**ФЕДЕРАЛЬНОЕ УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЪЕДИНЕНИЕ**

**В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ ПО УКРУПНЕННОЙ ГРУППЕ СПЕЦИАЛЬНОСТЕЙ И НАПРАВЛЕНИЙ ПОДГОТОВКИ**

**10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**



УТВЕРЖДАЮ

Председатель ФУМО ВО ИБ

А.Б. Пичкур

30 ноября 2021 г.

**Методические рекомендации**

**по разработке основной профессиональной образовательной программы   
высшего образования**

Направление подготовки

**Информационная безопасность**

Уровень высшего образования

**Бакалавриат**

Профиль № 3

**Техническая защита информации**

Москва, 2021 г.СОДЕРЖАНИЕ

Раздел 1. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ ПО ПРОФИЛЮ

1.1. Описание профессиональной деятельности выпускников

1.2. Перечень профессиональных стандартов, соотнесенных с программой по профилю

1.3. Перечень основных задач профессиональной деятельности выпускников по профилю

Раздел 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ В ЧАСТИ ПРОФИЛЯ

2.1. Перечень обязательных компетенций выпускников по профилю

2.2. Индикаторы достижения компетенций по профилю

Раздел 3. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ОПОП В ЧАСТИ ПРОФИЛЯ

3.1. Примерный учебный план в части профиля

3.2. Примерные программы дисциплин (модулей) в части профиля

Раздел 4. СПИСОК РАЗРАБОТЧИКОВ

Приложение 1. Перечень профессиональных стандартов, соотнесенных с программой по профилю № 3 «Техническая защита информации» ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность»

Приложение 2. Перечень обобщенных трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ бакалавриата по профилю № 3 «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность»

# Раздел 1. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ ПО ПРОФИЛЮ

***№ 3 Техническая защита информации***

## 1.1. Описание профессиональной деятельности выпускников

Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата по профилю (далее – выпускники), могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере защиты информации от утечки по техническим каналам и несанкционированного доступа);

12 Обеспечение безопасности (в сфере эксплуатации технических средств защиты информации);

сфера правоохранительной деятельности.

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

Типы задач профессиональной деятельности выпускников:

эксплуатационный;

проектно-технологический;

экспериментально-исследовательский.

При разработке и реализации программы бакалавриата Организация ориентируется на все типы задач профессиональной деятельности, к которым готовится бакалавр.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников по профилю № 3 «Техническая защита информации»:

- средства и технологии обеспечения информационной безопасности и защиты информации;

- экспертиза, сертификация и контроль защищенности информации и объектов информатизации;

- методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации.

## 1.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО и профилем № 3 «Техническая защита информации»

Перечень профессиональных стандартов, соотнесенных с ФГОС ВО и профилем № 3 «Техническая защита информации», приведен в приложении 1.

Перечень обобщенных трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ бакалавриата по профилю № 3 «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность», представлен в приложении 2.

## 1.3. Перечень основных задач профессиональной деятельности выпускников по профилю № 3 «Техническая защита информации»

Соотнесение областей, типов задач и конкретных трудовых функций (обобщенных трудовых функций) профильного и смежных профессиональных стандартов, имеющих отношение к профессиональной деятельности выпускника по профилю № 3 «Техническая защита информации» приведены в таблице 1.

Таблица 1.

Соотнесение областей, типов задач и конкретных трудовых функций (обобщенных трудовых функций) профессиональных стандартов

|  |  |  |
| --- | --- | --- |
| Область профессиональной деятельности  (по Реестру Минтруда) | Типы задач  профессиональной  деятельности | Коды трудовых функций (задачи профессиональной деятельности) профильного профессионального стандарта 06.034 «Специалист по технической защите информации» |
| *06 Связь, информационные и коммуникационные технологии (в сфере защиты информации от утечки по техническим каналам и несанкционированного доступа)* | *эксплуатационный* | 06.034 «Специалист по технической защите информации»:  B/02.6 Проведение работ по техническому обслуживанию защищенных технических средств обработки информации |
| *проектно-технологический* | 06.034 «Специалист по технической защите информации»:  B/01.6 Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации. |
| *экспериментально-исследовательский* | 06.034 «Специалист по технической защите информации»:  D/01.6 Проведение специальных исследований на ПЭМИН технических средств обработки информации;  D/02.6 Проведение контроля эффективности защиты информации от утечки за счет ПЭМИН;  D/03.6 Проведение контроля эффективности защиты акустической (речевой) информации от утечки по техническим каналам;  D/04.6 Проведение контроля защищенности информации от несанкционированного доступа |

**Раздел 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ В ЧАСТИ ПРОФИЛЯ**

**2.1. Перечень компетенций выпускников по профилю**

Перечень общепрофессиональных компетенций:

ОПК-3.1. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам;

ОПК-3.2. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа;

ОПК-3.3. Способен проводить контроль эффективности защиты информации от утечки по техническим каналам;

ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа.

**2.2. Индикаторы достижения компетенций выпускников по профилю**

Перечень индикаторов достижения общепрофессиональных компетенций выпускников, соотнесенных с компетенциями профиля № 3 «Техническая защита информации», приведен в таблице 2.

