



## **1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

### **1.1 Область применения программы**

Учебная программа дисциплины является частью образовательной программы в соответствии с ФГОС по специальности **10.02.01 «Организация и технология защиты информации»**, входящие в укрупненную группу специальностей **10.00.00 «информационная безопасность»** в части освоения основного вида профессиональной деятельности (ВПД): «Участие в планирование и организации работ по обеспечению защиты объекта» и формирования соответствующих профессиональных компетенций (ПК):

ПК 1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2 Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3 Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

ПК 1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.

ПК 1.6 Обеспечить технику безопасности при проведении организационно-технических мероприятий.

ПК 1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.

ПК 1.8 Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9 Участвовать в оценке качества защиты объекта.

### **1.2 Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

С целью овладения указанным видом профессиональной деятельности и формирования соответствующих профессиональных компетенций, обучающихся в ходе освоения профессионального модуля должен:

#### **Иметь практический опыт:**

- использование физических средств защиты информации;
- применение физических средств контроля доступа на объект;
- ведение текущей работы исполнителей с конфиденциальной информацией.

#### **Уметь:**

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности;
- использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;

-проводить инструктаж персонала по организации работы с конфиденциальной информацией;

-контролировать соблюдение персонала требований режима защиты информации.

**Знать:**

-виды и способы охраны объекта;

-особенности охраны персонала организации;

-основные направления и методы организации режима и охраны объекта;

-разрешительную систему доступа к конфиденциальной информации;

-принципы действия аппаратуры систем контроля доступа;

-принципы построения и функционирования биометрических систем безопасности;

-требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;

-требования режима защиты информации при приеме в организации посетителей;

-организацию работы при осуществлении международного сотрудничества;

-требования режима защиты информации в процессе рекламной деятельности;

-требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;

-задачи, функции и структуру подразделений защиты информации;

-принципы, методы и технологию управления подразделений защиты информации;

-порядок оформления допуска лиц к конфиденциальным сведениям;

-методы проверки персонала по защите информации;

-процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

**1.3.Количество часов на освоение программы учебной дисциплины:**

всего-**249** часа, в том числе:

максимальной учебной нагрузки обучающегося-**176** часа, включая:

обязательной аудиторной учебной нагрузки обучающегося- **76** часа;

самостоятельной работы обучающегося-**73** часов.

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимся видом профессиональной деятельности (ВПД) «Участие в планирование и организации работ по обеспечению защиты объекта», в том числе профессиональным (ПК) и общим (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.1	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.
ПК 1.2	Участвовать в разработке программ и методик организации защиты информации на объекте.
ПК 1.3	Осуществлять планирование и организацию выполнения мероприятий по защите информации.
ПК 1.4	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.
ПК 1.5	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.
ПК 1.6	Обеспечить технику безопасности при проведении организационно-технических мероприятий.
ПК 1.7	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.
ПК 1.8	Проводить контроль соблюдения персоналом требований режима защиты информации.
ПК 1.9	Участвовать в оценке качества защиты объекта.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2.	Организовать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (починных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Применять математический аппарат для решений различных задач.
ОК 11.	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12.	Ориентироваться в структуре федеральных органов исполнительной власти,

обеспечивающих информационную безопасность.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	249
Обязательная аудиторная учебная нагрузка, в том числе	176
Лабораторные занятия	
практические и семинарские занятия	76
Контрольные работы	
Курсовая работа (проект)	22
Самостоятельная работа обучающегося (всего)	73
В том числе:	
Внеаудиторная самостоятельная работа	
Самостоятельная работа над курсовой работой (проектом)	
<i>Промежуточная аттестация в 7 семестре в форме экзамена</i>	

**3.2. Тематический план профессионального модуля  
ПМ.01 Участие в планирование и организации работ по обеспечению защиты объекта**

Код ПК	Наименования разделов ПМ	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			
			Всего, часов	В т.ч., лабораторные работы и практические занятия, часов	В т.ч., курсовая работа (проект), часов	Всего, часов	В т.ч., курсовая работа (проект), часов	Учебная, часов	Производственная (по профилю специальности), часов
1	2	3	4	5	6	7	8	9	10
МДК.1.1 Обеспечение организации систем безопасностям		117	88	32	22	29	-	-	-
ПК 1.1 ПК 1.2 ПК 1.3	Раздел 1. Основные понятия безопасности предприятия	17	12	6	-	5	-	-	-
ПК 1.1 ПК 1.2 ПК 1.3 ПК 1.4	Раздел 2. Уязвимость информации	7	4	2	-	3	-	-	-
ПК 1.4 ПК 1.5	Раздел 3. Требования к защите информации	17	12	5	-	5	-	-	-
ПК 1.7 ПК 1.9	Раздел 4. Организация охраны	54	38	19	-	16	-	-	-

