**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

**УТВЕРЖДЕНО**
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
« 28 » мая 2020 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Техническая защита информации»

Направление подготовки
**10.03.01 «Информационная безопасность»**

Образовательная программа (профиль)
**«Безопасность компьютерных систем»**

Квалификация (степень) выпускника
**Бакалавр**

Форма обучения
**Очная**

Год приема - 2020

Москва 2020 г.

## 1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Техническая защита информации» следует отнести:

- теоретическую и практическую подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации.

К **основным задачам** освоения дисциплины «Техническая защита информации» следует отнести:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

## 2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Техническая защита информации» относится к числу профессиональных учебных дисциплин базовой части цикла Б.1.1 (Б.1.1.36) основной образовательной программы бакалавриата.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Математический анализ», «Теория вероятностей» и «Математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности», «Физические основы информационной безопасности».

## 3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

| **Код компетенции** | **В результате освоения образовательной программы обучающийся должен обладать** | **Перечень планируемых результатов обучения по дисциплине** |
|---|---|---|

| | | |
|---|---|---|
| ОПК - 3 | способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач | **знать:**<br>основные положения электротехники, электроники и схемотехники<br><br>**уметь:**<br>использовать положения электротехники, электроники и схемотехники для решения профессиональных задач |
| ПК-1 | способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | **знать:**<br>современные программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации<br>**уметь:**<br>выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации |
| ПК - 6 | способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | **знать:**<br>виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации<br><br>**уметь:**<br>организовывать и сопровождать контроль эффективности технических средств защиты информации<br><br>**владеть:**<br>навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения |
| ПСК-1.1 | Способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | **знать:**<br>типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах<br>**уметь:**<br>принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах |

## 4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. **144** академических часа (лабораторные занятия – 72 час, самостоятельная работа – 72 часа), форма контроля – экзамен в 6 семестре.

Структура и содержание дисциплины «Техническая защита информации» по срокам и видам работы отражены в приложении.

### Содержание разделов дисциплины

### Тема 1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы по технической защите информации.

Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

### Тема 2. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

### Тема 3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

### Тема 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.

### Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

### Тема 6. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

### Тема 7. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

### Тема 8. Организация технической защиты информации

Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.

Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.

Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации.

## 5. Образовательные технологии

Методика преподавания дисциплины «Техническая защита информации» » и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение интерактивных лекционных занятий с использованием интерактивной доски;
- проведение лабораторных работ (практических занятий по оценке опасности технических каналов утечки информации на базе специальной техники и программно-аппаратных комплексов), обсуждение и защита рефератов по темам дисциплины.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 70 % аудиторных занятий. Занятия лекционного типа составляют 30 % от объема аудиторных занятий.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

Темы презентаций (рефератов) и лабораторных занятий, а также контрольные вопросы для проведения экзамена приведены в приложении.

### 6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

#### 6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины (модуля) формируются следующие компетенции:

| Код компетенции | В результате освоения образовательной программы обучающийся должен обладать |
|---|---|
| ОПК - 3 | способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач |
| ПК - 1 | способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации |
| ПК - 6 | способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации |
| ПСК-1.1 | Способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах |

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

#### 6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

| **ОПК -3 способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач** | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| **знать:** основные положения электротехники, электроники и схемотехники | Обучающийся демонстрирует полное отсутствие или недостаточное знание основных положений электротехники, электроники и схемотехники | Обучающийся демонстрирует частичное (удовлетворительное) знание и понимание основных положений электротехники, электроники и схемотехники | Обучающийся демонстрирует полное знание и понимание основных положений электротехники, электроники и схемотехники, но допускает незначительные ошибки, неточности | Обучающийся демонстрирует полное знание и понимание основных положений электротехники, электроники и схемотехники |
| **уметь:** использовать положения электротехники, электроники и схемотехники для решения профессиональных задач | Обучающийся не умеет или в недостаточной степени умеет использовать положения электротехники, электроники и схемотехники для решения профессиональных задач | Обучающийся демонстрирует удовлетворительное умение использовать положения электротехники, электроники и схемотехники для решения профессиональных задач | Обучающийся демонстрирует полное умение использовать положения электротехники, электроники и схемотехники для решения профессиональных задач , но допускает незначительные ошибки, неточности | Обучающийся демонстрирует полное умение использовать положения электротехники, электроники и схемотехники для решения профессиональных задач |
| **ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации** | | | | |
| **знать:** современные программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации | Обучающийся демонстрирует полное отсутствие или недостаточное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | Обучающийся демонстрирует знание основныхсовременных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, но допускает существенные ошибки, неточности. | Обучающийся демонстрирует полное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, но допускает незначительные ошибки, неточности | Обучающийся демонстрирует полное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации |

| | | | | |
|---|---|---|---|---|
| **уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | Обучающийся не умеет или в недостаточной степени умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | Обучающийся демонстрирует умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации, но допускает существенные ошибки, неточности. | Обучающийся демонстрирует полное умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации, но допускает незначительные ошибки, неточности | Обучающийся демонстрирует полное умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации |
| **ПК – 6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации** | | | | |
| **знать:** виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации | Обучающийся не знает видов и методов контрольных проверок эффективности применяемых мер и средств защиты информации | Обучающийся знает виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации, но допускает существенные ошибки, неточности. | Обучающийся знает все виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации, но допускает незначительные ошибки, неточности | Обучающийся знает все виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации |
| **уметь:** организовывать и сопровождать контроль эффективности технических средств защиты информации | Обучающийся не умеет организовывать и сопровождать контроль эффективности технических средств защиты информации | Обучающийся имеет представление об организации и сопровождении контроля эффективности технических средств защиты информации, но допускает значительные неточности, ошибки | Обучающийся имеет представление об организации и сопровождении контроля эффективности технических средств защиты информации, но допускает незначительные неточности. | Обучающийся умеет организовать и сопровождать контроль эффективности технических средств защиты информации |
| **владеть:** навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения | Обучающийся не владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения | Обучающийся не в полной мере владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения | Обучающийся владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения, но допускает незначительные неточности | Обучающийся полностью владеет навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения |
| **ПСК-1.1 способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах** | | | | |
| **знать:** типовые | Обучающийся не имеет представления о | Обучающийся имеет общее представление | Обучающийся имеет полное представление | Обучающийся имеет полное |

| | | | | |
|---|---|---|---|---|
| модели политик безопасности, политик управления доступом и информационн ыми потоками в компьютерных системах | типовой структуре политики информационной безопасности и политике управления доступом и информационными потоками в компьютерных системах | о типовой структуре политики информационной безопасности и политике управления доступом и информационными потоками в компьютерных системах, допускает ошибки в определении понятий и терминов. | о типовой структуре политики информационной безопасности и политике управления доступом и информационными потоками в компьютерных системах, но допускает незначительные неточности | представление о типовой структуре политики информационной безопасности и политике управления доступом и информационными потоками в компьютерных системах |
| **уметь:** принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационн ыми потоками в компьютерных системах | Обучающийся не умеет или в недостаточной степени умеет принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | Обучающийся частично умеет принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | Обучающийся полностью умеет применять комплексный подход по разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, но допускает незначительные неточности | Обучающийся полностью умеет применять комплексный подход по разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах |

Шкалы оценивания результатов промежуточной аттестации и их описание:

***Форма промежуточной аттестации: экзамен.***

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| ***Шкала оценивания*** | ***Описание*** |
|---|---|
| *Отлично* | *Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.* |
| *Хорошо* | *Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков* |

| | |
|---|---|
| | *приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.* |
| *Удовлетворительно* | *Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.* |
| *Неудовлетворительно* | *Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.* |

Фонды оценочных средств представлены в приложении к рабочей программе.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### а) основная литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. том 1 Технические каналы утечки информа – М.: НПЦ «Аналитика», 2010
2. Рагозин Ю.Н. Инженерно-техническая защита информации: лабораторный практикум. – М: МГИУ, 2008
3. Рагозин Ю.Н. Инженерно-техническая защита информации: учебное пособие/ИЦ Санкт-Петербург, 2018 – 168 с.