Таблица 2

**Общепрофессиональные компетенции выпускников и индикаторы их достижения**

**по профилю № 3 «Техническая защита информации»**

**направления подготовки 10.03.01 «Информационная безопасность»**

| **Код и наименование компетенции** | **Код**  **индикатора** | **Индикаторы достижения общепрофессиональных компетенций профиля** | **Наименование учебной дисциплины (модуля), формирующие ОПК по примерному учебному плану** | **Код ПС,**  **код ОТФ, ТФ,**  **(при наличии)** |
| --- | --- | --- | --- | --- |
| **Общепрофессиональные компетенции (ОПК)** **по профилю № 3 «Техническая защита информации»** | | | | |
| **ОПК-3.1. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам** | ОПК-3.1.1.1 | знает основные положения электротехники, электроники и схемотехники для решения профессиональных задач | Основы радиотехники | ПС 06.034, ОТФ B, ТФ B/01.6, B/02.6 |
| ОПК-3.1.1.2 | знает принципы работы современной радиоэлектронной аппаратуры и физические процессы, протекающие в них |
| ОПК-3.1.1.3 | знает элементную базу, основные структуры и методы расчета устройств передачи, приема и обработки сигналов |
| ОПК-3.1.1.4 | знает методы разработки и моделирования радиотехнических узлов аппаратно-программных комплексов защиты информации, с использованием современных инструментальных и программных средств |
| ОПК-3.1.2.1 | умеет решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам |
| ОПК-3.1.2.2 | умеет моделировать, тестировать, испытывать и использовать аппаратные средства вычислительных систем и информационных систем для решения профессиональных задач |
| ОПК-3.1.3.1 | владеет навыками работы с радиотехническим оборудованием и программным обеспечением, а также с документацией по радиотехнике |
| ОПК-3.1.1.5 | знает основы построения и функционирования генераторов шума систем пространственного электромагнитного зашумления | Основы построения и функционирования специальных технических средств |
| ОПК-3.1.1.6 | знает основы построения и функционирования генераторов шума систем виброакустической маскировки |
| ОПК-3.1.2.3 | умеет проектировать и исследовать характеристики высокочастотных и низкочастотных генераторов шума |
| ОПК-3.1.1.7 | знает классификацию, основные этапы эксплуатации, технического обслуживания средств защиты информации (СЗИ) от утечки по техническим каналам | Основы эксплуатации систем защиты объектов информатизации |
| ОПК-3.1.2.4 | умеет разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СЗИ от утечки по техническим каналам |
| **ОПК-3.2. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа** | ОПК-3.2.1.1 | знает основные понятия, функции, состав, принципы работы, архитектуру операционной системы специального назначения | Информационные технологии. Операционные системы специального назначения | ПС 06.034, ОТФ B, ТФ B/01.6, B/02.6 |
| ОПК-3.2.1.2 | знает принципы управления ресурсами в операционной системе специального назначения |
| ОПК-3.2.2.1 | умеет устанавливать и конфигурировать современные операционные системы специального назначения |
| ОПК-3.2.1.3 | знает способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах | Защита информации от несанкционированного доступа |
| ОПК-3.2.1.4 | знает классификацию и общую характеристику уязвимостей и угроз несанкционированного доступа к информации в автоматизированной системе |
| ОПК-3.2.2.2 | умеет применять современные технологии управления доступом, аутентификации и идентификации для обеспечения безопасности автоматизированных систем |
| ОПК-3.2.1.5 | знает классификацию, основные этапы эксплуатации, технического обслуживания средств защиты информации (СЗИ) от несанкционированного доступа | Основы эксплуатации систем защиты объектов информатизации |
| ОПК-3.2.2.3 | умеет разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СЗИ от несанкционированного доступа |
| **ОПК-3.3. Способен проводить контроль эффективности защиты информации от утечки по техническим каналам** | ОПК-3.3.1.1 | знает основные понятия и определения метрологии, стандартизации, сертификации | Метрология, стандартизация и сертификация | ПС 06.034, ОТФ D, ТФ D/01.6, D/02.6, D/03.6 |
| ОПК-3.3.1.2 | знает методы измерения физических величин |
| ОПК-3.3.1.3 | знает принципы построения и работы измерительных устройств и приборов |  |
| ОПК-3.3.2.1 | умеет применять средства измерений различных физических величин, осуществлять выбор средств измерений по заданным метрологическим характеристикам |  |
|  | ОПК-3.3.2.2 | умеет обрабатывать данные и рассчитывать погрешности измерений при решении профессиональных задач |  |
|  | ОПК-3.3.3.1 | владеет методами оценивания погрешностей с применением современных информационных технологий |  |
|  | ОПК-3.3.1.4 | знает основы построения и функционирования средств радиоразведки | Основы построения и функционирования специальных технических средств |  |
|  | ОПК-3.3.1.5 | знает основы построения и функционирования средств акустической речевой разведки |  |
|  | ОПК-3.3.1.6 | знает основы построения и функционирования средств визуально-оптической и оптико-электронной разведки |  |
|  | ОПК-3.3.2.3 | умеет исследовать характеристики модулей (элементов) специальных радиоприемных устройств, средств акустической речевой, визуально-оптической и оптико-электронной разведок |  |
|  | ОПК-3.3.3.2 | владеет навыками проектирования и исследования характеристик модулей (элементов) специальных технических средств |  |
|  | ОПК-3.3.1.7 | знает классификацию, основные этапы эксплуатации, технического обслуживания средств контроля эффективности защиты информации (СКЭЗИ) от утечки по техническим каналам | Основы эксплуатации систем защиты объектов информатизации |  |
|  | ОПК-3.3.2.4 | разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СКЭЗИ от утечки по техническим каналам |  |
| **ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа** | ОПК-3.4.1.1 | знает виды и методы контроля и испытаний, методику их проведения и сопроводительную документацию | Метрология, стандартизация и сертификация | ПС 06.034, ОТФ D, ТФ D/04.6 |
| ОПК-3.4.1.2 | знает порядок проведения стандартных и сертифицированных испытаний средств защиты информации |  |
| ОПК-3.4.2.1 | умеет применять соответствующие методики контроля, испытаний и диагностики средств защиты информации |  |
|  | ОПК-3.4.1.3 | знает основные задачи администрирования и способы их выполнения в операционной системе специального назначения | Информационные технологии. Операционные системы специального назначения |  |
|  | ОПК-3.4.1.4 | знает модель управления доступом и информационными потоками в операционной системе специального назначения |  |
|  | ОПК-3.4.2.2 | умеет анализировать степень защищенности данных и ресурсов, определять политику безопасности и настраивать системы контроля доступа в операционных системах специального назначения |  |
|  | ОПК-3.4.1.5 | знает типовые средства для инструментальной оценки уровня защищённости автоматизированных систем | Защита информации от несанкционированного доступа |  |
|  | ОПК-3.4.2.3 | умеет проводить анализ защищенности информации от несанкционированного доступа в автоматизированных системах |  |
|  | ОПК-3.4.1.6 | знает классификацию, основные этапы эксплуатации, технического обслуживания средств контроля эффективности защиты информации (СКЭЗИ) от несанкционированного доступа | Основы эксплуатации систем защиты объектов информатизации |  |
|  | ОПК-3.4.2.4 | умеет разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СКЭЗИ от несанкционированного доступа |  |

