# Аннотация к рабочей программе дисциплины «Управление информационной безопасностью»

## Цель преподавания дисциплины

Целью преподавания дисциплины «Управление информационной безопасностью» является получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем.

## Задачи изучения дисциплины

- изучение основ управления информационной безопасности информационных систем (ИС);
- изучение и анализ классификации угроз информационной безопасности ИС;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- анализ оценочных стандартов в информационной безопасности;
- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;
- анализ методик и технологий управления рисками;
- изучение современных методов и средств анализа и управления рисками ИС компаний;
- анализ правовых мер обеспечения информационной безопасности;
- анализ организационных мер обеспечения безопасности компьютерных ИС;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в ИС;
- изучение основных юридических законов в области защиты информации.

**Компетенции, формируемые в результате освоения дисциплины**

Способен управлять проектом на всех этапах его жизненного цикла (УК-2)

Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели(УК-3)

Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки (УК-6)

Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности(ОПК-3)

Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи. (ОПК-5)

**Разделы дисциплины**

Основные понятия и анализ угроз информационной безопасности. Проблемы информационной безопасности сетей. Политика безопасности. Криптографическая защита информации. Технологии аутентификации. Технологии межсетевых экранов. Технологии защиты от вирусов. Требования к системам защиты информации. Основы правового обеспечения защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
*(наименование ф-та полностью)*

_____М.О. Таныгин
*(подпись, инициалы, фамилия)*

«31» 08 2021 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Управление информационной безопасностью
*(наименование дисциплины)*

ОПОП ВО 10.04.01 Информационная безопасность
*(шифр согласно ФГОС и наименование направления подготовки (специальности))*

направленность (профиль, специализация) «Защищённые информационные системы»
*наименование направленности (профиля, специализации)*

форма обучения очная
*( очная, очно-заочная, заочная)*

Курск – 2021

Рабочая программа дисциплины Управление информационной безопасностью составлена в соответствии с ФГОС ВО – магистрат по направлению подготовки (специальности) 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, одобренного Ученым советом университета (протокол № 6 «26» 07 2022г.).

Рабочая программа дисциплины Управление информационной безопасностью обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность Защищённые информационные системы на заседании кафедры информационной безопасности Протокол № 1 «30» 08 2022г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.воен.н., доцент Ханис А.Л.
Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Управление информационной безопасностью пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, одобренного Ученым советом университета протокол № 8

«28» 02 2023 г., на заседании кафедры ИБ №11 от 30.06.2022.
*(наименование кафедры, дата, номер протокола)*

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины Управление информационной безопасностью пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, одобренного Ученым советом университета протокол № 7

«28» 02 2022г., на заседании кафедры ИБ протокол №1 от 30.08.2023г.
*(наименование кафедры, дата, номер протокола)*

Зав. кафедрой

## 1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

### 1.1 Цель дисциплины

Целью преподавания дисциплины «Управление информационной безопасностью» является получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем.

### 1.2 Задачи дисциплины

- изучение основ управления информационной безопасности информационных систем (ИС);
- изучение и анализ классификации угроз информационной безопасности ИС;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- анализ оценочных стандартов в информационной безопасности;
- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;
- анализ методик и технологий управления рисками;
- изучение современных методов и средств анализа и управления рисками ИС компаний;
- анализ правовых мер обеспечения информационной безопасности;
- анализ организационных мер обеспечения безопасности компьютерных ИС;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;

- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;

- изучение основных требований и рекомендаций по защите информации в ИС;

- изучение основных юридических законов в области защиты информации.