	предприятия и физической защиты								
<b>МДК.1.2</b>	Организация работ подразделений защиты информации	66	44	22	-	22	-	-	-
<b>ПК 1.1</b> <b>ПК 1.2</b> <b>ПК 1.3</b> <b>ПК 1.4</b>	<b>Раздел 1.</b> Место и роль службы защиты информации в системе защиты информации	17	11	5	-	6	-	-	-
<b>ПК 1.4</b> <b>ПК 1.5</b> <b>ПК 1.6</b> <b>ПК 1.9</b>	<b>Раздел 2.</b> Принципы деятельности службы защиты информации	22	16	4	-	6	-	-	-
<b>ПК 1.1</b> <b>ПК 1.2</b> <b>ПК 1.3</b> <b>ПК 1.4</b> <b>ПК 1.5</b> <b>ПК 1.6</b>	<b>Раздел 3.</b> Подбор, расстановка и обучение сотрудников службы защиты информации	27	17	13	-	10	-	-	-
<b>МДК.1.3</b>	Организация работы персонала с конфиденциальной информацией	66	44	22	-	22	-	-	-
<b>ПК 1.1</b> <b>ПК 1.2</b> <b>ПК 1.3</b> <b>ПК 1.4</b>	<b>Раздел 1.</b> Особенности организации работ с конфиденциальным и документами	33	23	10	-	10	-	-	-
<b>ПК 1.4</b> <b>ПК 1.5</b>	<b>Раздел 2.</b> Особенности	33	21	12	-	12	-	-	-

<b>ПК 1.6</b> <b>ПК 1.9</b>	организации работ персонала с конфиденциальным и документами								
<b>ПК 1.1- ПК 1.9</b>	<b>Учебная практика, часов</b>	36						36	
<b>ПК 1.1- ПК 1.9</b>	<b>Производственная практика, (по профилю специальности), часов</b>	36							36
<b>Всего:</b>		249	176	76	22	73	-	36	36



**3.3. Содержание обучения по профессиональному модулю  
ПМ.1 «Участие в планирование и организации работ по обеспечению защиты объекта»**

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, домашняя работа	Объем часов	Уровень освоения	
<b>МДК.1.1 Обеспечение организации систем безопасности предприятия</b>		<b>117</b>		
<b>Раздел 1. Основные понятия безопасности предприятия</b>		<b>17</b>		
<b>Тема 1.1. Основные понятия безопасности предприятия</b>	<b>Содержание учебного материала</b>	<b>2</b>		
	1. Понятие и содержание безопасности предприятия. Цель обеспечение безопасности предприятия.	1	3	
	2. Предмет, объекты и субъекты безопасности предприятия.	1	3	
	<b>Практические занятия</b>		<b>2</b>	
	1. Концепция безопасности предприятия.	1		
	2. Структура концепции безопасности предприятия. Основные положения.	1		
	<b>Самостоятельная работа</b>		<b>1</b>	
	1. Подготовить доклад на тему: Средства и методы обеспечения безопасности предприятия. Критерии безопасности предприятия.	1		
<b>Тема 1.2. Виды угроз безопасности предприятия</b>	<b>Содержание учебного материала</b>	<b>3</b>		
	1. Понятие угроз безопасности предприятия и их классификация.	1	3	
	2. Сущность и содержание внутренних и внешних угроз безопасности предприятия.	1	3	
	3. Основные виды защищаемой информации.	1	3	
	<b>Практические занятия</b>		<b>2</b>	

	1.	Общая классификация охраняемой информации.	1	
	2.	Выделение категорий деловой информации.	1	
	<b>Самостоятельная работа</b>		<b>1</b>	
	1.	Подготовить доклад на тему: Определение и содержание наиболее важных показателей безопасности предприятия. Построение эффективной системы безопасности предприятия.	1	
<b>Тема 1.3.</b> Основные понятия безопасности предприятия	<b>Содержание учебного материала</b>		<b>1</b>	
	1.	Краткий обзор законодательства в области безопасности объекта.	1	3
	<b>Практические занятия</b>		<b>2</b>	
	1	Обзор российского законодательства в области безопасности объекта.	1	
	2.	Обзор зарубежного законодательства в области безопасности объекта.	1	
	<b>Самостоятельная работа</b>		<b>3</b>	
	1.	Подготовить доклад на тему: Диагностическое обследование системы безопасности предприятия. Последовательность работ при проведении аудита системы безопасности предприятия.	3	
<b>Раздел 2. Уязвимости информации</b>			<b>7</b>	
<b>Тема 2.1.</b> Методы и модели оценки уязвимости информации	<b>Содержание учебного материала</b>		<b>1</b>	
	1.	Эмпирический подход к оценке уязвимости информации.	1	3
	<b>Практические занятия</b>		<b>1</b>	
	1.	Практическая реализация модели «угроза –защита»	1	