# Раздел 3. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ПООП В ЧАСТИ ПРОФИЛЯ

**3.1. Примерный учебный план в части профиля**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Индекс | Наименование дисциплин (модулей), практик, аттестационных испытаний | Формы промежуточной аттестации | Трудоемкость | | | Коды форми-руемых компетенций |
| з.е. | часы | |
| всего | контакт-ная работа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Б.1** | **Блок 1. Дисциплины (модули)** |  | **Не менее 201** | **Не менее 7564** | **Не менее 3782** |  |
| **Б.1.О** | **Обязательная часть** |  | **Не менее 150** |  |  |  |
|  | **Дисциплины (модули) профиля** |  | **Не менее**  **27** | **Не менее 972** | **Не менее 420** |  |
|  | *3. Техническая защита информации* |  |  |  |  |  |
| **Б.1.П.3.1.** | Основы радиотехники | зачет | 4 | 144 |  | ОПК-3.1 |
| **Б.1.П.3.2.** | Метрология, стандартизация и сертификация | экзамен | 4 | 144 |  | ОПК-3.3, ОПК-3.4 |
| **Б.1.П.3.3.** | Информационные технологии. Операционные системы специального назначения | экзамен | 5 | 180 |  | ОПК-3.2, ОПК-3.4 |
| **Б.1.П.3.4.** | Основы построения и функционирования специальных технических средств | экзамен | 6 | 216 |  | ОПК-3.1, ОПК-3.3 |
| **Б.1.П.3.5.** | Защита информации от несанкционированного доступа | экзамен | 5 | 180 |  | ОПК-3.2, ОПК-3.4 |
| **Б.1.П.3.6.** | Основы эксплуатации систем защиты объектов информатизации | зачет | 3 | 108 |  | ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-3.4 |
|  | Дисциплины (модули) образовательной организации  (при необходимости) |  |  |  |  |  |

Организация в пределах требований, установленных ФГОС ВО, при формировании программы бакалавриата в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе:

конкретизировать наименование;

увеличивать трудоемкость;

уменьшать трудоемкость не более чем на 2 з.е. при условии, что итоговая величина составит не менее 3 з.е.;

устанавливать периоды обучения, в которых изучается учебная дисциплина (модуль), а также формы промежуточной аттестации по их окончании;

разделять учебные дисциплины (модули) при условии сохранения общей трудоемкости и индикаторов достижения формируемых компетенций, установленных ПООП для исходной учебной дисциплины (модуля).

Федеральные государственные образовательные организации, находящиеся   
в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. «Об образовании в Российской Федерации», при формировании программы бакалавриата в целях реализации квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого они находятся, в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе: изменять наименование и трудоемкость в пределах требований, установленных ФГОС ВО.

**3.2. Примерные программы дисциплин (модулей) в части профиля**

### Б.1.П.3.1. Дисциплина «Основы радиотехники»

Коды формируемых компетенций: ОПК-3.1.

В результате изучения дисциплины студент должен

**знать:**

- основные положения электротехники, электроники и схемотехники для решения профессиональных задач;

- принципы работы современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;

- элементную базу, основные структуры и методы расчета устройств передачи, приема и обработки сигналов;

- методы разработки и моделирования радиотехнических узлов аппаратно-программных комплексов защиты информации, с использованием современных инструментальных и программных средств;

**уметь:**

- ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам;

- моделировать, тестировать, испытывать и использовать аппаратные средства вычислительных систем и информационных систем для решения профессиональных задач;

**владеть:**

- навыками работы с радиотехническим оборудованием и программным обеспечением, а также с документацией по радиотехнике.

**Общий объем времени** – 144 час., 4 з.е.

**Примерное распределение часов:** 70 часов контактная работа (из них 40 – лекции, 30 – практические занятия).

**Форма контроля:** зачет

**Содержание дисциплины:**

**Основные радиотехнические сигналы и их параметры.** Классификация сигналов. Гармонический сигнал. Импульсные сигналы. Спектральное представление сигнала. Дискретизация сигналов.

**Радиотехнические цепи.** Расчет цепей при стационарных режимах. Анализ переходных процессов в радиотехнических цепях.

**Электронные приборы и компоненты.** Полупроводниковые приборы. Полупроводниковые диоды. Транзисторы. Операционный усилитель. Жидкокристаллические индикаторы. Усилители. Принцип работы усилителя. Дифференциальный усилительный каскад. Усилители мощности. Избирательные четырехполюсники.

