

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение  
высшего образования  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
по выполнению самостоятельных работ  
по дисциплине  
**КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА**  
**ПРЕДПРИЯТИИ**

Направление подготовки	10.03.01 Информационная безопасность
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск 2020 г.

## СОДЕРЖАНИЕ

	Стр.
1. Введение	4
2. Задание для выполнения самостоятельной работы	5
Приложения	6
Список рекомендуемой литературы	8

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

## “Комплексная система защиты информации на предприятии”

### 1. ВВЕДЕНИЕ.

Дисциплина "Комплексная система защиты информации на предприятии" является одной из общепрофессиональных дисциплин для студентов, обучающихся по направлению (специальности) 090900.62 " Информационная безопасность". Она формирует первоначальные знания по профилю специальности и овладение основным понятийным аппаратом и базовым теоретическим материалом, является обязательной для каждого студента.

Самостоятельная работа должна быть оформлена в электронном виде и на листах формата А4.

На титульном листе указывается фамилия, имя, отчество, наименование работы, вариант, курс, группа и домашний адрес. По всем вопросам, возникающим при изучении дисциплины, следует обращаться за разъяснением и консультацией на кафедру Комплексной защиты информации и стандартизации.

Самостоятельная работа ставит перед собой цель: теоретическая и практическая подготовка студентов в области проектирования, создания и эксплуатации комплексных систем защиты информации на предприятии.

Для осуществления цели необходимо ставятся задачи по следующим вопросам:

- сущность и задачи комплексной системы защиты информации (КСЗИ);
- принципы организации и этапы разработки КСЗИ;
- определение и нормативное закрепление объектов и субъектов защиты;
- анализ и оценка угроз безопасности информации;
- определение компонентов КСЗИ;
- построение моделей КСЗИ;
- принципы и методы планирования функционирования КСЗИ;
- состав методов и моделей оценки эффективности КСЗИ.

В результате выполнения работы студент должен освоить:

- состав компонентов комплексной системы обеспечения информационной безопасности;
- функциональные и вспомогательные подсистемы;
- технологию проектирования и оценки надежности системы защиты.

В результате выполнения работы студент должен научиться:

- самостоятельно анализировать и оценивать угрозы информации, применяя соответствующие модели;
- проектировать архитектуру системы защиты, ее технологическое и

организационное построение;

- применять эффективные методы управления безопасностью.

Получить навыки:

- выявления угроз информационной безопасности на предприятии;
- выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию;
- определения компонентов КСЗИ;
- разработки моделей КСЗИ;
- использования методов планирования функционирования КСЗИ;
- реализации методов и моделей оценки эффективности КСЗИ.

## **2. Задание для выполнения самостоятельной работы**

2.1. Отработать технический паспорт (Паспорт формуляр) на защищаемую информационную сеть. ОТСС, ВТСС.

2.2. Схемы на информационную сеть.

2.3. Схема электропитания.

2.4. Схема заземления.

Объекты защиты:

### **А. Автоматизированные системы различного уровня и назначения**

- 1) Автоматизированные рабочие места служащих
- 2) АРМ секретаря главы города
- 3) АРМ главы города

