

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования "Пермский  
государственный национальный исследовательский  
университет"**

**Кафедра радиоэлектроники и защиты информации**

**Авторы-составители: Лунегов Игорь Владимирович**

**Рабочая программа дисциплины  
ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ  
Код УМК 94107**

**Утверждено  
Протокол №4  
от «24» июня 2020 г.**

**Пермь, 2020**

## **1. Наименование дисциплины**

Введение в специальность

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем  
специализация Безопасность открытых информационных систем

### **3. Планируемые результаты обучения по дисциплине**

В результате освоения дисциплины **Введение в специальность** у обучающегося должны быть сформированы следующие компетенции:

**10.05.03** Информационная безопасность автоматизированных систем (специализация : Безопасность открытых информационных систем)

**УК.2** Способен управлять проектом, организовывать и руководить работой команды

#### **Индикаторы**

**УК.2.1** Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения

**УК.8** Знает правовые и этические нормы, способен оценивать последствия нарушения этих норм

#### **Индикаторы**

**УК.8.2** Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения

**ОПК.4** готовность к участию в проведении научных исследований

**ПК.1** способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке

**УК.10** Владеет базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии

#### 4. Объем и содержание дисциплины

<b>Направления подготовки</b>	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	3
<b>Объем дисциплины (з.е.)</b>	3
<b>Объем дисциплины (ак.час.)</b>	108
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	42
<b>Проведение лекционных занятий</b>	28
<b>Проведение практических занятий, семинаров</b>	14
<b>Самостоятельная работа (ак.час.)</b>	66
<b>Формы текущего контроля</b>	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
<b>Формы промежуточной аттестации</b>	Зачет (3 триместр)

## **5. Аннотированное описание содержания разделов и тем дисциплины**

### **Введение в специальность**

**Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ**  
Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна. Правовое обеспечение защиты информации.

**Терминологические основы защиты информации. Основные понятия и определения**  
Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы - определения, сопоставление.

**Общеметодологические принципы теории защиты информации**  
Этапы развития информационной безопасности:  
1. Системы безопасности ресурса.  
2. Этап развитой защиты (постепенное осознание необходимости комплексирования целей защиты, расширение арсенала используемых средств защиты, стали объединяться в функциональные самостоятельные системы защиты).  
3. Этап комплексной защиты. Требования к системе защиты информации. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная

**Угрозы. Классификация и анализ угроз информационной безопасности**  
Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы:  
1) подверженность физическому искажению или уничтожению;  
2) возможность несанкционированной (случайной или злоумышленной) модификации;  
3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.  
Характер происхождения угроз: умышленные факторы, естественные факторы.  
Источники угроз. Предпосылки появления угроз: объективные, субъективные.

**Способы нарушения конфиденциальности, целостности и доступности информации**  
Классы каналов несанкционированного получения информации:  
1) непосредственно с объекта;  
2) с каналов отображения информации;  
3) получение по внешним каналам;  
4) подключение к каналам получения информации.  
Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.  
Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.  
Основные функции защиты информации.  
Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия.

Архитектура систем защиты информации.  
Семирубежная модель защиты информации.

### **Причины, виды, каналы утечки и искажения информации**

Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.  
Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации.  
Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.

### **Функции и задачи защиты информации**

Методы формирования функций защиты. Соккрытие информации о средствах, комплексах, объектах и системах обработки информации.  
Дезинформация противника. Легендирование. Введение избыточности элементов системы.  
Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации.  
Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации.  
Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии. Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.

### **Итоговое контрольное мероприятие**

Проверка уровня усвоения дисциплины.  
Знания теории защиты информации, основных направлений. Обеспечение информационной безопасности и направления защиты.  
Комплексность (целевая, инструментальная, структурная, функциональная, временная). Требования к системе защиты информации. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.  
Система защиты информации. Классы каналов несанкционированного получения информации.  
Причины нарушения целостности информации. Методы и модели оценки уязвимости информации.  
Общая модель воздействия на информацию.  
Общая модель процесса нарушения физической целостности информации. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации.  
Допущения в моделях оценки уязвимости информации. Методы определения требований к защите информации.

## **6. Методические указания для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

## **7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

## **8. Перечень основной и дополнительной учебной литературы**

### **Основная:**

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/97562>

2. Дацун Н. Н. Моделирование информационных систем. Указания к выполнению лабораторных работ и проведению практических занятий. учебное пособие для студентов, обучающихся по направлению подготовки бакалавров "Прикладная математика и информатика", "Инфокоммуникационные технологии и системы связи" и специальности "Компьютерная безопасность" Ч. 1/Н. Н. Дацун ; М-во науки и высш. образования РФ, Перм. гос. нац. исслед. ун-т.-Пермь:ПГНИУ, 2019, ISBN 978-5-7944-3283-1.-Библиогр.: с. 101-102 <https://elis.psu.ru/node/570440>

### **Дополнительная:**

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451933>

2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/72345.html>



## **9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины**

<https://www.securitycode.ru/> Сайт компании "Код безопасности"

[www.infoguard.ru/](http://www.infoguard.ru/) сайт НТИЦ "Информационная безопасность"

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

Образовательный процесс по дисциплине **Введение в специальность** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:

- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Player";
- программа просмотра интернет контента (браузер) "Google Chrome".