## 1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| УК-2 | Способен управлять проектом на всех этапах его жизненного цикла. | УК-2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления. | ***Знать***: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования ИС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ИС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью. ***Уметь:*** управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС. ***Владеть:*** навыками управления и |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС. |
| | | УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения. | ***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем)<br>***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | требований выполнения функциональных обязанностей инженерно-техническим персоналом. |
| | | УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости | ***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС, этапы разработки типовой прикладной ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем.<br>***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта.<br>***Владеть:*** навыками организации выполнения работ в рамках |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | проектов по разработке прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов. |
| | | УК-2.4 Разрабатывает план реализации проекта с использованием инструментов планирования. | ***Знать:*** требования к разработке проектной и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру, архитектуру и состав типовых защищённых ИС, этапы разработки типовой защищённой ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации.<br>***Уметь***: организовать выполнение работ в рамках проекта по разработке защищённых ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и планово-экономических документов, разрабатывать плановые документы, сетевые графики, рассчитывать нагрузку персонала |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | в соответствии с должностными обязанностями.<br>***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке защищённых ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных документов; разработки плановых документов, сетевых графиков, расчёта нагрузки персонала в соответствии с должностными обязанностями. |
| | | УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта. | ***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС, этапы разработки типовой прикладной ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации.<br>***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | изменения в план реализации проекта, устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта.<br>***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и изменения в план реализации проекта, устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов, применения средств контроля и мониторинга бесперебойного функционирования защищённых ИС. |
| УК-3 | Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели. | УК-3.1 Вырабатывает стратегию сотрудничества и на ее основе организует отбор членов команды для достижения поставленной цели. | ***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. |
| | | УК-3.2 Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов. | ***Знать***: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования защищённых ИС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке защищённых ИС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | хозяйственной деятельностью.<br>***Уметь:*** управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС, корректировать и планировать работу персонала в зависимости от поставленных задач и профессиональных навыков членов команды.<br>***Владеть:*** навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС, корректировки и планирования работы персонала в зависимости от поставленных задач и профессиональных навыков членов команды.. |
| | | УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон. | ***Знать:*** классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых защищенных ИС предприятий; основы управления ИС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ИС; понятие, типы, примеры архитектур ИС, принципы работы ИС; типовые архитектуры ИС с точки зрения программно-аппаратной реализации; классификацию архитектур; особенности проектирования распределённых систем; методы и средства защиты |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | информации в ИС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС.<br>***Уметь:*** проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ИС; оценку вариантов предлагаемых к реализации архитектур ИС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ИС; формировать требования к структуре ИС исходя из решаемых задач; разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ИС.<br>***Владеть:*** навыками сравнительного анализа технических средств и оборудования из состава прикладных ИС, оценки предлагаемых к реализации вариантов построения прикладных ИС, выбора оптимальной архитектуры прикладной ИС исходя из решаемых системой задач, разрешения конфликтных ситуаций в ходе выполнения работ по разработке защищённых ИС. |
| | | УК-3.4 Организует дискуссии по | ***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям. | информационной безопасности ИС.<br>***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС.<br>***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС, организации обсуждений результатов работы команды с привлечением оппонентов разработанным идеям в рамках создания защищённых ИС. |
| | | УК-3.5<br>Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. | ***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем)<br>***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. |
| УК-6 | Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки. | УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. | ***Знать:*** классификацию программно-аппаратных и телекоммуникационных средств защиты, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации.<br>***Уметь:*** проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | программных и аппаратных средств для построения инфо-коммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации.<br>***Владеть:*** навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации. |
| | | УК-6.2<br>Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. | ***Знать:*** методы профессионального развития и совершенствования собственной деятельности.<br>***Уметь:*** определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.<br>***Владеть:*** навыками определения приоритетов профессионального роста и способов совершенствования собственной деятельности. |