**Системы связи.** Принцип радиосвязи. Классификация диапазонов радиоволн. Понятие об излучении электромагнитных волн. Антенны систем радиосвязи. Элементы теории распространения радиоволн. Особенности системы радиосвязи.

**Общая характеристика систем передачи информации.** Качественные характеристики каналов и трактов связи. Структурная схема радиосвязи. Модуляция сигналов. Аналоговые системы радиосвязи. Импульсные системы радиосвязи. Основы теории кодирования. Многоканальные радиосистемы передачи информации. Методы уплотнения и разделения каналов. Цифровые многоканальные радиосистемы передачи информации. Системы связи подвижной службы. Телевизионные радиосистемы. Волоконно-оптические линии связи.

**Радиопередающие устройства.** Структурная схема радиопередатчика. Основные технические характеристики радиопередатчика. Возбудители радиопередатчиков. Автогенераторы. Синтезаторы частот. Формирование радиосигналов. Принципы построения усилительных трактов радиопередатчиков. Усилительные элементы и их режим работы.

**Радиоприемные устройства.** Основные характеристики и структурная схема радиоприёмника. Входные цепи радиоприёмников. Усилители радиочастоты. Преобразователи частоты. Усилители промежуточной частоты. Обработка радиосигналов в радиоприёмниках. Регулировки в радиоприёмниках.

**Рекомендуемый перечень основной литературы**:

1. Березовский П.П. Основы радиотехники и связи: учебное пособие. – Екатеринбург: Изд-во Урал. Ун-та, 2017;

# 2. Иванов М.Т., Сергиенко А.Б., Ушаков В.Н. Теоретические основы радиотехники: учебное пособие. - М.: Высшая школа, 2002;

3. Гуменюк А.Д., Журавлев В.И., Мартюшев Ю.Ю., Петрухин Г.Д. Основы электроники, радиотехники и связи. – М.: Горячая линия-Телеком, 2008;

4. Новожилов О.П. Электроника и схемотехника. В 2-х частях: учебник для академического бакалавриата. – М.: Юрайт, 2019.

**Перечень материально-технического обеспечения:**

1. Учебная лаборатория, оснащённая оборудованием: осциллографы универсальные, генераторы сигналов низкочастотные, генераторы сигналов высокочастотные, мультиметры, частотомеры электронно-счётные, лабораторные стенды с макетами;

2. Компьютерный класс с установленным САПР по схемотехническому моделированию (MentorGraphics, Orcad, MultiSim), Matlab.

**Б.1.П.3.2. Дисциплина «Метрология, стандартизация и сертификация»**

Коды формируемых компетенций: ОПК-3.3, ОПК-3.4.

В результате изучения дисциплины студент должен

**знать:**

- основные понятия и определения метрологии, стандартизации, сертификации;

- методы измерения физических величин (ОПК‑3.3);

- принципы построения и работы измерительных устройств и приборов;

- виды и методы контроля и испытаний, методику их проведения и сопроводительную документацию;

- порядок проведения стандартных и сертифицированных испытаний средств защиты информации;

**уметь:**

- применять средства измерений различных физических величин, осуществлять выбор средств измерений по заданным метрологическим характеристикам;

- обрабатывать данные и рассчитывать погрешности измерений при решении профессиональных задач;

- применять соответствующие методики контроля, испытаний и диагностики средств защиты информации;

**владеть:**

- методами оценивания погрешностей с применением современных информационных технологий.

**Общий объем времени** – 144 час., 4 з.е.

**Примерное распределение часов:** 70 часов контактная работа (из них 40 – лекции, 30 – практические занятия).

**Форма контроля:** экзамен

**Содержание дисциплины:**

**Основы метрологии.** Измерения физических величин. Эталоны единиц электрических величин. Воспроизведение и передача размеров физических величин. Классификация измерений и средств измерений. Основные характеристики измерений. Основные виды и методы измерений. Средства измерений и их классификация. Погрешности измерений. Классификация погрешностей. Систематические погрешности. Случайные погрешности. Описание и оценка результатов наблюдений. Метрологические характеристики средств измерений. Нормирование метрологических характеристик средств измерений. Классы точности средств измерений. Регулировка и градуировка средств измерений. Обработка результатов измерений: прямых однократных измерений, прямых многократных измерений, косвенных измерений, совместных и совокупных измерений. Формы представления результатов измерений. Погрешность и неопределенность результатов измерений.

**Измерительный эксперимент.** Планирование и организация эксперимента. Отличительные и ограничительные признаки измерительного эксперимента. Основные этапы физического эксперимента. Структурная модель и основные элементы измерительного эксперимента. Техника физического эксперимента по определению функциональной зависимости. Установление вида математической модели функциональной зависимости. Подбор аппроксимирующих функций. Расчет параметров аппроксимирующей функции. Методы моделирования измеряемых данных. Интерполяционные полиномы. Регрессионный анализ. Выбор вида математической модели многофакторных зависимостей. Методы измерения характеристик случайных процессов. Измерение математического ожидания. Измерение средней мощности и дисперсии. Измерение корреляционных функций и спектральных характеристик. Анализ распределения вероятностей.

**Организационно-правовые основы метрологической деятельности.** Государственная система обеспечения единства измерений. Состав и структура государственной системы обеспечения единства измерений. Нормативно-правовые основы обеспечения единства измерений. Метрологические службы и организации. Государственный метрологический надзор и контроль. Метрологическое обеспечение при разработке, производстве и эксплуатации технических устройств. Менеджмент измерений в системе качества.