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

## **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Аудитория для проведения занятий лекционного и практического типа оснащена презентационной техникой:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для текущего контроля:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для индивидуальных (групповых) консультаций:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для самостоятельной работы:

- 1) компьютерная техника с возможностью подключения к сети «Интернет», с доступом в электронную информационно-образовательную среду ПГНИУ;
- 2) помещения Научной библиотеки ПГНИУ

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

- Операционная система ALT Linux;
- Офисный пакет Libreoffice.
- Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине  
Введение в специальность**

**Планируемые результаты обучения по дисциплине для формирования компетенции.  
Индикаторы и критерии их оценивания**

**ОПК.4**

**готовность к участию в проведении научных исследований**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ОПК.4</b> готовность к участию в проведении научных исследований	знать требования к проведению научных исследований, уметь решать нестандартные задачи, владеть навыками аналитического мышления	<p><b>Неудовлетворител</b> не знает требований к проведению научных исследований, не умеет решать нестандартные задачи, не владеет навыками аналитического мышления</p> <p><b>Удовлетворительн</b> частично сформированные знания требования к проведению научных исследований, частично сформированные умения решать нестандартные задачи, частично сформированные навыки аналитического мышления</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания требования к проведению научных исследований, сформированные, но содержащие пробелы умения решать нестандартные задачи, сформированные, но содержащие пробелы навыки аналитического мышления</p> <p><b>Отлично</b> сформированные знания требования к проведению научных исследований, сформированные умения решать нестандартные задачи, сформированные навыки аналитического мышления</p>

**ПК.1**

**способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ПК.1</b> способность осуществлять поиск, изучение, обобщение и	знать лексику и грамматику одного из иностранных языков, уметь читать техническую литературу на иностранном	<p><b>Неудовлетворител</b> не знает лексику и грамматику ни одного из иностранных языков, не умеет читать техническую литературу на иностранном</p>

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке	языке, владеть навыками поиска, изучения, обобщения и систематизации научно-технической информации	<p><b>Неудовлетворител</b> языке, не владеет навыками поиска, изучения, обобщения и систематизации научно-технической информации</p> <p><b>Удовлетворительн</b> частично сформированные знания лексики и грамматики одного из иностранных языков, частично сформированные умения читать техническую литературу на иностранном языке, частично сформированные навыки поиска, изучения, обобщения и систематизации научно-технической информации</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания лексики и грамматики одного из иностранных языков, сформированные, но содержащие пробелы умения читать техническую литературу на иностранном языке, сформированные, но содержащие пробелы навыки поиска, изучения, обобщения и систематизации научно-технической информации</p> <p><b>Отлично</b> сформированные знания лексики и грамматики одного из иностранных языков, сформированные умения читать техническую литературу на иностранном языке, сформированные навыки поиска, изучения, обобщения и систематизации научно-технической информации</p>

### **УК.10**

**Владеет базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>УК.10</b> Владеет базовыми знаниями в области информатики, навыками использования программных средств и	знать базовые законы информатики, уметь использовать программные средства для решения прикладных задач, владеть навыками использования современных информационных	<p><b>Неудовлетворител</b> не знает базовые законы информатики, не умеет использовать программные средства для решения прикладных задач, не владеет навыками использования современных информационных технологий для приобретения новых знаний</p>

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии	технологий для приобретения новых знаний	<p><b>Удовлетворительн</b> частично сформированные знания базовых законов информатики, частично сформированные умения использовать программные средства для решения прикладных задач, частично сформированные навыки использования современных информационных технологий для приобретения новых знаний</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания базовых законов информатики, сформированные, но содержащие пробелы умения использовать программные средства для решения прикладных задач, сформированные, но содержащие пробелы навыки использования современных информационных технологий для приобретения новых знаний</p> <p><b>Отлично</b> сформированные знания базовых законов информатики, сформированные умения использовать программные средства для решения прикладных задач, сформированные навыки использования современных информационных технологий для приобретения новых знаний</p>