| | | УК-6.3<br>Выстраивает гибкую профессиональную траекторию, используя инструменты | ***Знать:*** психологические основы и способы формирования профессиональной траектории с использованием инструментов непрерывного образования.<br>***Уметь:*** применять приемы и алгоритмы выстраивания гибкой |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. | профессиональной траектории. ***Владеть:*** навыками анализа профессиональной траектории с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. |
| ОПК-3 | Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности. | ОПК-3.2 Рассчитывает риски информационной безопасности. | ***Знать:*** классификацию, виды и типы угроз безопасности ИС, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования ИС; основные компоненты ИС, состав, структуры и принципы функционирования современных ИС, требования основных законов и нормативных документов в области безопасности ИС; методы, способы и методики анализа рисков безопасности ИС; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности ИС; основные принципы построения комплексной системы защиты ИС. ***Уметь:*** определять угрозы безопасности ИС, определять возможные риски нарушения безопасности функционирования ИС; определять состав, структуру и принципы функционирования современных ИС, анализировать требования основных законов и нормативных документов в |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | области безопасности ИС; применять методики анализа рисков безопасности ИС; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности ИС.<br>***Владеть:*** навыками анализа защищенности ИС; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности ИС, выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированных систем; методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты ИС, методами расчёта рисков ИБ ИС. |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности. | ***Знать:*** типовые архитектуры, модели, компоненты, интерфейсы, технические характеристики ИС, виды и методы проектирования ИС; способы конструирования, принципы проектирования, структуру, стадии и этапы разработки проекта, методы и способов управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства разработки проектов, конструкторской и технической документации.<br>***Уметь:*** выбирать архитектуры ИС, модели, компоненты, интерфейсы, технические характеристики ИС, применять методы проектирования ИС; применять методы для управления персоналом и проектом, разрабатывать техническую и конструкторскую документацию, применять программные средства для разработки проектов, конструкторской и технической документации.<br>***Владеть:*** навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС, методами и способами проектирования ИС; методами и методиками управления персоналом и проектами, применения программных средств разработки проектов, конструкторской и технической документации. |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности. | ***Знать:*** основные принципы организации технического, программного и информационного обеспечения защищенных ИС, методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений. ***Уметь:*** осуществлять выбор функциональной структуры системы обеспечения информационной безопасности, обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности, осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | обеспечения информационной безопасности.<br>***Владеть:*** навыками управления информационной безопасностью ИС, освоения, внедрения и сопровождения документации, в том числе и в команде; нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правового применения нормативного законодательства в данной сфере; поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы. |
| | | ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем. | ***Знать:*** этапы построения системы информационной безопасности ИС, условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации, классификацию угроз, основные направления защиты информации на объекте, последствия и виды несанкционированных действий с информацией, классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, оценки состояния степени защищённости информации, методы и методики оценки рисков информационной безопасности при использовании |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | программных средств и информационных систем управления, модели, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз.<br>***Уметь:*** применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы, применять типовые методики для получения характеристик рисков и угроз, использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками.<br>***Владеть:*** навыками анализа защищенности объекта информатизации, методами проведения анализа угроз информационной безопасности; разделения рисков на приемлемые и неприемлемые, оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками, разработки моделей угроз и нарушителей информационной безопасности ИС. |
| ОПК-5 | Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять | ОПК-5.1 Проводит патентные исследований, объектом которых могут являться | ***Знать:*** методы и методики проведения и обработки результатов экспериментальных исследований, методы проведения обработки и оформления отчётной научно-технической |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи. | объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр. | документации (ОНТД), требования руководящих документов, ГОСТов. ***Уметь:*** применять требования стандартов и ГОСТов для проведения патентных исследований, разработки содержательной части и оформления ОНТД, в том числе отчётов о проведении патентные исследований, выбирать правильный метод обработки экспериментальных данных и оценивать его результаты, соблюдать правила оформления докладов, статей по результатам исследований. ***Владеть:*** навыками обработки данных экспериментальных исследований и оформления ОНТД, анализа научной документации, разработки отчётов о проведении патентных и научных исследований в соответствии с требованиями ГОСТов, нормативных и руководящих документов. |
| | | ОПК-5.2 Составляет отчеты о научных исследованиях. | ***Знать:*** требования руководящих документов, ГОСТов проведения НИР, методы и методики проведения научных исследований и обработки результатов экспериментальных исследований, методы анализа, обработки научного материала и оформления отчётной научно-технической документации (ОНТД). ***Уметь:*** разрабатывать ОНТД в соответствии с требованиями руководящих документов, ГОСТов на проведение НИР, применять методы анализа, |