	<b>Самостоятельная работа</b>	<b>1</b>	
	1. Подготовить доклад на тему: Государственная информационная политика. Проблемы информационной войны.	1	
<b>Тема 2.2.</b> Оценки уязвимости информации	<b>Содержание учебного материала</b>	<b>1</b>	
	1. Определение методики выявления уязвимостей объекта.	1	3
	<b>Практические занятия</b>	<b>1</b>	
	1. Рекомендации по использованию моделей оценки уязвимостей информации.	1	
	<b>Самостоятельная работа</b>	<b>2</b>	
	1. Подготовить доклад на тему: Проблемы информационной безопасности в сфере государственного и муниципального управления.	2	
<b>Раздел 3. Требования к защите информации</b>		<b>17</b>	
<b>Тема 3.1.</b> Методы определения требований к защите информации	<b>Содержание учебного материала</b>	<b>3</b>	
	1. Требования к защите информации, обусловленные спецификой объекта защиты	1	3
	2. Требования, определяемые структурой объекта защиты.	1	3
	3. Требования к безопасности информационных систем в России.	1	3
	<b>Практические занятия</b>	<b>2</b>	
	1. Классы защищенности средств вычислительной техники от несанкционированного доступа.	1	
	2. Факторы, влияющие на требуемый уровень защиты информации объекта защиты.	1	
	<b>Самостоятельная работа</b>	<b>1</b>	
1	Подготовить доклад на тему:	1	

		Государственная система правового обеспечения защиты информации в РФ. Государственная информационная безопасность РФ.		
<b>Тема 3.2.</b> Функции и задачи защиты информации	<b>Содержание учебного материала</b>		<b>2</b>	
	1.	Общие положения. Методы формирования функций защиты.	1	3
	2.	Функции защиты. Состояние и функции системы защиты информации.	1	3
	<b>Практические занятия</b>		<b>1</b>	
	1.	Классы задач защиты информации.	1	
	<b>Самостоятельная работа</b>		<b>2</b>	
	1.	Подготовить доклад на тему: Законодательство в области информационной безопасности. Радиоэлектронные системы и устройства защиты информации.	2	
<b>Тема 3.3.</b> Стратегии защиты информации.	<b>Содержание учебного материала</b>		<b>2</b>	
	1.	Организация защиты информации.	1	3
	2.	Уровень технологических схем обработки.	1	3
	<b>Практические занятия</b>		<b>2</b>	
	1.	Уровень структурно-организационного построения объекта обработки информации.	1	
	2.	Виды стратегии защиты информации.	1	
	<b>Самостоятельная работа</b>		<b>2</b>	
1	Подготовить доклад на тему: Информационные инфекции. Политика и модели безопасности.	2		

<b>Раздел 4. Организация охраны предприятия и физической защиты его объектов</b>		<b>83</b>		
<b>Тема 4.1.</b> Организация охраны предприятия	<b>Содержание учебного материала</b>		<b>8</b>	
	1.	Основные объекты охраны предприятия. Виды и способы охраны объекта.	2	3
	2.	Основные задачи охраны объекта. Основные направления и методы организации режима и охраны объекта.	2	3
	3.	Задачи и функции службы безопасности предприятия.	2	3
	4.	Основные обязанности сотрудников подразделений охраны объекта. Особенности охраны персонала организации.	2	3
	<b>Практические занятия</b>		<b>3</b>	
	1.	Требования, предъявляемые к системе охраны.	1	
	2.	Организация охраны персонала, территорий, зданий, помещений и продукции организации.	1	
	3.	Разработка инструкций по организации охраны предприятия.	1	
	<b>Самостоятельная работа</b>		<b>9</b>	
	1.	Подготовить сообщение на темы: 1. Требования, связанные с размещением защищаемой информации. 2. Требования, обусловленные видом защищаемой информации. 3. Анализ существующих методик определение требований к защите информации. 4. Оценка состояния безопасности ИС. 5. Методы защиты информации. 6. Средства защиты информации. 7. Требования к криптосистемам. Основные алгоритмы шифрования. 8. Цифровые подписи. Криптографические хеш-функции. 9. Криптографические генераторы случайных чисел. 10. Криптоанализ и атаки на криптосистемы. 11. Требования к архитектуре СЗИ. Построение СЗИ.	9	
	<b>Тема 4.2.</b> Физическая	<b>Содержание учебного материала</b>	<b>6</b>	

