

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА

Рецензент, начальник технического
отдела АО «Гранит Информ»

_____ А.С. Жаворонкин
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2019 г.

**Подготовка Муниципального учреждения
«Расчетно-технический центр по отрасли «Образование»
города Магнитогорска к аттестации**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ - 10.05.03.2019.378.ПЗ ВКР**

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент

_____ Н.В. Глотова
_____ 2019 г.

Руководитель проекта,
к.п.н., доцент

_____ О.Р. Уторов
_____ 2019 г.

Автор проекта,
студент группы КЭ-570

_____ Г.В. Гайворонский
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2019 г.

АННОТАЦИЯ

Гайворонский Г.В. Подготовка Муниципального учреждения «Расчетно-технический центр по отрасли «Образование» города Магнитогорска к аттестации - Челябинск: ЮУрГУ, КЭ-570, 149 с., 1 ил., 10 табл., библиогр. список - 29 наим., 21 прил.

Выпускная квалификационная работа выполнена с целью подготовки МУ РТЦ «Образование» г. Магнитогорска к аттестации, которая заключается в создании системы защиты персональных данных.

В выпускной квалификационной работе отражены все этапы создания системы защиты персональных данных, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных.

Работа состоит из 4 глав. В первой главе описывается процесс анализа исходной защищенности информационной системы учреждения. В частности, проведение предпроектного обследования и подготовка документов, необходимых для начала работ. Во второй главе затрагиваются теоретические аспекты защиты персональных данных. Третья глава описывает основную часть работ по созданию системы защиты персональных данных. В частности, организационные, инженерно-технические и программно-аппаратные меры по защите информации. Четвертая глава посвящена безопасности жизнедеятельности.

					ЮУрГУ – 10.05.03.2019.378.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.	Гайворонский				<i>Подготовка Муниципального учреждения «Расчетно-технический центр по отрасли «Образование» города Магнитогорска к аттестации</i>	Лит.	Лист	Листов
Пров.	Уторов						6	149
Реценз.	Жаворонкин					ЮУрГУ		
Н. Контр.	Мартынов					Кафедра ЗИ		
Утв.	Соколов							

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	10
ВВЕДЕНИЕ	11
ГЛАВА 1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИСПДН	12
1.1 Предпосылки к аттестации	12
1.2 Описание объекта информатизации	13
1.3 Обследование информационной системы персональных данных	14
1.3.1 Определение границы контролируемой зоны	15
1.3.2 Выявление защищаемой информации	16
1.3.3 Описание технологического процесса	16
1.3.4 Разработка технического паспорта	16
1.3.5 Определение уровня защищенности ИСПДн	17
1.4 Разработка модели нарушителя	17
1.4.1 Классификация нарушителей	18
1.4.2 Внешний нарушитель	19
1.4.3 Внутренний нарушитель	20
1.4.4 Потенциал нарушителей	21
1.4.5 Возможные способы реализации угроз безопасности информации	23
1.5 Разработка модели угроз	25
1.5.1 Определение исходного уровня защищенности ИСПДн	26
1.5.2 Вероятность реализации УБПДн	27
1.5.3 Возможность реализуемости угроз	28
1.5.4 Оценка опасности угроз	28
1.5.5 Определение актуальности угроз в ИСПДн	28
1.5.6 Угрозы безопасности информации	29
1.6 Разработка технического задания	44
1.7 Выводы	44
ГЛАВА 2. ТЕОРИТИЧЕСКИЕ ОСНОВЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	46
2.1 Основные понятия в области защиты персональных данных	46
2.2 Законодательство Российской Федерации в области защиты персональных данных	47
2.2.1 Обязанности операторов персональных данных	50
2.2.2 Ответственность за несоблюдение законодательства в области защиты персональных данных	51