| *Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)* | | *Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной* | *Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций* |
|---|---|---|---|
| *код компетенции* | *наименование компетенции* | | |
| | | | обработки научного материала и оформления отчётной научно-технической документации (ОНТД).<br>***Владеть:*** навыками обработки данных экспериментальных исследований и оформления ОНТД, анализа научной документации, разработки отчётов о проведении патентных и научных исследований в соответствии с требованиями ГОСТов на НИР, нормативных и руководящих документов. |

## 2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Управление информационной безопасностью», входит в обязательную часть блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы магистратуры (специалитета, бакалавриата) 10.04.01 Информационная безопасность, направленность Защищённые информационные системы. Дисциплина изучается на 1 курсе во 2 семестре.

## 3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 - Объём дисциплины

| Виды учебной работы | Всего, часов |
|---|---|
| Общая трудоемкость дисциплины | 180 |
| Контактная работа обучающихся с преподавателем по видам учебных занятий (всего) | 106 |

| Виды учебной работы | Всего, часов |
|---|---|
| в том числе: | |
| лекции | 30 |
| лабораторные занятия | 30 |
| практические занятия | 46 |
| Самостоятельная работа обучающихся (всего) | 44,85 |
| Контроль (подготовка к экзамену) | 27 |
| Контактная работа по промежуточной аттестации (всего АттКР) | 2,15 |
| в том числе: | |
| зачет | не предусмотрен |
| зачет с оценкой | не предусмотрен |
| курсовая работа (проект) | 2 |
| экзамен (включая консультацию перед экзаменом) | 0,15 |

## 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### 4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

| № п/п | Раздел, (тема) дисциплины | Содержание |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Основные понятия и анализ угроз информационной безопасности | Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы. |
| 2 | Проблемы информационной безопасности сетей | Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях. |

| | | |
|---|---|---|
| 3 | Политика безопасности | Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети: |
| 4 | Криптографическая защита информации | Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты. |
| 5 | Технологии аутентификации | Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутен-тификация пользователя. Аппаратно-программные системы идентификации и аутентификации. |
| 6 | Технологии межсетевых экранов | Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределен-ные межсетевые экраны. Проблемы безопасности межсетевых экранов. |

| | | |
|---|---|---|
| 7 | Технологии защиты от вирусов | Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети. |
| 8 | Требования к системам защиты информации | Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования. |
| 9 | Основы правового обеспечения защиты информации | Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности. |

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

| № п/п | Раздел (тема) дисциплины | Виды деятельности | | | Учебно-методические материалы | Формы текущего контроля успеваемости *(по неделям семестра)* | Компетенции |
|---|---|---|---|---|---|---|---|
| | | Лек. час | № лаб | № пр. | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Основные понятия и анализ угроз | 4 | - | - | У-1, У-2, У-3, | УО - 2 | УК-2, УК-3, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | информационной безопасности | | | | У-4, У-5, У-7, МУ-9 | | УК-6 |
| 2 | Проблемы информационной безопасности сетей | 4 | - | - | У-2, У-7, У-10, МУ-9 | УО - 4 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 3 | Политика безопасности | 3 | 1 | - | У-1, У-3, У-5, У-7, МУ-1, МУ-4 | УО-6, ЗЛР - 6 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 4 | Криптографическая защита информации | 4 | - | 1,2 | У-1, У-4, У-7, МУ-5, МУ-6, МУ-9 | УО – 8<br>ЗПР – 4,8 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 5 | Технологии аутентификации | 3 | - | - | У-4, У-6, У-7, У-10, МУ-9 | УО -10 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 6 | Технологии межсетевых экранов | 3 | - | - | У-1,У-2, У-4,У-6, У-9, У-10, МУ-9 | УО -12 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 7 | Технологии защиты от вирусов | 3 | - | 3 | У-2, У-4, У-8, У-9, У-10, МУ-7, МУ-9 | УО, ЗПР, ККР – 14 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 8 | Требования к системам защиты информации | 3 | 2,3 | - | У-1-6, У-10, МУ-2, МУ-3, МУ-4 | УО – 16<br>ЗЛР – 12,16<br>ККР – 12,16 | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 |
| 9 | Основы правового обеспечения защиты информации | 3 | - | 4 | У-1-7, МУ-8, МУ-9 | УО, ЗПР, ККР - 18 | УК-2, УК-3, УК-6, ОПК-3 |
| | Всего | 30 | 30 | 46 | | | |

УО – устный опрос, ЗЛР – лабораторная работа, ЗПР – практическая работа, ККР – контроль выполнения этапов курсовой работы.

