

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 отдела ин-
формационно-электронного обору-
дования МУП Дворец спорта
«Юность» _____ А.В. Милов
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

**Разработка системы защиты
информационной системы персональных данных
МУП Дворец спорта «Юность»**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.05.2019.402.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-572

_____ О.А. Горшков
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Горшков О.А Организация защиты информационной системы персональных данных МУП Дворец спорта «Юность» – Челябинск: ЮУрГУ, КЭ-572, 93 с., 5 ил., 14 табл., библиогр. список – 20 наим., 10 прил.

Выпускная квалификационная работа выполнена с целью создания защиты информационной системы персональных данных в МУП Дворец спорта «Юность».

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.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающих информационную систему персональных данных предприятия. Было проведено проектирование системы защиты, включающее в себя выбор средств защиты, предотвращающих актуальные угрозы предприятия.

					ЮУрГУ – 10.05.05.2019.402.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Горшков			<i>Разработка системы защиты информационной системы персональных данных МУП Дворец спорта «Юность»</i>	Лит.	Лист	Листов
Пров.		Уторов					6	93
Реценз.		Милов				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ.....	9
ВВЕДЕНИЕ.....	11
1 ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ МУП ДВОРЕЦ СПОРТА «ЮНОСТЬ».....	12
1.1 Разработка технического паспорта.....	12
1.2 Выявление защищаемой информации.....	12
1.3 Информационные ресурсы.....	12
1.4 Выявление объектов защиты.....	15
1.5 Выбор и обоснование модели нарушителя.....	16
1.6 Перечень мер защиты информации для защиты ИСПДн.....	16
1.7 Разработка частной модели угроз и уязвимостей для важных объектов защиты.....	16
1.7.1 Расчет рисков важных объектов защиты.....	23
1.8 Разработка технического задания.....	26
1.9 Вывод.....	27
2 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	28
2.1 Анализ российского и зарубежного опыта в области персональных данных.....	28
2.1.1 Законодательство США в области защиты персональных данных.....	28
2.1.2 Российское законодательство в области защиты персональных данных.....	30
2.2. Методика расчета рисков.....	31
2.3 Сравнение систем защиты информации от НСД.....	32
2.3.1 Возможности Secret Net 7.....	32
2.3.2 Возможности Dallas Lock 8.0 – К.....	34
2.4 Сравнение систем межсетевого экранирования.....	35
2.4.1 Межсетевой экран Security Studio Endpoint Protection.....	35
2.4.2 Межсетевой экран ViPNet Coordinator HW 1000.....	36
2.5 Антивирус Kaspersky Endpoint Protection 10 для Windows.....	37
2.6 Вывод.....	38
3 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МУП ДВОРЕЦ СПОРТА «ЮНОСТЬ».....	39
3.1 Описание объекта.....	39
3.2 Резюме проекта.....	39
3.3 Цели и задачи проекта.....	39
3.4 Объекты поставки проекта.....	39
3.4.1 Организационно-распорядительная документация.....	39
3.4.2 Программно-аппаратные и инженерно-технические меры.....	40
3.4.3 Обучение персонала.....	40
3.5 Структура разбиения работ.....	40

3.6 Структурная схема организации проекта.....	42
3.7 Матрица ответственности.....	42
3.8 Диаграмма Ганта и сетевой график.....	43
3.9 Вывод.....	43
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	44
4.1 Организация рабочего места.....	44
4.2 Требования к микроклимату.....	44
4.3 Требования к уровню шума.....	45
4.4 Требования к освещенности.....	45
4.5 Требования к организации рабочих мест.....	46
4.6 Электробезопасность.....	47
4.7 Пожарная безопасность.....	48
4.8 Рекомендации по организации режима труда и отдыха.....	49
4.9 Сравнение параметров рабочего места с допустимыми нормами....	50
4.10 Вывод.....	52
ЗАКЛЮЧЕНИЕ.....	53
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	54
ПРИЛОЖЕНИЕ А.....	56
ПРИЛОЖЕНИЕ Б.....	61
ПРИЛОЖЕНИЕ В.....	65
ПРИЛОЖЕНИЕ Г.....	67
ПРИЛОЖЕНИЕ Д.....	69
ПРИЛОЖЕНИЕ Е.....	76
ПРИЛОЖЕНИЕ Ж.....	81
ПРИЛОЖЕНИЕ З.....	86
ПРИЛОЖЕНИЕ К.....	89
ПРИЛОЖЕНИЕ Л.....	92

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
БД – база данных;
ВТСС – вспомогательные технические средства и системы;
ОТСС – основные технические средства и системы;
ЗИ – защита информации;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИБ – информационная безопасность;
ИТ – информационные технологии;
КЗ – контролируемая зона;
КСЗ – комплекс средств защиты;
НСД – несанкционированный доступ;
ОС – операционная система;
ПО – программное обеспечение;
ПДн – персональные данные;
ПЭВМ – персональная электронно-вычислительная машина;
ПЭМИН – побочные электромагнитные излучения и наводки;
РД – руководящие документы;
РФ – Российская Федерация;
ТЗ – техническое задание;
ФЗ – Федеральный закон;
ФСБ – Федеральная Служба Безопасности
ФСТЭК – Федеральная Служба по Техническому и Экспортному Контролю;
ЭВМ – электронно-вычислительная машина.

Объект защиты информации – информация или носитель информации, или информационный процесс, который необходимо защищать в соответствии и целью защиты информации;

Защита информации от НСД – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами или обладателями информации прав и правил разграничения доступа к защищаемой информации;

Угроза – совокупность факторов и условий, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

Уязвимость – свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

Модель угроз информационной безопасности – физическое, описательное, математическое представление свойств или характеристик угроз безопасности информации.

ВВЕДЕНИЕ

Развитие информационных технологий в различных отраслях деятельности приводят к увеличению оборота информации. Можно наблюдать тенденцию развития электронного документооборота, который постепенно вытесняет бумажный. В настоящее время на любом предприятии персональные данные сотрудников и клиентов хранятся и обрабатываются на электронных носителях.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

- многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации;
- увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры;
- персональные данные все чаще интересуют злоумышленников.

Объектом выпускной квалификационной работы является МУП Дворец спорта «Юность».

Предметом выпускной квалификационной работы является ИСПДн МУП Дворец спорта «Юность».

Целью дипломной работы является организация защиты ИСПДн.

В соответствии с поставленной целью необходимо решить следующие задачи:

- проанализировать информационные системы предприятия с целью выявления информации ограниченного доступа, уязвимостей и угроз к этой информации;
- провести анализ и теоретическое обоснование выбора средств защиты информации;
- разработать техническое задание по организации системы защиты ИСПДн МУП Дворец спорта «Юность».
- разработать технический паспорт;
- выявить защищаемую информацию, объекты защиты;
- разработать модель угроз ИСПДн;
- рассчитать риски для выявленных объектов защиты;
- рассмотреть подробно актуальные угрозы исходя из модели угроз ИСПДн;
- сравнить и выбрать средства защиты информации;
- провести соответствующие работы по защите информации;