2.3 Порядок проведения работ по обработке персональных данных	52
2.4 Сравнение средств защиты информации.....	55
2.4.1 СЗИ от НСД	55
2.4.2 Средства антивирусной защиты	57
2.5 Выводы	58
ГЛАВА 3. ВНЕДРЕНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	60
3.1 Организационные меры по обеспечению безопасности персональных данных	60
3.2 Инженерно-технические меры по обеспечению безопасности персональных данных	63
3.3 Программно-аппаратные меры по обеспечению безопасности персональных данных	63
3.4 Выводы	70
ГЛАВА 4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	71
4.1 Общие положения	71
4.2 Требования к помещениям для работы с ПЭВМ	72
4.3 Требования к микроклимату, уровню шума и освещению.....	73
4.4 Обеспечение пожарной и электробезопасности	75
4.5 Сравнение требуемых параметров к рабочему месту	77
4.6 Выводы	79
ЗАКЛЮЧЕНИЕ	81
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	82
ПРИЛОЖЕНИЕ А	85
ПРИЛОЖЕНИЕ Б.....	90
ПРИЛОЖЕНИЕ В	91
ПРИЛОЖЕНИЕ Г.....	95
ПРИЛОЖЕНИЕ Д	96
ПРИЛОЖЕНИЕ Е.....	102
ПРИЛОЖЕНИЕ Ж.....	104
ПРИЛОЖЕНИЕ И	107
ПРИЛОЖЕНИЕ К	108
ПРИЛОЖЕНИЕ Л	109
ПРИЛОЖЕНИЕ М.....	110
ПРИЛОЖЕНИЕ Н	112
ПРИЛОЖЕНИЕ П	115

ПРИЛОЖЕНИЕ Р	123
ПРИЛОЖЕНИЕ С	127
ПРИЛОЖЕНИЕ Т	133
ПРИЛОЖЕНИЕ У	136
ПРИЛОЖЕНИЕ Ф	140
ПРИЛОЖЕНИЕ Х	143
ПРИЛОЖЕНИЕ Ц	146
ПРИЛОЖЕНИЕ Ш	149

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ - автоматизированное рабочее место;
АС - автоматизированная система;
БЖД - безопасность жизнедеятельности;
ВКР - выпускная квалификационная работа;
ВТСС - вспомогательные технические средства и системы;
ЗИ - защита информации;
ИБ - информационная безопасность;
ИБП - источник бесперебойного питания;
ИС - информационная система;
ИСПДн - информационная система персональных данных;
КЗ - контролируемая зона;
МЭ - межсетевой экран;
НСД - несанкционированный доступ;
ОТСС - основные технические средства и системы;
ПДн - персональные данные;
ПЭВМ - персональная электронно-вычислительная машина;
ПЭМИН - побочные электромагнитные излучения и наводки;
ПО - программное обеспечение;
РД - руководящий документ;
РФ - Российская Федерация;
САВЗ - средство антивирусной защиты;
СЗИ - средства защиты информации;
СЗПДн - система защиты персональных данных;
ТС - технические средства;
ФЗ - Федеральный закон;
ФСБ - Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ЛВС - локальная вычислительная сеть;
НДВ - недекларируемые возможности;
СВТ - средства вычислительной техники;
СКЗИ - средство криптографической защиты информации;
ТЗ - техническое задание.

ВВЕДЕНИЕ

Согласно Конституции РФ [29], каждый человек имеет право на неприкосновенность частной жизни, личную и семейную тайну (п.1 ст.23), а также сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (п.1 ст.24). Следовательно, защита персональных данных - деятельность, которой нужно уделять особое внимание.

Актуальность работы обусловлена наличием требований к обработке персональных данных на законодательном уровне. Более того, существует административная, и даже уголовная ответственность за неправильное ее осуществление. Так как незнание закона не освобождает человек от ответственности, необходимо ответственно подойти к вопросу защиты персональных данных.

Объектом выпускной квалификационной работы является Муниципальное учреждение «Расчетно-технический центр по отрасли «Образование» города Магнитогорска.

Предметом выпускной квалификационной работы является информационная система персональных данных «Бухгалтерия» МУ «РТЦ «Образование» г. Магнитогорска, аттестацию, которой проводило АО «Гранит Информ».

Целью данной дипломной работы является подготовка МУ «РТЦ «Образование» г. Магнитогорска к аттестации, путем создания системы защиты персональных данных на базе учреждения. Для реализации поставленной цели будем руководствоваться порядком проведения аттестации, утвержденным Положением по аттестации объектов информатизации по требованиям безопасности информации[7]:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с объектом информатизации;
- проведение экспертного обследования объекта информатизации и разработка документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний информатизации и утверждение заключения по результатам аттестации.

В результате работы должна получиться функционирующая система защиты персональных данных, которая удовлетворяет всем требованиям законодательства в области защиты персональных данных.