### 4.2 Лабораторные работы и (или) практические занятия

#### 4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

| № п/п | Наименование лабораторной работы | Объем, час. |
|---|---|---|
| 1 | Система аудита информационной безопасности ГИС | 10 |
| 2 | Решение ситуационных задач (кейсов) | 10 |
| 3 | Основные методы управления информационной безопасностью в ГИС | 10 |
| Итого | | 30 |

### 4.2.2 Практические занятия

Таблица 4.2.2 - Практические занятия

| № п/п | Наименование практической работы | Объем, час. |
|---|---|---|
| 1 | Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение. | 10 |
| 2 | Определение показателей защищенности информации при несанкционированном доступе. | 12 |
| 3 | Критерии оценки и выбора CASE-средств. | 12 |
| 4 | Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности. | 12 |
| Итого | | 46 |

### 4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

| № раздела (темы) | Наименование раздела дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|---|---|---|---|
| 1 | Основные понятия и анализ угроз информационной безопасности | 2 неделя | 4,85 |
| 2 | Проблемы информационной безопасности сетей | 4 неделя | 5 |
| 3 | Политика безопасности | 6 неделя | 5 |
| 4 | Криптографическая защита информации | 8 неделя | 5 |
| 5 | Технологии аутентификации | 10 неделя | 5 |
| 6 | Технологии межсетевых экранов | 12 неделя | 5 |
| 7 | Технологии защиты от вирусов | 14 неделя | 5 |
| 8 | Требования к системам защиты информации | 16 неделя | 5 |
| 9 | Основы правового обеспечения защиты информации | 18 неделя | 5 |
| Итого | | | 44,85 |

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических работ и т.д.

*типографией университета:*

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

## 6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках

дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

| № | Наименование раздела (лекции, практического или лабораторного занятия) | Используемые интерактивные образовательные технологии | Объем в часах |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | Лекция №1. Основные понятия и анализ угроз информационной безопасности. | Анализ конкретных ситуаций | 1 |
| 2 | Лекция №2. Проблемы информационной безопасности сетей. | Анализ конкретных ситуаций | 1 |
| 3 | Лекция №3. Политика безопасности. | Анализ конкретных ситуаций | 1 |
| 4 | Лекция №8. Требования к системам защиты информации. | Анализ конкретных ситуаций | 1 |
| 5 | Практическое занятие №1. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение. | Анализ конкретных ситуаций | 2 |
| 6 | Практическое занятие №2. Определение показателей защищенности информации при несанкционированном доступе. | Анализ конкретных ситуаций | 2 |
| 7 | Практическое занятие №3. Критерии оценки и выбора CASE-средств. | Анализ конкретных ситуаций | 2 |
| Итого | | | 10 |

**Технологии использования воспитательного потенциала дисциплины**

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных и практических занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

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

### 7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

| Код и наименование компетенции | Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция | | |
|---|---|---|---|
| | начальный | основной | завершающий |
| 1 | 2 | 3 | 4 |

| | | | |
|---|---|---|---|
| УК-2. Способен управлять проектом на всех этапах его жизненного цикла. | Экономика и управление. | Экономика и управление. | Подготовка к процедуре защиты и защита выпускной квалификационной |
| УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной | Управление разработкой систем безопасности. | Управление разработкой систем безопасности. | Управление разработкой систем безопасности. Подготовка к процедуре защиты и защита выпускной |
| УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки. | Управление разработкой систем безопасности. | Управление разработкой систем безопасности. Технологии обеспечения информационной безопасности | Управление разработкой систем безопасности. Подготовка к процедуре защиты и защита выпускной квалификационной |
| ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной | | | Производственная проектно-технологическая практика. Подготовка к процедуре защиты и защита выпускной |
| ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных | Производственная практика (научно-исследовательская работа). | Производственная практика (научно-исследовательская работа). | Производственная практика (научно-исследовательская работа). Подготовка к процедуре защиты и защита выпускной квалификационной работы. |

