/5_R0_T1.html

17. Data Masking: What You Need to Know A Net 2000 Ltd. White Paper. – 2016. Режим доступа: <http://www.datamasker.com>