

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, Заместитель директора
по информационной безопасности
ООО «ИТ Энигма»

_____ Г.М. Галина
_____ 2020 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2020 г.

**Обеспечение безопасности информации информационных
систем и автоматизированных систем управления
ГБУЗ «Противотуберкулёзный диспансер»**

Руководитель проекта,
начальник _____ отдела
информационной безопасности
Специального управления
ЮУрГУ

_____ И.С. Антясов
_____ 2020 г.

Автор проекта,
студент группы КЭ-555

_____ Н.А. Шестопалова
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Шестопалова Н.А. Обеспечение безопасности информации информационных систем и автоматизированных систем управления ГБУЗ «Противотуберкулёзный диспансер» – Челябинск: ЮУрГУ, КЭ-555, 203 с., 2 ил., 16 табл., библиогр. список – 12 наим., 8 прил.

Работа посвящена исследованию вопроса обеспечения информационной безопасности медицинского учреждения как объекта критической информационной инфраструктуры областного центра.

Первая глава посвящена анализу субъекта критической инфраструктуры, выявлению процессов на основании видов деятельности ГБУЗ «Противотуберкулёзный диспансер», отраженных в учредительных документах, лицензиях. Содержится информация о существующих информационных системах и автоматизированных системах управления, являющихся объектами критической информационной инфраструктуры.

Вторая глава включает анализ угроз информационной безопасности, а также разработку требований, предъявляемые к объектам критической инфраструктуры медицинского учреждения.

Третья глава посвящена совершенствованию системы защиты критической информационной инфраструктуры в части внедрения организационных мер, технической и физической защиты информации.

					ЮУрГУ – 10.05.03.2020.419.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Шестопалова			Обеспечение информационной безопасности информации информационных систем и автоматизированных систем управления ГБУЗ «Противотуберкулёзный диспансер»	Лит.	Лист	Листов
Пров.		Антясов					6	203
Реценз.		Галина				ЮУрГУ		
Н. Кон.		Маргынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ	9
ВВЕДЕНИЕ.....	10
1 СВЕДЕНИЯ О СУБЪЕКТЕ КИИ.....	11
1.1 Общая информация о субъекте КИИ	11
1.2 Деятельность субъекта КИИ.....	12
1.3 Создание комиссии по категорированию объектов критической информационной инфраструктуры	13
1.4 Определение и описание процессов предприятия.....	14
1.5 Определение критических процессов	16
1.6 Объекты критической информационной инфраструктуры	17
1.7 Информационные системы, обеспечивающие критические процессы..	23
1.8 Автоматизированные системы управления, обеспечивающие критические процессы	26
1.9 Выводы.....	28
2 КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ.....	29
2.1 Источники угроз безопасности информации и результаты оценки возможностей нарушителя (модель нарушителя)	29
2.2 Определение актуальных угроз информационной безопасности учреждения.....	36
2.3 Оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на ОКИИ.....	43
2.4 Определение категории значимости выявленных ОКИИ.....	44
2.5 Выводы.....	46
3 СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ объектов КИИ.....	47
3.1 Установление требований к обеспечению безопасности значимого объекта.....	47
3.2 Выбор средств защиты информации.....	54
3.3 Разработка ОРД.....	56
3.4 Определение оптимального комплекса мер и методов обеспечения информационной безопасности	57
3.5 Выводы.....	66
ЗАКЛЮЧЕНИЕ	67
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	68
ПРИЛОЖЕНИЕ А	70

ПРИЛОЖЕНИЕ Б.....	71
ПРИЛОЖЕНИЕ В	74
ПРИЛОЖЕНИЕ Г.....	75
ПРИЛОЖЕНИЕ Д.....	159
ПРИЛОЖЕНИЕ Е	161
ПРИЛОЖЕНИЕ Ж	163
ПРИЛОЖЕНИЕ З.....	171
ПРИЛОЖЕНИЕ И.....	180

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

АИБ – администратор информационной безопасности
АПКШ – аппаратно-программный комплекс шифрования
АРМ – автоматизированное рабочее место
АС – автоматизированная система
ВКР – выпускная квалификационная работа
ЗОКИИ – значимый объект критической информационной инфраструктуры
ИАС – информационно-аналитическая система
ИБ – информационная безопасность
ИБП – источник бесперебойного питания
ИС – информационная система
ИСПДн – информационная система персональных данных
КИИ – критическая информационная инфраструктура
НЖМД – накопитель на жестких магнитных дисках
НСД – несанкционированный доступ
ОКИИ - объект критической информационной инфраструктуры
ОС – операционная система
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПЭВМ – персональная электронная вычислительная машина
САВЗ – средство антивирусной защиты
СВТ – средство вычислительной техники
СЗИ – система защиты информации
СКЗИ – система криптографической защиты информации
СКИИ – субъект критической информационной инфраструктуры
СрЗИ – средство защиты информации
ТС – техническое средство
ФСТЭК – Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

Объектом выпускной квалификационной работы было выбрано Государственное бюджетное учреждение здравоохранения «Противотуберкулезный диспансер», действующий в области здравоохранения и являющийся субъектом критической информационной инфраструктуры.

Противотуберкулёзный диспансер является центром фтизиатрической службы, в котором проводят дифференциальную диагностику туберкулёза, медицинские осмотры, осуществляют консультирование и комплексное лечение больных туберкулёзом различной локализации, а также динамическое наблюдение пациентов и постоянно контактирующих с ними лиц.

Предметом выпускной квалификационной работы является безопасность объектов критической информационной инфраструктуры ГБУЗ «Противотуберкулезный диспансер».

Целью дипломной работы является обеспечение безопасности объектов критической информационной инфраструктуры ГБУЗ «Противотуберкулезный диспансер».

Задачи, необходимые для выполнения поставленной цели:

1. Создание комиссии по категорированию;
2. Определение процессов учреждения;
3. Выявление критических процессов;
4. Определение объектов КИИ;
5. Формирование перечня объектов КИИ;
6. Сбор исходных данных об объекте КИИ;
7. Оценка значимости объектов КИИ;
8. Присвоение категории значимости объектов КИИ;
9. Составление Актов категорирования объектов КИИ;
10. Подготовка сведений о категорировании объектов КИИ;
11. Разработка мер по обеспечению безопасности значимых объектов КИИ.