**Основы стандартизации.** История развития стандартизации. Федеральный закон «О техническом регулировании». Сущность стандартизации. Основные принципы стандартизации. Документы в области стандартизации. Правовые основы стандартизации и ее задачи. Органы и службы по стандартизации. Порядок разработки стандартов. Государственный контроль и надзор за соблюдением обязательных требований стандартов. Маркировка продукции знаком соответствия государственным стандартам. Нормоконтроль технической документации. Единая система конструкторской документации (ЕСКД) Виды и комплектность конструкторской документации. Текстовые и графические документы, общие требования к их выполнению. Схемы. Основные функции стандартизации. Научно-методические основы стандартизации. Методы стандартизации.

**Основы сертификации.** Цели и задачи подтверждения соответствия. Понятие системы сертификации. Функции системы сертификации. Структура системы сертификации РФ. Формы подтверждения соответствия: обязательная сертификация, декларирование соответствия и добровольная сертификация. Участники обязательной сертификации, участники добровольной сертификации, участники декларирования соответствия. Системы сертификации. Законодательные и организационно-правовые основы подтверждения соответствия. Нормативная база сертификации. Правила и порядок проведения сертификации и декларирования соответствия. Аккредитация органов по сертификации и испытательных лабораторий. Схемы сертификации и декларирования соответствия. Сертификация услуг. Сертификация систем качества. Сертификация средств измерений.

**Рекомендуемый перечень основной литературы**:

1. Бисерова В.А, Демидова Н.В., Якорева А.С. Метрология, стандартизация и сертификация. – М.: Т8, 2021;

2. Сергеев А.Г. Метрология, стандартизация и сертификация. Часть 1. Метрология: учебник и практикум для бакалавриата. – М.: Юрайт, 2019;

3. Сергеев А.Г. Метрология, стандартизация и сертификация. Часть 2. Стандартизация и сертификация: учебник и практикум для бакалавриата. – М.: Юрайт, 2019;

**Перечень материально-технического обеспечения:**

1. Учебная лаборатория, оснащённая оборудованием: осциллографы универсальные, мультиметры, частотомеры электронно-счётные;

2. Компьютерный класс с установленным программным обеспечением Matlab.

### Б.1.П.3.3. Дисциплина «Информационные технологии. Операционные системы специального назначения»

Коды формируемых компетенций: ОПК-3.2, ОПК-3.4.

В результате изучения дисциплины студент должен

**знать:**

- основные понятия, функции, состав, принципы работы, архитектуру операционной системы специального назначения (Astra Linux);

- принципы управления ресурсами в операционной системе специального назначения (Astra Linux);

- основные задачи администрирования и способы их выполнения в операционной системе специального назначения (Astra Linux);

- модель управления доступом и информационными потоками в операционной системе специального назначения (Astra Linux);

**уметь:**

- устанавливать и конфигурировать современные операционные системы специального назначения;

- анализировать степень защищенности данных и ресурсов, определять политику безопасности и настраивать системы контроля доступа в операционных системах специального назначения.

**Общий объем времени** – 180 час., 5 з.е.

**Примерное распределение часов:** 90 часов контактная работа (из них 40 – лекции, 50 – практические занятия).

**Форма контроля:** экзамен

**Содержание дисциплины:**

**Обеспечение безопасности операционных систем семейства Linux.** Понятие защищённой (доверенной) операционной системы. Обзор защищённых операционных систем семейства Linux. Архитектура, назначение и области применения операционных систем специального назначения (ОССН).

**Основы пользовательской работы и администрирования в ОССН.** Варианты загрузки, экраны входа и выхода из ОССН. Основные приёмы работы с защищённой графической подсистемой Fly. Основные задачи администрирования ОССН.

**Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux.** Подход к формированию модели в её иерархическом представлении. **Уровень ролевого управления доступом.** Элементы состояния системы. Условия корректности состояний и переходов между ними. Де-юре правила преобразования состояний. Подходы к моделированию ролевого управления доступом в СУБД PostgreSQL. **Уровень мандатного контроля целостности.** Элементы состояния системы. Функционально или параметрически ассоциированные сущности. Условия корректности мандатного контроля целостности для состояний системы. Фактическое владение и де-факто правила преобразования состояний. Нарушение безопасности системы в смысле мандатного контроля целостности. **Уровни мандатного управления доступом.** Элементы состояния системы. Условия корректности мандатного управления доступом и правила преобразования состояний. Достаточные условия безопасности системы в смысле Белла-ЛаПадулы. Достаточные условия безопасности системы в смысле информационных потоков по времени. **Управление безопасностью ОССН. Мандатное управление доступом**. Проблемы реализации мандатного управления доступом в операционных системах. Реализация мандатного управления доступом в ОССН. Администрирование мандатного управления доступом в ОССН. Мандатный контроль целостности. Управление доступом к объектам графической подсистемы. Особенности аутентификации. Особенности аудита.

**Сетевое взаимодействие в ОССН. Организация доменной инфраструктуры.** Логические уровни сетевой инфраструктуры. Формирование базового уровня сетевой инфраструктуры ОССН. Формирование корпоративного уровня сетевой инфраструктуры ОССН. Единое пространство пользователей. Служба ALD. Администрирование доменной сетевой инфраструктуры ОССН. Служба FreeIPA. Формирование гетерогенной доменной сетевой инфраструктуры.

**Рекомендуемый перечень основной литературы**:

1. Буренин П.В., Девянин П.Н., Лебеденко Е.В. Безопасность операционной системы специального назначения Astra Linux Special Edition: учебное пособие. – М.: Горячая линия - Телеком, 2019;

2. Операционная система общего назначения «ASTRA LINUX COMMON EDITION». Руководство пользователя.