## 7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

| Код компетенции/ этап (указывается название этапа из п.7.1) | Показатели оценивания компетенций *(индикаторы достижения компетенций,* | Критерии и шкала оценивания компетенций | | |
|---|---|---|---|---|
| | | Пороговый (удовлетворительно) | Продвинутый (хорошо) | Высокий (отлично) |

| | | | | |
|---|---|---|---|---|
| | *закрепленные за дисциплиной)* | | | |
| 1 | 2 | 3 | 4 | 5 |
| УК-2, завершающий. | УК-2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления.<br><br>УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, | Знать: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования ИС.<br>Уметь: управлять материальными, нематериальными, финансовыми ресурсами.<br>Владеть: навыками управления и распределения материальными, нематериальными, финансовыми ресурсами.<br><br>Знать: нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ. | Знать: порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ИС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления.<br>Уметь: управлять инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС.<br>Владеть: навыками применения инструментов и оборудования необходимыми для выполнения работ по проектированию ИС.<br>Знать: требования к разработке алгоритмов, программных средств, параметры и характеристики | Знать: программные продукты и системы управления хозяйственной деятельностью.<br>Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, управлять инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС.<br>Владеть: навыками применения программных средств защиты информации, применения инструментов и оборудования необходимыми для выполнения работ по проектированию ИС.<br><br>Знать: параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой |

| | | | | |
|---|---|---|---|---|
| | обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.<br><br>УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости. | Уметь: организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта.<br>Владеть: навыками организации, распределения, контроля и выполнения задач по проектированию ИС.<br><br>Знать: требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС.<br>Уметь: организовать выполнение работ в рамках проекта по разработке прикладных ИС.<br>Владеть: | покупных комплектующих изделий, спецификации комплектующих компьютерных средств.<br>Уметь: осуществлять контроль выполнения работ, проверять, разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ.<br>Владеть: навыками проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.<br>Знать: этапы разработки типовой прикладной ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала.<br>Уметь: контролировать выполнение задач персоналом на соответствие требованиям ТЗ, | ИС; функциональные обязанности руководителя проекта и персонала.<br>Уметь: Контролировать и требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>Владеть: навыками проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом, разработки цели, задач, актуальности, значимости ожидаемых результатов проекта.<br><br>Знать: нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы |

| | | | | |
|---|---|---|---|---|
| | | навыками организации выполнения работ в рамках проектов по разработке прикладных ИС. | других нормативных и юридических документов.<br>Владеть:<br>навыками контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов. | защищенности автоматизированных систем.<br>Уметь:<br>своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта.<br>Владеть:<br>навыками своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов. |
| | УК-2.4 Разрабатывает план реализации проекта с использованием инструментов планирования. | Знать:<br>требования к разработке проектной и планово-экономической документации, этапы и технологические циклы проведения работ по проекту.<br>Уметь:<br>организовать выполнение работ в рамках проекта по разработке защищённых ИС.<br>Владеть:<br>навыками организации выполнения работ в рамках проектов по разработке прикладных ИС. | Знать:<br>классификацию, номенклатуру, архитектуру и состав типовых защищённых ИС, этапы разработки типовой защищённой ИС.<br>Уметь:<br>контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и планово-экономических документов.<br>Владеть:<br>навыками контроля выполнения задач персоналом на соответствие | Знать:<br>сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации.<br>Уметь:<br>разрабатывать |

| | | | | |
|---|---|---|---|---|
| | УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта. | Знать: требования к разработке научно-технической и планово-экономической документации. Уметь: организовать выполнение работ в рамках проекта по разработке ИС. Владеть: навыками организации выполнения работ в рамках проектов по разработке ИС. | требованиям ТЗ, других нормативных и юридических документов. Знать: этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС, этапы разработки типовой ИС. Уметь: контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов. Владеть: навыками контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов. | плановые документы, сетевые графики, рассчитывать нагрузку персонала в соответствии с должностными обязанностями. Владеть: навыками разработки плановых документов, сетевых графиков, расчёта нагрузки персонала в соответствии с должностными обязанностями. Знать: сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации. Уметь: своевременно вносить коррективы в разработанную документацию и изменения в план реализации проекта, устранять замечания, недостатки и несоответствия, |

