

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

РАБОТА ПРОВЕРЕНА

Начальник отдела защиты инфор-
мационных систем ООО «ПНК»

_____ О.А. Наумова
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2019 г.

**Разработка системы защиты персональных данных
в муниципальном бюджетном учреждении здравоохранения**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2019.385.ПЗ ВКР**

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент

_____ Н.В. Глотова
_____ 2019 г.

Экономическая часть,
ст.преп

_____ С.А. Сабельников
_____ 2019 г.

Руководитель проекта,
Индивидуальный
предприниматель

_____ С.А. Сабельников
_____ 2019 г.

Автор проекта,
студент группы КЭ-570

_____ К.С. Полуянов
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Полуянов К.С. Разработка системы защиты персональных данных в муниципальном бюджетном учреждении здравоохранения. – Челябинск: ЮУрГУ, КЭ-570, 88 с., 8 ил., 9 табл., библиогр. список – 20 наим., 7 прил.

Целью выполнения выпускной квалификационной работы является создание системы защиты персональных данных в учреждении здравоохранения, а именно в Муниципальном бюджетном учреждении здравоохранения Городская клиническая больница №11.

В ходе выполнения работы на примере организации здравоохранения показано, как проходит адаптация информационной системы и персонала, допущенного к обработке персональных данных, к выполнению требований законодательства в области защиты персональных данных. Также показано, как организовать внутреннюю работу.

В первой главе работы было проведено обследование учреждения, в рамках которого была описана ИСПДн «Пациенты», а также составлены необходимые документы, регламентирующие порядок защиты информации.

Во второй главе из всех возможных методов защиты выбраны необходимые с точки зрения требований законодательства для актуальных угроз.

В третьей главе раскрыта организация и состав работ по защите ИСПДн, «Пациенты»: расчет рисков, матрица ответственности и диаграмма Гранта.

Четвертая глава посвящена безопасности жизнедеятельности.

Ввиду того, что информация, приведённая в данной выпускной квалификационной работе, является информацией ограниченного доступа, некоторые данные могут быть искажены.

					ЮУрГУ – 10.05.03.2019.385.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Полуянов			<i>Разработка системы защиты персональных данных в муниципальном бюджетном учреждении здравоохранения.</i>	Лит.	Лист	Листов
Пров.		Сабельников					6	88
Реценз.		Наумова				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ.....	9
ВВЕДЕНИЕ	10
1 ПРОВЕДЕНИЕ ОБСЛЕДОВАНИЯ УЧРЕЖДЕНИЯ.....	11
1.1 Правовые основы защиты информации	11
1.2 Описание информационной системы	11
1.3 Описание технологического процесса	15
1.4 Разработка технического паспорта на информационную систему	18
1.5 Определение объектов защиты	20
1.6 Разработка частной модели угроз для важных объектов	20
защиты	20
1.6.1 Вероятность реализации угроз безопасности персональных данных	22
1.6.2 Определение уровня исходной защищенности ИСПДн.....	22
1.6.3 Определение вероятности реализации угроз в ИСПДн.....	24
1.6.4 Возможность реализации угроз	24
1.6.5 Оценка опасности угроз.....	24
1.6.6 Определение актуальности угроз в ИСПДн	25
1.7 Разработка технического задания.....	28
1.8 Вывод по первой главе.....	29
2 ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ	31
2.1 Теоретическое обоснование использования сертифицированных средств	31
защиты информации	31
2.2 Обзор представленных на рынке средств защиты информации.....	31
2.2.1 Средства защиты от несанкционированного доступа	31
2.2.2 Средства антивирусной защиты	32
2.3 Угрозы несанкционированного доступа информации.....	32
2.5 Вывод по второй главе.....	33
3 ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ	34
3.1 Описание объекта защиты	34
3.2 Объекты поставки	34
3.2.1 Организационно-распорядительная документация	34
3.2.2 Программно-аппаратные меры	35
3.2.3 Обучение персонала	35
3.3 Матрица ответственности	35
3.4 Диаграмма Ганта	37

3.5 Вывод по третьей главе.....	40
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ	41
4.1 Общие требования к организации рабочих мест пользователей.....	41
4.2 Требования к помещениям для размещения рабочего места.....	42
4.3 Требования к уровням шума на рабочих местах.....	43
4.4 Требования к освещению на рабочих местах	43
4.5 Требования к микроклимату	44
4.6 Требования к электробезопасности	45
4.7 Пожарная безопасность	46
4.8 Сравнение параметров рабочего места с допустимыми нормами.....	47
4.9 Вывод по четвертой главе	48
ЗАКЛЮЧЕНИЕ	49
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	50
ПРИЛОЖЕНИЕ А	52
ПРИЛОЖЕНИЕ Б.....	54
ПРИЛОЖЕНИЕ В.....	59
ПРИЛОЖЕНИЕ Г	64
ПРИЛОЖЕНИЕ Д	67
ПРИЛОЖЕНИЕ Е.....	83
ПРИЛОЖЕНИЕ Ж.....	86

СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
МЭ – межсетевой экран;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОС – операционная система;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
СВТ – средство вычислительной техники;
СЗИ – средства защиты информации;
УБПДн – угрозы безопасности персональных данных;
ФЗ – Федеральный закон;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ВВЕДЕНИЕ

Сведения о состоянии здоровья относятся к специальной категории персональных данных в соответствии с частью 1 статьи 10 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»[1]. Раскрытие этих сведений о субъекте персональных данных поставит под угрозу неприкосновенность его частной жизни, личную и семейную тайну, защита которых и является основной целью вышеупомянутого федерального закона.

За последние несколько лет произошел значительный скачок в развитии информационной инфраструктуры лечебных учреждений. Появилась возможность удалённой записи на прием к врачу, активно внедряются специальные медицинские информационные системы (далее – МИС). В перспективе ожидается внедрение электронной медицинской карты, полная автоматизация лабораторий и создание единой информационной системы федерального уровня, а также полноценное автоматизированное обслуживание операционных и поддержка оперирующего врача в режиме реального времени. По мере информатизации отрасли и автоматизации сети лечебно-профилактических учреждений (далее – ЛПУ) вопрос защиты персональных данных встает особо остро. Именно поэтому необходимо обеспечивать защиту информационных систем персональных данных в муниципальных учреждениях здравоохранения, двери которых открыты для каждого, без исключения, гражданина Российской Федерации.

Объектом данной выпускной квалификационной работы является городская клиническая больница.

Предметом выпускной квалификационной работы является ИСПДн «Пациенты».

Целью работы является организация защиты информационной системы, обрабатывающей данные о пациентах.

Таким образом, актуальность данной работы обусловлена требованиями закона «О персональных данных», и, как следствие, необходимостью обеспечения защиты ИСПДн «Пациенты».

В соответствии с поставленной целью необходимо решить следующие задачи:

- провести обследование учреждения для того, чтобы определить исходный уровень защищенности, программный и аппаратный состав автоматизированных рабочих мест (далее – АРМ) в ЛПУ;
- выбрать необходимые средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения информационной безопасности;
- разработать пакет организационно-распорядительной документации учреждения;
- обеспечить реализацию режима безопасности помещений больницы.