защита предприятия	1.	Основные составляющие системы физической защиты предприятия. Особенности проектирования системы физической защиты предприятия.	1	3	
	2.	Деятельность структурных подразделений службы безопасности предприятия.	1	3	
	3.	Основные задачи инженерно-технической системы защиты информации. Разрешительная система доступа к конфиденциальной информации.	2	3	
	4.	Принцип действия аппаратуры систем контроля доступа.	2	3	
	<b>Практические занятия</b>			<b>6</b>	
	1.	Изучение работы аппаратуры систем контроля доступа.	1		
	2.	Выделение зон доступа по типу и степени конфиденциальностью работ.	1		
	3.	Классификация принципов инженерно-технической систем защиты информации.	1		
	4.	Классификация методов инженерно-технической системы защиты информации.	1		
	5.	Права, обязанности и ответственность сотрудников службы безопасности предприятия.	1		
	6.	Нештатные структуры службы безопасности предприятия.	1		
	<b>Самостоятельная работа</b>			<b>3</b>	
	1.	Подготовить сообщения на темы: 1. Требования, связанные с размещением защищаемой информации. 2. Требования, обусловленные видом защищаемой информации. 3. Анализ существующих методик определение требований к защите информации. 4. Оценка состоянии безопасности ИС. 5. Методы защиты информации.	3		
<b>Тема 4.3.</b>	<b>Содержание учебного материала</b>		<b>5</b>		
Инженерно-технические средства	1.	Виды технической средств физической защиты. Принципы построения и функционирования биометрических систем безопасности.	1	3	

физической защиты	2.	Требования и особенности оборудования режимных помещений.	1	3	
	3.	Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров. Требования режима защиты информации при приеме в организации посетителей.	1	3	
	4.	Организация работы при осуществлении международного сотрудничества.	1	3	
	5.	Требования режима защиты информации в процессе рекламной деятельности. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.	1	3	
	<b>Практические занятия</b>			<b>10</b>	
	1.	Определение порядка организации и проведения рабочих совещаний.	1		
	2.	Использование методов защиты информации в рекламной и выставочной деятельности.	1		
	3.	Средства контроля доступа на территорию объекта.	2		
	4.	Основные принципы организации и применения средств контроля доступа и средств охранной сигнализации.	2		
	5.	Система наблюдения за охраняемыми объектами.	2		
	6.	Изучение принципов действия физических барьеров.	2		
	<b>Самостоятельная работа</b>			<b>4</b>	
	1.	Подготовить сообщение на темы: 1. Требования, связанные с размещением защищаемой информации. 2. Требования, обусловленные видом защищаемой информации. 3. Анализ существующих методик определение требований к защите информации. 4. Оценка состояния безопасности ИС. 5. Методы защиты информации. 6. Средства защиты информации.	4		

	7. Требования к криптосистемам. Основные алгоритмы шифрования. 8. Цифровые подписи. Криптографические хеш-функции.		
<b>Обязательная аудиторная учебная нагрузка по курсовой работе ПМ.01 «Участие в планирование и организации работ по обеспечению защиты объекта»</b>		<b>22</b>	
1.	Общая характеристика курсовой работы	1	
2.	Постановка задачи курсовой работы	1	
3.	Подбор и анализ литературных источников. Интернет поиск	1	
4.	Анализ системы информационной безопасности на предприятии	1	
5.	Характеристика предприятия	1	
6.	Организационная структура предприятия	1	
7.	Характеристика информационных ресурсов предприятия	1	
8.	Меры, методы и средства защиты, применяемые на предприятии	1	
9.	Совершенствование системы информационной безопасности предприятия	1	
10.	Выявление недостатков в системе защиты информации	1	
11.	Цели и задачи формирования системы информационной безопасности на предприятии	1	
12.	Предлагаемые мероприятия по улучшению системы информационной безопасности предприятия	1	
13.	Эффективность предложенных мероприятий	1	
14.	Модель информационной безопасности	1	



15. Аудит информационной безопасности предприятия	1	
16. Угрозы и уязвимости информационной безопасности предприятия	1	
17. Определение экспертной группы информационной безопасности предприятия. Расчет коэффициентов авторитета экспертов информационной безопасности	1	
18. Перечень защищаемых информационных ресурсов. Составление списка элементов информационной системы защиты информации и расчет их стоимости	1	
19. Выводы проведенного аудита информационной безопасности. Мера для повышения экономической эффективности информационной системы	2	
20. Защита курсовой работы	2	
<b>Рабочая тематика курсовых работ ПМ.01 «Участие и планирование и организация работ по обеспечению защиты объекта»</b>		
Анализ и совершенствование системы информационной безопасности на предприятии МОБУ СОШ № 3 г. Якутск.		
Анализ и совершенствование системы информационной безопасности на предприятии МОБУ СОШ № 1 г. Якутск		
Совершенствование системы информационной безопасности на предприятии ПАО «Сбербанк» г. Якутск		
Совершенствование системы информационной безопасности на предприятии АКБ «Алмазэргиэнбанк» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ПАО «Мегафон» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ГАУ «Технопарк» г. Якутск		
Совершенствование системы информационной безопасности на предприятии АНО «Редакционная Группа «Якутск Вечерний» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ООО «Якутскэкосети» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ОАО «МТС» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ОАО «ВТБ» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ООО «Якутиндустрия» г. Якутск		
Совершенствование системы информационной безопасности на предприятии ООО «Якутгазпроект» г. Якутск		