| | | | | |
|---|---|---|---|---|
| | | | | выявленные в ходе выполнения работ проекта.<br>Владеть:<br>навыками своевременного внесения корректив в разработанную документацию и изменения в план реализации проекта, устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов, применения средств контроля и мониторинга бесперебойного функционирования защищённых ИС. |
| УК-3, завершающий. | УК-3.1 Вырабатывает стратегию сотрудничества и на ее основе организует отбор членов команды для достижения поставленной цели. | Знать:<br>нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ.<br>Уметь:<br>организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта.<br>Владеть:<br>навыками организации, распределения, контроля и выполнения задач по проектированию ИС. | Знать:<br>требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования.<br>Уметь:<br>осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие | Знать:<br>компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала.<br>Уметь:<br>требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>Владеть:<br>навыками организации, распределения, контроля и выполнения задач по проектированию |

| | | | | |
|---|---|---|---|---|
| | | | требованиям ТЗ, нормативным документа, ГОСТ.<br>Владеть:<br>навыками проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. | ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. |
| | УК-3.2<br>Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов. | Знать:<br>сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования защищённых ИС.<br>Уметь:<br>управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС.<br>Владеть:<br>навыками организации, распределения, контроля и выполнения задач по | Знать:<br>порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке защищённых ИС.<br>Уметь:<br>корректировать и планировать работу персонала в зависимости от поставленных задач и профессиональных навыков членов команды.<br>Владеть:<br>навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС. | Знать:<br>знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью.<br>Уметь:<br>требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала.<br>Владеть:<br>навыками корректировки и планирования работы персонала в зависимости от поставленных задач и профессиональных |
| | УК-3.3<br>Разрешает конфликты и противореч | | | |

| | | | | |
|---|---|---|---|---|
| | ия при деловом общении на основе учета интересов всех сторон.<br><br>УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением | проектированию ИС.<br><br>Знать: классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых защищенных ИС предприятий.<br>Уметь: проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ИС защищённых ИС.<br>Владеть: навыками сравнительного анализа технических средств и оборудования из состава ИС.<br><br>Знать: | Знать: основы управления ИС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ИС; понятие, типы, примеры архитектур ИС, принципы работы ИС.<br>Уметь: оценку вариантов предлагаемых к реализации архитектур ИС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ИС; формировать требования к структуре ИС исходя из решаемых задач.<br>Владеть: оценки предлагаемых к реализации вариантов построения ИС.<br><br>Знать: порядок отладки | навыков членов команды.<br><br>Знать: типовые архитектуры ИС с точки зрения программно-аппаратной реализации; классификацию архитектур; особенности проектирования распределённых систем; методы и средства защиты информации в ИС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС.<br>Уметь: разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ИС.<br>Владеть: навыками выбора оптимальной архитектуры прикладной ИС исходя из решаемых системой задач, разрешения конфликтных ситуаций в ходе |

| | | | | |
|---|---|---|---|---|
| | оппонентов разработанным идеям.<br><br>УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. | порядок внедрения систем обеспечения информационной безопасности ИС.<br>Уметь:<br>организовать внедрение систем обеспечения информационной безопасности защищённых ИС.<br>Владеть:<br>навыками организации и управления внедрением систем обеспечения информационной безопасности защищённых ИС.<br><br>Знать:<br>нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ.<br>Уметь:<br>организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта.<br>Владеть:<br>навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по | систем обеспечения информационной безопасности ИС.<br>Уметь:<br>управлять систем обеспечения информационной безопасности защищённых ИС.<br>Владеть:<br>навыками организации и управления отладкой и этапами разработки систем обеспечения информационной безопасности защищённых ИС.<br>Знать:<br>требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств.<br>Уметь:<br>осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, | выполнения работ по разработке защищённых ИС.<br>Знать:<br>этапы разработки систем обеспечения информационной безопасности ИС.<br>Уметь:<br>организовать и управлять этапами разработки систем обеспечения информационной безопасности защищённых ИС.<br>Владеть:<br>навыками организации обсуждений результатов работы команды с привлечением оппонентов разработанным идеям в рамках создания защищённых ИС.<br><br>Знать:<br>параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС;<br>функциональные обязанности руководителя проекта и персонала.<br>Уметь: требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. |