**Перечень материально-технического обеспечения:**

1. Компьютерный класс с установленной ОССН Astra Linux.

### Б.1.П.3.4. Дисциплина «Основы построения и функционирования специальных технических средств»

Коды формируемых компетенций: ОПК-3.1, ОПК-3.3.

В результате изучения дисциплины студент должен

**знать:**

- основы построения и функционирования средств радиоразведки;

- основы построения и функционирования средств акустической речевой разведки;

- основы построения и функционирования средств визуально-оптической и оптико-электронной разведки;

- основы построения и функционирования генераторов шума систем пространственного электромагнитного зашумления;

- основы построения и функционирования генераторов шума систем виброакустической маскировки;

**уметь:**

- исследовать характеристики модулей (элементов) специальных радиоприемных устройств, средств акустической речевой, визуально-оптической и оптико-электронной разведок;

* проектировать и исследовать характеристики высокочастотных и низкочастотных генераторов шума;

**владеть:**

- навыками проектирования и исследования характеристик модулей (элементов) специальных технических средств.

**Общий объем времени** – 216 час., 6 з.е.

**Примерное распределение часов:** 100 часов контактная работа (из них 60 – лекции, 40 – практические занятия).

**Форма контроля:** экзамен

**Содержание дисциплины:**

**Радиопередающие устройства специального назначения.** Обобщенная структурная схема и принцип работы передающего устройства. Классификация передающих устройств, используемых в системах перехвата информации. Принципы построения и основные характеристики аналоговых передающих устройств. Принципы построения и основные характеристики цифровых передающих устройств.

**Основы построения генераторов пространственного и линейного зашумления.** Электромагнитные шумы. Отношение сигнал/шум. Структурная схема, характеристики генераторов пространственного и линейного зашумления.

**Основы построения мониторинговых радиоприемников.** Обобщенная структурная схема радиоприемного устройства. Классификация радиоприемных устройств. Многоканальные и матричные радиоприемные устройства. Цифровые сканирующие приемники. Интерсепторы. Основные характеристики мониторинговых радиоприемников (диапазон частот, избирательность, чувствительность, динамический диапазон, скорость сканирования и т.д.).

**Акустические сигналы и их характеристики.** Основные направления акустики. Звук, основные характеристики. Акустический речевой сигнал. Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи.

**Акустоэлектрический эффект. Акустоэлектрические преобразователи. Микрофоны.** Классификация АЭП. Микрофонный эффект. Классификация, принципы построения и основные характеристики направленных микрофонов (параболических, трубчатых, микрофонных решеток).

**Основы построения систем виброакустической защиты.** Структурная схема генератора шума систем виброакустической маскировки. Акустические излучатели (классификация и основные характеристики). Виброизлучатели (классификация и основные характеристики).

**Основы построения визуально-оптических средств.** Классификация и характеристики оптического излучения. Строение глаза человека. Основные характеристики зрения: спектральная чувствительность, фокусное расстояние и апертура. Схемы построения и основные характеристики оптических средств наблюдения (фокусное расстояние, апертура, относительное отверстие, разрешающая способность, угол зрения).

**Объективы оптико-электронных средств.** Классификация объективов. Основы построения и основные характеристики линзовых объективов (фокусное расстояние, диафрагма, относительное отверстие, угол зрения, частотно-контрастная характеристики (разрешающая способность), спектральная чувствительность). Принципы построения и основные характеристики зеркальных объективов (фокусное расстояние, диафрагма, относительное отверстие, угол зрения, частотно-контрастная характеристики (разрешающая способность), спектральная чувствительность). Система фокусировки. Объективы с переменным фокусным расстоянием.

**Приемники оптического излучения.** Классификация приемников оптического излучения. ПЗС-матрицы: размеры, устройство, принцип работы и основные характеристики (размер элемента разложения фотоприемника, спектральная чувствительность, пороговая освещенность, частотно-контрастная характеристика (разрешающая способность), динамический диапазон). Цветные ПЗС-матрицы. **Основы построения цифровых камер.** Структурная схема и принцип работы цифровой камеры. Структурная схема и принцип работы цифровой телевизионной камеры. Цифровые камеры с объективом типа пинхоул. Основные характеристики цифровых камер. **Основы построения тепловизоров.** Тепловое излучение (Спектральная плотность теплового излучения, закон излучения Планка, закон смещения Вина, коэффициент теплового излучения). Классификация инфракрасного излучения (ближний, средний и дальний инфракрасные поддиапазоны). Классификация тепловизоров. Структурная схема и принцип работы тепловизора. Принципы построения приемников оптического излучения (ПОИ), работающих в инфракрасном диапазоне длин волн. Характеристики ПОИ (размер элемента разложения ПОИ, спектральная чувствительность, пороговая чувствительность по температуре, частотно-контрастная характеристика (разрешающая способность), динамический диапазон). Основные характеристики современных тепловизоров. **Основы построения лазерных акустических систем разведки.** Отражение лазерного излучения от оконных стекол. Триппель призмы. Классификация лазерных акустических систем разведки. Структурные схемы, принцип работы и основные характеристики лазерных акустических систем разведки.

**Рекомендуемый перечень основной литературы**:

1. Хорев А.А. Техническая защита информации. Том 1 «Технические каналы утечки информации»: учебное пособие. – М.: НПЦ Аналитика, 2008;

2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В.Технические средства и методы защиты информации: учебник. – М.: Горячая линия-Телеком, 2018;

3. Новожилов О.П. Электроника и схемотехника. В 2-х частях: учебник для академического бакалавриата. – М.: Юрайт, 2019.