Совершенствование системы информационной безопасности на предприятии ОАО «ЯТЭК» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ООО «Евросеть» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ПАО «Якутскэнерго» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Лукойл» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутдорсторой» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутская птицефабрика» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ООО «Яндекс» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутоптторг» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Газпром» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутскгеофизика» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутагропромпроект» г. Якутск				
Совершенствование системы информационной безопасности на предприятии ОАО «Якутский Хлебокомбинат» г. Якутск				
<b>МДК.1.2 Организация работ подразделений защиты информации</b>			66	
<b>Раздел 1. Место и роль службы защиты информации в системе защиты информации</b>			<b>17</b>	
<b>Тема 1.1.</b> Место и роль службы защиты информации в системе защиты информации	<b>Содержание учебного материала</b>		<b>3</b>	
	1.	Назначение службы защиты информации.	1	3
	2.	Место службы защиты информации как составляющая часть системы защиты информации.	1	3
	3	Служба защиты информации как составляющая часть системы защиты информации.	1	3
	<b>Практические занятия</b>		<b>4</b>	
1.	Служба защиты информации как орган управления защитой информации.	1		

	2.	Статус службы защиты информации в структуре безопасности предприятия.	2	
	3.	Разработка организационно-правовых аспектов деятельности службы защиты информации.	1	
	<b>Самостоятельная работа</b>		<b>3</b>	
	1.	Подготовить сообщения на темы: Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации.	3	
<b>Тема 1.2.</b> Задачи, функции и структура подразделений защиты информации	<b>Содержание учебного материала</b>		<b>3</b>	
	1.	Задачи, функции и структура подразделений защиты информации.	1	3
	2.	Общая структура схема службы защиты информации. Подразделений службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации.	1	3
	3.	Место и роль службы защиты информации в системе защиты информации. Задачи и функции службы защиты информации. Структуры и штаты службы защиты информации.	1	3
	<b>Практические занятия</b>		<b>1</b>	
	1.	Разработка организационной структуры службы защиты информации.	1	
	<b>Самостоятельная работа</b>		<b>3</b>	
	1.	Подготовить сообщения на темы: Виды и типы организационных структур службы защиты информации. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ.	3	
	<b>Раздел 2. Принципы деятельности службы защиты информации</b>		<b>22</b>	
<b>Тема 2.1.</b> Принципы и методы управления службой защиты информации	<b>Содержание учебного материала</b>		<b>6</b>	
	1.	Принципы и методы и технологии управления службой подразделений защиты информации. Принципы управления службой защиты информации.	2	3
	2.	Система методов управления. Взаимосвязь методов управления.	2	3
	3.	Необходимость комплексного и системного применения методов управления службой защиты информации.	2	3

	<b>Самостоятельная работа</b>	<b>3</b>	
	1. Подготовить сообщения на темы: Организация труда сотрудников службы защиты информации. Организационные основы и принципы деятельности службы защиты информации.	3	
<b>Тема 2.2.</b> Организационные основы и принципы деятельности службы защиты информации	<b>Содержание учебного материала</b>	<b>6</b>	
	1. Порядок создания службы защиты информации.	2	3
	2. Структура и содержания положения о службе защиты информации.	2	3
	3. Основные принципы организации и деятельности службы защиты информации.	2	3
	<b>Практические занятия</b>	<b>4</b>	
	1. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации.	2	
	2. Экспертная оценка мероприятий по защите информации в службе защиты информации.	2	
	<b>Самостоятельная работа</b>	<b>3</b>	
	Подготовить сообщения на темы: Оценка производительности труда по результатам оптимизации процессов в службе защиты информации. Принципы и методы управления службой защиты информации.	3	
<b>Раздел 3. Подбор, расстановка и обучение сотрудников службы защиты информации</b>		<b>25</b>	
<b>Тема 3.1.</b> Подбор, расстановка и обучение сотрудников службы защиты информации.	<b>Содержание учебного материала</b>	<b>2</b>	
	1. Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации	2	3
	<b>Практические занятия</b>	<b>3</b>	
	1. Критерии подбора и расстановки сотрудников подразделений защиты информации.	1	
	2. Состав и характеристика процесса проектирования деятельности службы защиты информации.	1	
	3. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.	1	
	<b>Самостоятельная работа</b>	<b>3</b>	
	1. Подготовить сообщения на темы:	3	

		Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров.		
<b>Тема 3.2.</b> Организация труда сотрудников службы защиты информации	<b>Содержание учебного материала</b>		<b>2</b>	
	1.	Специфика деятельности сотрудников службы защиты информации.	2	3
	<b>Практические занятия</b>		<b>6</b>	
	1.	Организации рабочих мест сотрудников службы защиты информации.	2	
	2.	Структура и содержание должностных инструкций сотрудников службы защиты информации.	2	
	3.	Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации.	2	
	<b>Самостоятельная работа</b>		<b>3</b>	
1.	Подготовить сообщения на темы: Методы получения информации о кандидатурах на должности. Распределение обязанностей между сотрудниками службы защиты информации.	3		
<b>Тема 3.3.</b> Технология управления службой защиты информации	<b>Практические занятия</b>		<b>4</b>	
	1.	Технологии управления службой защиты информации.	2	
	2.	Значение управленческих решений.	2	
	<b>Самостоятельная работа</b>		<b>4</b>	
1.	Подготовить сообщения на темы: Методы организационного проектирования деятельности службы защиты информации.	4		
<b>МДК.1.3 Организация работы персонала с конфиденциальной информацией</b>			66	
<b>Раздел 1. Особенности организации работ с конфиденциальными документами</b>			33	
<b>Тема 1.1.</b> Понятие о конфиденциальных документах	<b>Содержание учебного материала</b>		<b>5</b>	3
	1.	Общие положения. Классификация информации и документов по категориям доступа.	1	
	2.	Понятие ценной и конфиденциальной информации. Перечень сведений конфиденциального характера.	1	3
	3.	Представление и распространение информации. Персональные данные	1	3

	4.	Тайна следствия и судопроизводство. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Ноу-хау.	1	3
	5.	Нормативная база конфиденциального делопроизводства.	1	3
	<b>Практические занятия</b>		<b>6</b>	
	1.	Обработка персональных данных без использования средств информатизации.	2	
	2.	Нормативно-правовая база организации работы с конфиденциальными документами.	2	
	3.	Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация.	2	
	<b>Самостоятельная работа</b>		<b>5</b>	
	1.	Написать сообщение на темы: 1. Законы РФ «О коммерческой тайне», «Об информации, информатизации и защите информации», «О персональных данных». 2. Нормативно-методическая база организации работы с документами, содержащими служебную тайну. 3. Сущность и принципы ограничения доступа к информации и документам. 4. Нормативно-правовые основы организации работы с документами, содержащими коммерческую тайну.	5	
<b>Тема</b>	<b>1.2.</b>	<b>Содержание учебного материала</b>	<b>8</b>	
Особенности работы с конфиденциальной информацией	1.	Особенности документирование конфиденциальной информации. Оформление реквизитов конфиденциальных документов при документации информации.	2	3
	2.	Ограничение доступа к документам и использование отметки конфиденциальности при оформлении документов. Порядок оформления допуска лиц к конфиденциальным сведениям.	2	3
	3.	Перечень конфиденциальной информации.	2	3
	4.	Основные этапы разработки перечня конфиденциальной документированной информации.	2	3
	<b>Практические занятия</b>		<b>4</b>	
	1.	Разработка перечня документированной конфиденциальной информации.	1	
	2.	Определение степени разграничения доступа к документами использование отметки конфиденциальности при оформлении документов.	1	

	3.	Учет и регистрация внутренних конфиденциальных документов.	1	
	4.	Исполнение и контроль над исполнением конфиденциальных документов.	1	
	<b>Самостоятельная работа</b>		<b>5</b>	
	1.	Написать сообщение на темы: 1. Создание и изготовление конфиденциальных документов с помощью ЭВМ их печатания \, тиражирования и размножение. 2. Учет использования и хранение печатей, штампов, бланков, необходимых для оформления документов. 3. Понятие «внутри объектовый режим». Его основное назначение при ведении конфиденциальных работ и обращении с охраняемыми изделиями и документами. 4. Порядок определения перечня предметов, запрещенных к проносу провозу на режимную территорию. Общие требования внутри объектового режима.	5	
<b>Раздел 2. Особенности организации работ персонала с конфиденциальными документами</b>			<b>33</b>	
<b>Тема 2.1.</b> Текущая работа с персоналом, обладающий конфиденциальной	<b>Содержание учебного материала</b>		<b>3</b>	
	1.	Профессиональная ориентация и обучение персонала. Методы проверки персонала по защите информации.	1	3
	2.	Мотивация персонала выполнению требований по защите информации.	1	3
	3.	Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.	1	3
	<b>Практические занятия</b>		<b>6</b>	
	1.	Организация работы с персоналом, имеющим доступ к конфиденциальной информации.	2	
	2.	Проведение инструктажа персонала по организации работы с конфиденциальной информацией.	2	
	3.	Контроль соблюдения персоналом требований режима защиты информации.	2	
	<b>Самостоятельная работа</b>		<b>5</b>	
	1.	Написать сообщение на темы: 1. Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальной информацией. 2. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта.	5	

