

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

Начальник технического отдела –
главный инженер

АО «Гранит-Информ»

_____ А.С. Жаворонкин
_____ 2020 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2020 г.

**Комплексная защита информационной системы персональных
данных в Пермской таможне Приволжского таможенного
управления Федеральной таможенной службы России**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2020.457.ПЗ ВКР

Руководитель проекта,
доцент кафедры
«Защита информации»

_____ В.Ю. Бердюгин
_____ 2020 г.

Автор проекта,
студент группы КЭ-555

_____ К.А. Шевалдин
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Шевалдин К.А. Комплексная защита информационной системы персональных данных в Пермской таможне Приволжского таможенного управления Федеральной таможенной службы России – Челябинск: ЮУрГУ, КЭ-555, 97 с., 2 ил., 7 табл., библиогр. список – 14 назим., 9 прил.

Выпускная квалификационная работа выполнена с целью создания комплексной системы защиты персональных данных в Пермской таможне.

В выпускной квалификационной работе отражены все этапы создания системы защиты персональных данных, от сбора исходных данных до выработке рекомендаций по защите персональных данных, обрабатываемых в ИСПДН.

Первая глава посвящена сбору общей информации об объекте защиты. На основе полученных данных был составлен Акт присвоения уровня значимости и Частная модель угроз.

Во второй главе был составлен перечень мер по обеспечению защиты информации, обрабатываемой в ИСПДн «Обращения заявителей» и разработана Концепция информационной безопасности информационных систем персональных данных Пермской таможни, определяющая систему взглядов на проблему обеспечения безопасности информации в ИСПДн Пермской таможни, и излагающая цели и задачи защиты, принципы построения, организационные, инженерно-технические и физические аспекты обеспечения на объекте защиты.

Третья глава посвящена определению реализации мер обеспечения ИБ, выявленных во второй главе.

					ЮУрГУ – 10.05.03.2020.457.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Шевалдин			<i>Комплексная защита информационной системы персональных данных в Пермской таможне Приволжского таможенного управления Федеральной таможенной службы России</i>	Лит.	Лист	Листов
Пров.		Бердюгин					6	97
Реценз.		Жаворонкин				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	9
ВВЕДЕНИЕ.....	12
1 АНАЛИЗ И ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	14
1.1 Анализ деятельности организации.....	14
1.2 Организационная система	16
1.3 Характеристика ИСПДн	17
1.4 Объекты защиты.....	20
1.5 Перечень персональных данных	21
1.6 Определение уровня защищенности ИСПДн	22
1.7 Создание Частной модели угроз.....	22
1.8 Выводы по главе.....	24
2 РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ.....	25
2.1 Определения перечня мер по обеспечению безопасности информации... ..	25
2.2 Разработка Концепции информационной безопасности информационных систем персональных данных Пермской таможни.....	30
2.3 Выводы по главе.....	30
3 РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.....	31
3.1 Программно-аппаратные меры	31
3.1.1. Проверка соответствия установленным СЗИ требованиям по ЗИ.....	31
3.1.2. Проверка настроек СЗИ.....	31
3.2 Организационные меры.....	32
3.3 Инженерно-технические и физические меры защиты	33
3.4 Реализация мер по обеспечению безопасности в ИСПДн	34
3.5 Выводы по главе.....	40
ЗАКЛЮЧЕНИЕ	42
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	43
ПРИЛОЖЕНИЕ А	45
ПРИЛОЖЕНИЕ Б.....	46
ПРИЛОЖЕНИЕ В	55
ПРИЛОЖЕНИЕ Г	72
ПРИЛОЖЕНИЕ Д	79

ПРИЛОЖЕНИЕ Е	83
ПРИЛОЖЕНИЕ Ж	87
ПРИЛОЖЕНИЕ К	91
ПРИЛОЖЕНИЕ Л	94

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место.

БД – база данных.

ИС – информационная система.

НСД – несанкционированный доступ.

ОС – операционная система.

ОТСС – основные технические средства и системы.

ПДн – персональные данные.

ПК – персональный компьютер.

ПИ – программное изделие.

ПО – программное обеспечение.

СЗИ – средство защиты информации.

СЗИ от НСД – средство защиты информации от несанкционированного доступа.

УЗ – уровень защищенности.

ФСБ – Федеральная служба безопасности Российской Федерации.

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ФТС – Федеральная таможенная служба.

ТЗ – техническое задание.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Администрирование – один из этапов технологического процесса, в рамках которого производятся служебные операции как с хранимой информацией (резервирование и восстановление), так и с программными средствами обработки и защиты информации.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Ввод информации – один из этапов технологического процесса, в рамках которого производится создание либо перемещение информации с внешних носителей на внутренние носители (несъемные МН).

Вывод информации – один из этапов технологического процесса, в рамках которого происходит перемещение информации с внутренних МН на внешние носители (в том числе монитор).

Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Обработка информации – один из этапов технологического процесса, в рамках которого происходит преобразование информации, которая получена на этапе ввода или которая хранится в упорядоченном виде, для последующего ее вывода или хранения.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Система защиты информации от несанкционированного доступа (СЗИ от НСД) – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Средство защиты от несанкционированного доступа (Средство защиты от НСД) – программное, техническое или программно-техническое средство, назна-

чение которого – предотвращение или существенное препятствие несанкционированного доступа.

Субъект доступа – Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технологический процесс обработки информации (ТП) – порядок действий пользователей при работе с информацией, которые включает в себя: ввод, обработку (преобразование), хранение, передачу, вывод, администрирование (резервирование, управление доступом).

Техническое обслуживание – этап технологического процесса, на котором производятся служебные операции с аппаратными средствами обработки и защиты информации.

Хранение информации – этап технологического процесса, на котором информация размещается в структурированном виде в период между двумя любыми этапами технологического процесса.

ВВЕДЕНИЕ

Информация всегда была важным ресурсом, как для человека, так и для организации, но сейчас при стремительном развитии информационных технологий, очень остро стоит вопрос о защите этого ресурса, ведь злоумышленники так же оперативно находят всё новые и новые способы, методы и инструменты, направленные на нарушение целостности, доступности и конфиденциальности информации. Надежная обработка и сохранность персональных данных является необходимым элементом в развитии любой сферы деятельности. Защитить информационные ресурсы можно с помощью построения комплексной системы защиты информации.

Комплексная система защиты информации (КСЗИ) – это сочетание организационно-правовых мероприятий и инженерно-технических методов и средств, нацеленных на обеспечение эффективной защиты информации от разглашения, утечки и несанкционированного доступа.

Актуальность данной работы заключается в создании комплексной системы защиты информации в Пермской таможне в целях соответствия требованиям безопасности, предъявляемым к информационным системам персональных данных.

Объектом выпускной квалификационной работы является Пермская таможня.

Предметом моей выпускной квалификационной работы является комплексная система защиты информационной системы персональных данных «Обращения заявителей».

Целью выпускной квалификационной работы является создание комплексной защиты информационной системы персональных данных «Обращения заявителей».

Для достижения поставленной цели необходимо выполнить:

1. Анализ деятельности Пермской таможни, характеристика ИСПДн, защищаемой информации.
2. Создание частной модели угроз на основе нормативных документов ФСТЭК и ФТС.

3. Разработка Концепции информационной безопасности информационной системы персональных данных Пермской таможни

4. Определение перечня мер по обеспечению безопасности ИСПДн «Обращения заявителей»

5. Выработка рекомендаций комплексной системы защиты информации.