### б) дополнительная литература

### в) программное обеспечение и интернет-ресурсы:

- специальное программное обеспечение СПО «СПРУТ-мини» для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам;
- специальное программное обеспечение СПО «Навигатор» для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ;
- специальное программное обеспечение СПО «Крона +» для радиомониторинга защищаемых помещений;
- Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.
- Портал технического комитета по стандартизации «Защита информации». – http://tk.gost.ru/wps/portal/tk362
- Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/
- Портал по безопасности. – http://www.sec.ru/.
- http://uchebnik.online/uchebnik-predprinimatelstvo/elektromagnitnyie-kanalyi-... Электромагнитные каналы утечки информации
- Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/

## 8. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Для проведения лабораторных (практических) занятий необходимы:

- анализатор спектра с демодуляторами с полосой частот 9КГц-3ГГц;
- интерфейс анализатора спектра с компьютером (GPIB, USB);
- набор электрических и магнитных антенн (полоса частот 9КГц-3ГГц);
- эквивалент сети;
- генераторы пространственного и линейного электромагнитного зашумления;
- генераторы акустического и виброакустического зашумления;
- программно-аппаратный комплекс «СПРУТ-мини»;
- многофункциональный поисковый прибор SN-031 «Пиранья»;
- измеритель спектра вторичных полей (детектор нелинейных переходов).

## 9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются занятия ***лекционного типа*** **и самостоятельная работа студентов**.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные (практические) занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на занятиях лекционного типа и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков работы с программно-аппаратными комплексами, которые используются в профессиональной деятельности специалистов по информационной безопасности.

Самостоятельная работа по дисциплине предполагает выполнение студентами домашних заданий (подготовка презентаций по темам дисциплины). Домашние задания содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, посещение различных выставок и конференций по проблемным вопросам защиты информации, использование справочной литературы и др.

При выдаче заданий (тем презентаций) для самостоятельной работы используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:
- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

## 10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

**Программу составил:** доцент, к.э.н., доц. Рагозин Ю.Н.

**Программа утверждена на заседании кафедры «Информационная безопасность»** «29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность автоматизированных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая

Кафедра: «Информационная безопасность»

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ПО ДИСЦИПЛИНЕ

## «Техническая защита информации»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Темы презентаций (докладов)
Экзамен

**Составители: к.э.н., доцент Рагозин Ю.Н.**

Москва, 2020 год

Таблица

**ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

| **Техническая защита информации** | | | | | |
|---|---|---|---|---|---|
| ФГОС ВО **10.03.01 «Информационная безопасность»** | | | | | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**: | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технология формирования компетенций** | **Форма оценоч-ного средств** | **Степени уровней освоения компетенций** |
| **ИН-ДЕКС** | **ФОРМУЛИРОВКА** | | | | |
| ОПК - 3 | способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач | **знать:**<br>основные положения электротехники, электроники и схемотехники<br><br>**уметь:**<br>использовать положения электротехники, электроники и схемотехники для решения профессиональных задач | Лабораторные и практические занятия, самостоятельная работа | Экзамен | **Базовый уровень:**<br>способен продемонстрировать знание основных положений электротехники, электроники и схемотехники<br><br>**Повышенный уровень:**<br>Способен продемонстрировать полное знание и понимание основных положений электротехники, электроники и схемотехники |

| | | | | | |
|---|---|---|---|---|---|
| ПК - 1 | способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | **знать:**<br>современные программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации<br>**уметь:**<br>выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | Лабораторные и практические занятия, самостоятельная работа | Экзамен | **Базовый уровень:**<br>способен продемонстрировать знание основных современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации<br><br>**Повышенный уровень:**<br>способен продемонстрировать полное знание современных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. |

| | | | | | |
|---|---|---|---|---|---|
| ПК - 6 | способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | **знать:**<br>виды и методы контрольных проверок эффективности применяемых мер и средств защиты информации<br>**уметь:**<br>организовывать и сопровождать контроль эффективности технических средств защиты информации<br>**владеть:**<br>навыками работы с контрольно-измерительной аппаратурой и программно-аппаратными комплексами специального назначения | Лабораторные и практические занятия, самостоятельная работа | Экзамен | **Базовый уровень:**<br>способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации<br><br>**Повышенный уровень:**<br>Способен самостоятельно организовать проведение контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации |

| | | | | | |
|---|---|---|---|---|---|
| ПСК – 1.1 | способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | **знать:**<br>типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах<br>**уметь:**<br>принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | Лабораторные и практические занятия, самостоятельная работа | Экзамен | **Базовый уровень:**<br>способность принимать участие в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах<br><br>**Повышенный уровень:**<br>способность самостоятельно разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах |

**Оценочные средства для текущей аттестации**

**Примерные темы презентаций (докладов):**

1. Современные цифровые диктофоны.
2. Типы микрофонных систем и их технические характеристики.
3. Область применения электронных стетоскопов (радиостетоскопов).
4. и их конструктивные особенности.
5. Лазерные акустические систем разведки.
6. Цифровые анализаторы спектра.
7. Векторные анализаторы сигналов.
8. Измерительные цифровые приемники.
9. Измерительные антенны, токосъемники, пробники для проведения специальных исследований средств вычислительной техники.
10. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
11. Портативные шумомеры и виброметры.
12. Аудиоанализаторы и область применения.
13. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
14. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
15. Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
16. Индикаторы электромагнитного поля.
17. Радиочастотомеры.
18. Сканирующие радиоприемники.
19. Специальные поисковые приемники ближней зоны и интерсепторы.
20. Программно-аппаратные комплексы радиомониторинга.
21. Анализаторы проводных линий.
22. **Программно-аппаратные комплексы для исследования проводных линий.**
23. Нелинейные радиолокаторы.
24. Рентгенотелевизионные комплексы.
25. Портативные металлоискатели.
26. Эндоскопы.
27. Нормативно-методические документы ФСТЭК в области технической защиты информации.

**Оценочные средства для промежуточной аттестации**

**Вопросы экзаменационных билетов**

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС).
2. Вспомогательные технические средства и системы (ВТСС).
3. Технический канал утечки информации (определение). Схема технического канала утечки информации
4. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

5. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

6. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.

7. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

8. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

9. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата).

10. Дальность перехвата речевого сигнала средствами акустической разведки.

11. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации.

12. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.

13. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

14. Экранирующие материалы, их основные характеристики.

15. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.

16. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).

17. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

18. Основные требования к системе пространственного электромагнитного зашумления.

19. Схема установки системы пространственного зашумления на объекте информатизации.

20. Основные требования по установке системы пространственного зашумления на объекте информатизации.

21. Основные характеристики генераторов шума.

22. Основные требования к системе электропитания технических средств.

23. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений.

24. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств.

25. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.

26. Характеристики речевого сигнала. Разборчивость речи.

27. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

28. Средства звуко- и виброизоляции выделенных помещений.

29. Звукоизолирующие кабины. Специальные защищенные помещения.

30. Порядок проведения контроля эффективности защиты ВТСС.

31. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

32. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

33. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.

34. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

35. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

36. Сканирующие приемники (принцип работы, основные характеристики). Этапы выявления РЗ. Методы обнаружения, идентификации РЗ и определения их местоположения.

37. Порядок организации защиты информации на объектах информатизации.

38. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

39. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

**40.** Заключение по результатам аттестационной проверки объекта информатизации. Аттестат соответствия объекта информатизации.

**Структура и содержание дисциплины «Техническая защита информации»**
**по направлению подготовки**
**10.03.01 «Информационная безопасность»**
**(бакалавр)**
**Профиль: Безопасность автоматизированных систем**

| n/n | Раздел | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах | | | | | Виды самостоятельной работы студентов | | | | | Формы аттестации | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Л | П/С | Лаб | СРС | КСР | К.Р. | К.П. | ДЗ | Реферат | К/р | Э | З |
| 1 | **Технические каналы утечки акустической (речевой) информации** Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики. | 6 | 1-4 | | | 16 | 16 | | | | | + | | | |
| 2 | **Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными** | 6 | 5-8 | | | 16 | 16 | | | | | + | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **системами**<br>Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации. | | | | | | | | | | | | | | |
| 3 | **Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами**<br>Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, | 6 | 9-12 | | | 16 | 16 | | | | | + | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники. | | | | | | | | | | | | | | |
| 4 | **Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам** Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи). | 6 | 13-16 | | | 16 | 16 | | | | | + | | | |
| 5 | **Организация технической защиты информации** Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации. | 6 | 17-18 | | | 8 | 8 | | | | | + | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации. | | | | | | | | | | | | | | |
| | ***Форма аттестации*** | | 18 | | | | | | | | | | | Э | |
| | **Всего часов по дисциплине в пятом семестре** | | | | | **72** | **72** | | | | | | | | |