		3. Порядок допуска работников в помещения, где ведутся конфиденциальные работы.		
<b>Тема 2.2.</b> Подготовка и проведение совещаний и переговоров по конфиденциальным вопросам	<b>Содержание учебного материала</b>		<b>6</b>	
	1.	Основные требования, предъявляемые к подготовке и проведению совещаний и переговорам по конфиденциальным вопросам.	1	3
	2.	Порядок назначения ответственных лиц и их обязанности по проведению совещаний и переговоров.	1	3
	3.	Подбор персонала на должности, связанные с работой с конфиденциальной информацией.	1	3
	<b>Практические занятия</b>		<b>6</b>	
	1.	Организация защиты информации при осуществлении рекламной и публицистической деятельности.	2	
	2.	Организация защиты информации при подготовке материалов к открытому опубликованию.	2	
	3.	Аналитическая работа как основа управления системой организационной защиты информации.	2	
	<b>Самостоятельная работа</b>		<b>7</b>	
	1.	Написать сообщение на темы: 1. Организация работы по защите информации при осуществлении публицистической деятельности и связей с прессой; участие ней Службы безопасности. 2. Организация контроля за выполнения распорядка дня лицами, работающими на режимных объектах. 3. Создание отдельных (вычислительных) производительных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организациями и контроля доступа.	7	
<b>ПП.1.01 Производственная практика (по профилю специальности)</b>				
<b>Виды работ:</b> 1. Использование физических средств защиты объекта. 2. Применение физических средств контроля доступа на объекта. 3. Ведение текущей работы исполнительней с конфиденциальными документами.			36	
<b>УП 1.01 Учебная практика</b>				
<b>Виды работ:</b> Получение информации из открытых источников:			36	



1.	Использование Google для сбора информации;		
2.	Поиск информации о людях;		
3.	Получение информации о домене;		
4.	Автоматизирование процесса;		
5.	Упорядочение информации.		
<b>Всего:</b>		249	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1 - ознакомительный (узнавание ранее изученных объектов, свойств);
- 2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
- 3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 4.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Реализация учебной дисциплины требует наличия учебного кабинета информатики.

#### Оборудование учебного кабинета математики:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методической документации.

#### Технические средства обучения:

- персональный компьютер;
- проекционный экран;
- мультимедийный проектор;
- доска;
- колонки.

### 4.2. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы.

#### Основные источники:

1. Кубашева, Е.С. Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: Е.С. Кубашева, И.А. Малашкевич, Е.Н. Чекулаева; Поволжский государственный технологический университет. – Йошкар-Ола: ПГТУ, 2019. – 66 с.: (<http://biblioclub.ru/index.php?page=book&id=562246>)

2. Информационная безопасность: учеб./ под ред. В.П. Мельникова. - М.: Кнорус, 2018. –Рек. ФИРО

3. Вычислительная техника: Уч.пос. / Т.Л. Партыка – 3-е изд. - М.: Форум, НИЦ ИНФРА-М, 2018. – 445 с. - (Профессиональное образование)

#### Дополнительная литература

1. Родичев Юрий Андреевич. Нормативная база и стандарты в области информационной безопасности. М.: Питер. Серия: учебник для вузов. 2017 г. -256 с.

2. С.А. Нестеров. Основы информационной безопасности. М.: Лань. Серия: учебник для вузов. Специальная литература. 2017 г. -324 с.

3. В.В. Бондарь. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана. 2017 г. -252 с.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2017. – 416 с.: ил. - (Профессиональное образование). – Рек. МО

#### Интернет источники:

1. Системы безопасности предприятия. [https://studopedia.ru/18\\_46205\\_sistema-bezopasnosti-predpriyatiya.html](https://studopedia.ru/18_46205_sistema-bezopasnosti-predpriyatiya.html)

2. Система безопасности. <http://datasolution.ru/sistema-bezopasnosti-predpriyatiya-2>

3. Обеспечение организации системы безопасности предприятия. <https://itforever.jimdo.com>