### **В. Системы связи, системы отображения и размножения**

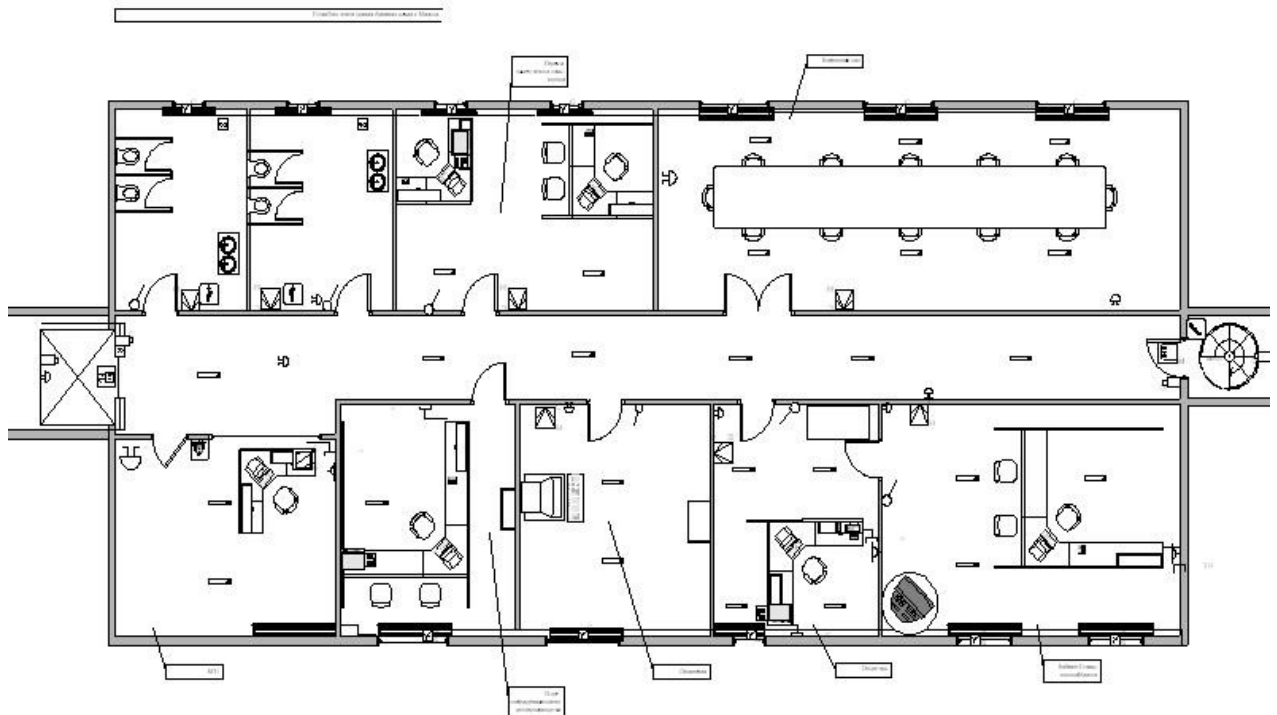
- 1) средства и системы телефонной, внутренней телефонной, громкоговорящей связи;
- 2) телефонная система «Внутренняя»
- 3) средства и системы звукоусиления;
- 4) система конфиденциального делопроизводства (учет, размножение и движение бумажных и прочих внешних носителей информации);
- 5) система обработки информации в вычислительной сети (ввод, вычисления, хранение, вывод);
- 6) система обработки речевой информации в специально предназначенных (защищаемых) помещениях (переговоры, совещания);
- 7) автоматизированная система передачи информации между сетями по неконтролируемой территории (файлы, базы данных, факсы, телефонные разговоры).

### **С. Помещения, в которых установлены А, В, С.**

- 1) Кабинет главы города
- 2) Кабинет секретаря главы города

- 3) Архив/серверная
- 4) Бухгалтерия
- 5) Юридический отдел
- 6) Отдел муниципальной службы кадров
- 7) Отдел службы безопасности
- 8) Отдел по работе с кадрами и защите прав потребителей.

Приложения:  
План здания



Форма технического паспорта на автоматизированную систему

УТВЕРЖДАЮ

Руководитель автоматизированной системы

\_\_\_\_\_

"\_\_" \_\_\_\_\_ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

*указывается полное наименование автоматизированной системы*

РАЗРАБОТАЛ

СОГЛАСОВАНО

Представитель подразделения  
по защите информации

"\_\_" \_\_\_\_\_ г.

(Год)

1. Общие сведения об АС

1.1. Наименование АС: *полное наименование АС*

1.2. Расположение АС: *адрес, здание, строение, этаж, комнаты*

1.3. Класс АС: *номер и дата акта классификации АС, класс АС*

2. Состав оборудования АС

2.1. Состав ОТСС:

Таблица 1

ПЕРЕЧЕНЬ  
основных технических средств и систем, входящих в состав АС

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам

2.2. Состав ВТСС объекта:

Таблица 2

ПЕРЕЧЕНЬ  
вспомогательных технических средств, входящих в состав АС  
(средств вычислительной техники, не участвующих в обработке  
конфиденциальной информации)

№ п/п	Тип ВТСС	Заводской номер	Примечание

2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта:

- о структурная (топологическая) схема с указанием информационных связей между устройствами; схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны, схема прокладки линий передачи конфиденциальной информации с привязкой к границам контролируемой зоны объекта.

2.4. Системы электропитания и заземления:

- о схемы электропитания и заземления ОТСС объекта. Схемы прокладки кабелей и шины заземления. Схемы расположения трансформаторной подстанции и заземляющих устройств с привязкой к границам контролируемой зоны объекта. Схемы электропитания розеточной и осветительной сети объекта. Сведения о величине сопротивления заземляющего устройства.

## 2.5. Состав средств защиты информации:

Таблица 3

ПЕРЕЧЕНЬ  
средств защиты информации, установленных на АС

№ п/п	Наименование и тип и технического средства	Заводской номер	Сведения о сертификате	Место и дата установки

### 3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

- о инвентарные номера аттестата соответствия, заключения по результатам аттестационных испытаний, протоколов испытаний и даты их регистрации.

### 4. Результаты периодического контроля.

Таблица 4

Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, номер отчетного документа

### Лист регистрации изменений

### Список рекомендуемой литературы:

1. Гафнер В. В. Г24 Информационная безопасность : учеб. пособие / В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с. — (Высшее образование). ISBN 978-5-222-17389-3.
2. Программно-аппаратная защита информации: [учеб. пособие]/ П. Б. Хорев.- М.: Форум, 2012.- 352 с. ISBN 978-5-91134-353-8.