## **УК.2**

### **Способен управлять проектом, организовывать и руководить работой команды**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>УК.2.1</b> Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения	знать требования к созданию проектов, уметь защищать подготовленный проект, владеть навыками публичных выступлений	<p><b>Неудовлетворител</b> не знает требования к созданию проектов, не умеет защищать подготовленный проект, не владеет навыками публичных выступлений</p> <p><b>Удовлетворительн</b> частично сформированные знания требований к созданию проектов, частично сформированные умения защищать подготовленный проект, посредственное владение навыками публичных выступлений</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания требований к созданию проектов,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p><b>Хорошо</b> сформированные, но содержащие пробелы умения защищать подготовленный проект, неуверенное владение навыками публичных выступлений</p> <p><b>Отлично</b> сформированные знания требований к созданию проектов, сформированные умения защищать подготовленный проект, уверенное владение навыками публичных выступлений</p>

### УК.8

**Знает правовые и этические нормы, способен оценивать последствия нарушения этих норм**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>УК.8.2</b> Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения</p>	<p>Знать этические нормы поведения и последствия их нарушения, уметь вести себя в обществе в соответствии с принятым этикетом, владеть навыками делового общения</p>	<p><b>Неудовлетворител</b> не знает этические нормы поведения и последствиях их нарушения, не умеет вести себя в обществе в соответствии с принятым этикетом, не владеет навыками делового общения</p> <p><b>Удовлетворительн</b> частично сформированные знания этических норм поведения и последствий их нарушения, частично сформированные умения вести себя в обществе в соответствии с принятым этикетом, частично сформированные навыки делового общения</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания этических норм поведения и последствий их нарушения, сформированные, но содержащие пробелы умения вести себя в обществе в соответствии с принятым этикетом, сформированные, но содержащие пробелы навыки делового общения</p> <p><b>Отлично</b> сформированные знания этических норм поведения и последствий их нарушения, сформированные умения вести себя в обществе в соответствии с принятым этикетом, сформированные навыки делового общения</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично общения

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Зачет

**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

**Максимальное количество баллов :** 100

### Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 43 до 60

«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>Входной контроль</b>	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ <b>Входное тестирование</b>	проверка остаточных знаний по курсу общая физика и представлений о распространении звуковых и электромагнитных волн
<b>ОПК.4</b> готовность к участию в проведении научных исследований <b>УК.10</b> Владеет базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии	Угрозы. Классификация и анализ угроз информационной безопасности <b>Защищаемое контрольное мероприятие</b>	Знания нормативной базы в области защиты информации. Умения классифицировать угрозы безопасности информации. Знание способов нарушения конфиденциальности, целостности, полноты и доступности



Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.1</b> способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке</p> <p><b>ОПК.4</b> готовность к участию в проведении научных исследований</p> <p><b>УК.8.2</b> Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения</p>	<p>Причины, виды, каналы утечки и искажения информации</p> <p><b>Защищаемое контрольное мероприятие</b></p>	<p>Знание каналов утечки информации, видов инженерно-технической защиты и организационных мероприятий по защите информации.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.1</b> способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке</p> <p><b>УК.2.1</b> Формулирует на основе поставленной проблемы проектную задачу и предлагает способы ее решения</p> <p><b>ОПК.4</b> готовность к участию в проведении научных исследований</p> <p><b>УК.8.2</b> Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения</p> <p><b>УК.10</b> Владеет базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии</p>	<p>Итоговое контрольное мероприятие</p> <p><b>Итоговое контрольное мероприятие</b></p>	<p>знание нормативной базы в области защиты информации, каналов утечки информации, технических средств защиты.</p>

### Спецификация мероприятий текущего контроля

#### Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
-----------------------	-------

Допущено менее 10% ошибок при тестировании	81
Допущено менее 30% ошибок при тестировании	61
Допущено менее 50% ошибок при тестировании	41
Допущено более 50% ошибок при тестировании	0

### **Угрозы. Классификация и анализ угроз информационной безопасности**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

<b>Показатели оценивания</b>	<b>Баллы</b>
представить доклад по теме дисциплины	12
уметь определять вероятность реализации угроз	9
знать типы угроз и уметь их классифицировать	9

### **Причины, виды, каналы утечки и искажения информации**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

<b>Показатели оценивания</b>	<b>Баллы</b>
Представить доклад по теме дисциплины	12
Знание каналов утечки информации. Умение выявлять причину и источники технических каналов утечки информации	9
Знание видов защиты информации, способов их применения и реализации.	9

### **Итоговое контрольное мероприятие**

Продолжительность проведения мероприятия промежуточной аттестации: **6 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знать: Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. Методологические подходы к оценке уязвимости информации.	10
Знать: Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.	10
Знать основы нормативно-правовой базы в области защиты информации, иерархию	

законодательных актов в области защиты информации	10
Знать: Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации. Методы определения требований к защите информации. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации. Требования к защите, определяемые структурой автоматизированной системы обработки данных. Требования к защите, обуславливаемые видом защищаемой информации. Требования, обуславливаемые взаимодействием пользователя с комплексом средств автоматизации. Анализ существующих методик определения требований к защите информации.	10