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения дисциплины является формирования у студентов четкого представления о планировании и организации работ по обеспечению защиты объекта.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результат	Формы и методы контроля и оценки
ПК 1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	<ul style="list-style-type: none"> <li>- определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации.</li> <li>-выполнение анализа научной литературы;</li> <li>- обоснование выбора соответствующих решений по защите информации объекта;</li> <li>- обоснование использованных методов обнаружения технических каналов утечки информации.</li> </ul>	Текущий контроль: -ситуационные задачи, -практические работы, -самостоятельная работа, -защита работ на различных этапах производственной практики.
ПК 1.2 Участвовать в разработке программ и методик организации защиты информации на объекте.	<ul style="list-style-type: none"> <li>-определение предложений по разработке программ защиты информации на объекте;</li> <li>-определение методик защиты информации на предприятии.</li> </ul>	Текущий контроль: -ситуационные задачи, -практические работы, -самостоятельная работа, -защита работ на различных этапах производственной практики.
ПК 1.3 Осуществлять планирование и организацию выполнения мероприятий по защите информации.	<ul style="list-style-type: none"> <li>-выполнение работ по защите конфиденциальной информацией;</li> <li>- определение качества защиты информации;</li> <li>-выполнение мероприятий по комплексной защите информации.</li> </ul>	Текущий контроль: -ситуационные задачи, -практические работы, -самостоятельная работа, -защита работ на различных этапах производственной практики.
ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.	<ul style="list-style-type: none"> <li>-обоснование выбранных организационных решений на объектах информатизации;</li> <li>- обоснование мер по внедрению организационных решений на предприятии.</li> </ul>	Текущий контроль: -ситуационные задачи, -практические работы, -самостоятельная работа, -защита работ на различных этапах производственной практики.
ПК 1.5 Вести учет,	-обоснование	Текущий контроль:

<p>обработку, хранение, передачу, использование различных носителей конфиденциальной информации.</p>	<p>использования носителей конфиденциальной информации;          -определение методики обработки и хранения защищаемой информации;          -организация выполнения передачи конфиденциальной информации на различных носителях;          -полнота и эффективность соблюдения правил использования носителей секретной информации.</p>	<p>-ситуационные задачи,          -практические работы,          -самостоятельная работа,          -защита работ на различных этапах производственной практики.</p>
<p>ПК 1.6 Обеспечить технику безопасности при проведении организационно-технических мероприятий.</p>	<p>-определение правил техники безопасности при комплексной защите информации;          -определение методики защиты информации при проведении организационно-технических мероприятий.</p>	<p>Текущий контроль:          -ситуационные задачи,          -практические работы,          -самостоятельная работа,          -защита работ на различных этапах производственной практики.</p>
<p>ПК 1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.</p>	<p>-обоснование выбранных методов проверок организаций, информации которых подлежит защите;          -проведение проверки объектов информатизации;          -проведение проверки организаций, работающих с конфиденциальной информацией.</p>	<p>Текущий контроль:          -ситуационные задачи,          -практические работы,          -самостоятельная работа,          -защита работ на различных этапах производственной практики.</p>
<p>ПК 1.8 Проводить контроль соблюдения персоналом требований режима защиты информации.</p>	<p>-определение методов и способов контроля персонала, работающего с конфиденциальной информацией;          -определение последовательности действий при проведении проверок соблюдения требований персонала режима защиты информации;          -организации проведения контроля за работой персонала, задействованного в защите информации организации.</p>	<p>Текущий контроль:          -ситуационные задачи,          -практические работы,          -самостоятельная работа,          -защита работ на различных этапах производственной практики.</p>

ПК 1.9 Участвовать в оценке качества защиты объекта.	- выполнение оценки качества комплексной защиты информации организации; -выполнение оценки качества защиты объекта информатизации; Определение и анализ недостатков качества защиты информации на предприятии.	Текущий контроль: -ситуационные задачи, -практические работы, -самостоятельная работа, -защита работ на различных этапах производственной практики.
------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только форсированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умения.

<b>Результаты (освоенные общие компетенции)</b>	<b>Основные показания оценки результата</b>	<b>Формы и методы контроля и оценки</b>
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	- демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам.	-тестирование, -практические работы, - самостоятельная работа, -защита работ на различных этапах производственной практики.
ОК 2. Организовать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в организации и технологии защиты информации; -оценка эффективности и качества выполнения работ.	
ОК 3.Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач.	
ОК4.Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и	-эффективный поиск необходимой информации; -использование различных источников, включая электронные.	

личностного развития.		
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- использование программ автоматизации профессиональной деятельности (владеть навыками работы в специальных программах, а также текстовые и табличные редакторах, программах по созданию презентации).	
ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	-взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения	<ul style="list-style-type: none"> <li>-тестирование,</li> <li>-практические работы,</li> <li>- самостоятельная работа,</li> <li>-защита работ на различных этапах производственной практики.</li> </ul>
ОК 7. Брать на себя ответственность за работу членов команды (починных), за результат выполнения заданий.	-самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассных мероприятиях.	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	-организация самостоятельных занятий при изучении профессионального модуля.	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	-анализ инноваций в области защиты информации.	
ОК 10. Применять математический аппарат для решений различных задач.	- демонстрация готовности к исполнению воинской обязанности.	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	- уметь применять средства математической логики для решения задач.	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	- уметь оценивать документы, используемые в области защиты информации.	