**Перечень материально-технического обеспечения:**

1. Лаборатория «Технической защиты информации» с лабораторными стендами, оснащенными специализированным оборудованием:

- по защите речевой информации от утечки по акустовибрационным и акустооптическим каналам;

- по защите речевой информации от утечки по акустоэлектрическим каналам;

- по защите СВТ от утечки информации по каналам побочных электромагнитных излучений и наводок;

- по контролю защищенности СВТ от утечки информации по каналам побочных электромагнитных излучений и наводок.

### Б.1.П.3.5. Дисциплина «Защита информации от несанкционированного доступа»

Коды формируемых компетенций: ОПК-3.2, ОПК-3.4.

В результате изучения дисциплины студент должен

**знать:**

- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;

- классификацию и общую характеристику уязвимостей и угроз несанкционированного доступа к информации в автоматизированной системе;

- типовые средства для инструментальной оценки уровня защищённости автоматизированных систем;

**уметь:**

- применять современные технологии управления доступом, аутентификации и идентификации для обеспечения безопасности автоматизированных систем;

- проводить анализ защищенности информации от несанкционированного доступа в автоматизированных системах.

**Общий объем времени** – 180 час., 5 з.е.

**Примерное распределение часов:** 90 часов контактная работа (из них 40 – лекции, 50 – практические занятия).

**Форма контроля:** экзамен

**Содержание дисциплины:**

**Угрозы информации в автоматизированных системах (АС).** Объекты несанкционированного доступа (НСД). Способы, каналы и методы НСД к информации. Причины и виды утечек информации. Понятие угрозы информации в АС. Методы нарушения секретности, целостности и доступности информации. Классификация основных видов атак на АС. Понятие политики безопасности. Модель нарушителя. Дискреционная политика безопасности. Мандатная политика безопасности. Ролевое разграничение доступа. Модели безопасности компьютерных систем.

**Защита в операционных системах (ОС).** Назначение и функции ОС. Популярные архитектуры ОС. Управление ресурсами. Особенности ОС семейства Unix и Windows. Идентификация пользователей в ОС. Локальная аутентификация в ОС семейства Windows. PAM-модули аутентификации в ОС Linux. Угрозы безопасности в ОС. Субъекты и объекты доступа. Архитектура подсистемы защиты в ОС семейства Unix и Windows. Политики разграничения доступа в ОС. Политики обеспечения целостности информации.

**Защита в системах управления базами данных (СУБД).** Общая характеристика, назначения и возможности СУБД. Распределенные базы данных. Модели данных. Эксплуатация баз данных. Идентификация и аутентификация в СУБД. Модели безопасности в СУБД. Организация разграничения доступа в современных СУБД. Шифрование данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Целостность баз данных. Способы поддержания ссылочной целостности. Транзакции. ACID. Режимы блокировок. Тупиковые ситуации, их распознавание и устранение.

**Защита в ВС.** Криптографические средства и методы обеспечения целостности и конфиденциальности на различных уровнях модели ISO/OSI. Назначение, основные возможности, принципы функционирования и варианты реализации виртуальных частных сетей (VPN). Организация туннелирования на различных уровнях модели ISO/OSI. Место и роль межсетевых экранов (МЭ) в обеспечении безопасности ресурсов ВС. Основные возможности и схемы развертывания МЭ. Организация экранирования на различных уровнях модели ISO/OSI. Персональные и корпоративные МЭ.

**Обеспечение информационной безопасности с использованием средств антивирусной защиты.** Вредоносное программное обеспечение (ПО). Методы внедрения. Классификация вредоносных программ. Признаки присутствия вредоносного ПО. Методы защиты. Методы обнаружения. Классификация средств антивирусной защиты. Возможности и ограничения антивирусных программ.

**Критерии защищенности АС. Требования к средствам защиты информации.** Критерии оценки безопасности компьютерных систем. Основные положения и структура руководящих документов Гостехкомиссии в области защиты информации. Концепция защиты СВТ и АС от НСД. Единые критерии безопасности информационных технологий.

**Рекомендуемый перечень основной литературы**:

1. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите. — М.: Горячая линия-Телеком, 2008;

2. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации. – М.: Книжный дом «ЛИБРОКОМ», 2012.

**Перечень материально-технического обеспечения:**

### 1. Компьютерный класс со специализированным программным обеспечением.

### Б.1.П.3.6. Дисциплина «Основы эксплуатации систем защиты объектов информатизации»

Коды формируемых компетенций: ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-3.4.

В результате изучения дисциплины студент должен

**знать:**

- классификацию, основные этапы эксплуатации, технического обслуживания средств защиты информации (СЗИ) от утечки по техническим каналам;

- классификацию, основные этапы эксплуатации, технического обслуживания средств защиты информации (СЗИ) от несанкционированного доступа;

- классификацию, основные этапы эксплуатации, технического обслуживания средств контроля эффективности защиты информации (СКЭЗИ) от утечки по техническим каналам;

- классификацию, основные этапы эксплуатации, технического обслуживания средств контроля эффективности защиты информации (СКЭЗИ) от несанкционированного доступа;

**уметь:**

- разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СЗИ от утечки по техническим каналам;

- разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СЗИ от несанкционированного доступа;

- разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СКЭЗИ от утечки по техническим каналам;

- разрабатывать документы по приему, выдаче, закреплению, вводу в эксплуатацию, выводу из эксплуатации и списанию СКЭЗИ от несанкционированного доступа.

**Общий объем времени** – 108 час., 3 з.е.

**Примерное распределение часов:** 60 часов контактная работа (из них 30 – лекции, 30 – практические занятия).

**Форма контроля:** зачет

**Содержание дисциплины:**

**Основы организации эксплуатации систем защиты объектов информатизации.** Термины и определения в области эксплуатации СЗИ. Классификация СЗИ (технические, программные, программно-технические). Средства контроля эффективности защиты информации (СКЭЗИ). Основные этапы эксплуатации СЗИ и СКЭЗИ, их краткая характеристика.

**Ввод средств защиты информации в эксплуатацию.** Порядок приема, выдачи и закрепления СЗИ.Аттестационные испытания СЗИ. Порядок ввода СЗИ в эксплуатацию. **Вывод из эксплуатации и списание средств защиты информации.** Порядок вывода из эксплуатации СЗИ и СКЭЗИ. Организация списания и утилизации СЗИ и СКЭЗИ. Обеспечение режима секретности при утилизации СЗИ и СКЭЗИ.

**Меры безопасности при эксплуатации средств защиты информации.** Общие требования по обеспечению безопасности при эксплуатации СЗИ. Меры безопасности при эксплуатации СЗИ. Порядок допуска личного состава к самостоятельной работе со СЗИ. Виды, порядок и сроки инструктажей личного состава по технике безопасности.

**Основы технического обслуживания средств защиты информации**. Роль и место системы технического обслуживания и ремонта в системе эксплуатации СЗИ и СКЭЗИ.Состав и содержание эксплуатационной документации на СЗИ и СКЭЗИ. Обеспечение режима секретности при эксплуатации и техническом обслуживании СЗИ.

**Основы метрологического обеспечения средств защиты информации.** Общие сведения о метрологии и метрологическом обеспечении. Виды и методы измерений. Погрешности измерений. Виды средств измерений. Метрологические характеристики средств измерений. Классы точности средств измерений. Виды и периодичность поверок средств измерений. Организация поверок средств измерений. Калибровка средств измерений.

**Техническое обслуживание технических средств защиты информации.** Техническое обслуживание систем пространственного и линейного электромагнитного зашумления.Техническое обслуживание систем виброакустической защиты**.**

**Контроль, диагностирование и восстановление программного обеспечения**. Методы диагностирования программного обеспечения и СВТ. Средства диагностирования программного обеспечения и СВТ. Средства восстановленияпрограммного обеспечения. Организация восстановления программного обеспечения при сбоях.

**Неисправности СВТ, характерные особенности их проявления и методы восстановления работоспособности**. Конфликты при установке оборудования и способы их устранения. Типовые алгоритмы поиска неисправностей в СВТ. Перечень возможных неисправностей материнской платы, BIOS и CMOS-памяти, оперативной памяти, жесткого диска, сетевой карты, оптических дисков, flash-накопителей, принтеров, сканеров и др. Восстановление их работоспособности.

**Рекомендуемый перечень основной литературы**:

1. Хорев А.А. Техническая защита информации. Том 1 «Технические каналы утечки информации»: учебное пособие. – М.: НПЦ Аналитика, 2008;

2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В.Технические средства и методы защиты информации: учебник. – М.: Горячая линия-Телеком, 2018;

3. Извозчикова В.В. Эксплуатация и диагностирование технических и программных средств информационных систем: учебное пособие. – Оренбург: Оренбургский государственный университет, 2017.

**Перечень материально-технического обеспечения:**

1. Лаборатория «Технической защиты информации» с лабораторными стендами, оснащенными специализированным оборудованием:

- по защите речевой информации от утечки по акустовибрационным и акустооптическим каналам;

- по защите речевой информации от утечки по акустоэлектрическим каналам;

- по защите СВТ от утечки информации по каналам побочных электромагнитных излучений и наводок;

- по контролю защищенности СВТ от утечки информации по каналам побочных электромагнитных излучений и наводок.

### 2. Компьютерный класс со специализированным программным обеспечением.

# Раздел 4. СПИСОК РАЗРАБОТЧИКОВ

|  |  |
| --- | --- |
| Ф.И.О. разработчика | Должность |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Приложение 1

Перечень профессиональных стандартов, соотнесенных с программой по профилю № 3 «Техническая защита информации» ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность»

|  |  |  |
| --- | --- | --- |
| № п/п | Код профессионального стандарта | Наименование области профессиональной деятельности. Наименование профессионального стандарта |
| 06 Связь, информационные и коммуникационные технологии | | |
| 1. | 06.034 | Профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44443) |
| 12 Обеспечение безопасности | | |
| 2. | 12.005 | Профессиональный стандарт, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 25 декабря 2015 г. № 15с (зарегистрирован Министерством юстиции Российской Федерации 22 января 2016 г., регистрационный № 40706) |

Приложение 2

Перечень обобщенных трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ бакалавриата по профилю № 3 «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность»

| **Код и**  **наименование**  **профессионального стандарта** | **Обобщенные трудовые функции** | | | **Трудовые функции** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Код** | **Наименование** | **Уровень**  **квалификации** | **Наименование** | **Код** | **Уровень (подуровень) квалификации** |
| 06.034 Специалист по технической защите информации | B | Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации | 6 | Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации | B/01.6 | 6 |
| Проведение работ по техническому обслуживанию защищенных технических средств обработки информации | B/02.6 | 6 |
| D | Проведение контроля защищенности информации | 6 | Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации | D/01.6 | 6 |
| Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок | D/02.6 | 6 |
| Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам | D/03.6 | 6 |
| Проведение контроля защищенности информации от несанкционированного доступа | D/04.6 | 6 |