| | | | | |
|---|---|---|---|---|
| | | проектированию защищённых ИС. | ГОСТ.<br>Владеть:<br>навыками проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. | Владеть:<br>навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом. |
| УК-6, завершающий. | УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. | Знать:<br>классификацию программно-аппаратных и телекоммуникационных средств защиты.<br>Уметь:<br>проводить анализ защищенности локальной вычислительной сети.<br>Владеть:<br>навыками выбора программно-аппаратных средств и телекоммуникационного оборудования. | Знать:<br>технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения вредоносных программ.<br>Уметь:<br>настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков.<br>Владеть:<br>навыками эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов. | Знать:<br>методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации.<br>Уметь:<br>определять оптимальный состав программных и аппаратных средств для построения инфо-коммуникационных сетей, применять действующие нормативные |

| | | | | |
|---|---|---|---|---|
| | | | | документы и юридические законы в области защиты информации.<br>Владеть:<br>навыками разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации. |
| | УК-6.2<br>Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. | Знать:<br>методы профессионального развития и совершенствования собственной деятельности.<br>Уметь:<br>определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.<br>Владеть:<br>навыками определения приоритетов профессионального роста и способов совершенствования собственной деятельности. | Знать:<br>методы профессионального развития и совершенствования собственной деятельности.<br>Уметь:<br>определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.<br>Владеть:<br>навыками определения приоритетов профессионального роста и способов совершенствования собственной деятельности. | Знать:<br>методы профессионального развития и совершенствования собственной деятельности.<br>Уметь:<br>определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.<br>Владеть:<br>навыками определения приоритетов профессионального роста и способов совершенствования собственной деятельности.. |
| | УК-6.3<br>Выстраивает гибкую профессиональную траекторию, используя инструменты | Знать:<br>психологические основы и способы формирования профессиональной траектории с использованием инструментов | Знать:<br>психологические основы и способы формирования профессиональной траектории с | |

| | | | | |
|---|---|---|---|---|
| | непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. | непрерывного образования.<br>Уметь:<br>применять приемы и алгоритмы выстраивания гибкой профессиональной траектории.<br>Владеть:<br>навыками анализа профессиональной траектории с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. | использованием инструментов непрерывного образования.<br>Уметь:<br>применять приемы и алгоритмы выстраивания гибкой профессиональной траектории.<br>Владеть:<br>навыками анализа профессиональной траектории с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. | Знать:<br>психологические основы и способы формирования профессиональной траектории с использованием инструментов непрерывного образования.<br>Уметь:<br>применять приемы и алгоритмы выстраивания гибкой профессиональной траектории.<br>Владеть:<br>навыками анализа профессиональной траектории с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда. |
| ОПК-3 | ОПК-3.2 Рассчитывает риски информационной безопасности. | Знать:<br>классификацию, виды и типы угроз безопасности ИС, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования ИС.<br>Уметь:<br>определять угрозы безопасности ИС, определять возможные риски нарушения | Знать:<br>основные компоненты ИС, состав, структуры и принципы функционирования современных ИС, требования основных законов и нормативных документов в области безопасности ИС.<br>Уметь:<br>определять | Знать:<br>методы, способы и методики анализа рисков безопасности ИС; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности ИС; |

| | | | | |
|---|---|---|---|---|
| | | безопасности функционирования ИС.<br>Владеть:<br>навыками анализа защищенности ИС; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности ИС. | состав, структуру и принципы функционирования современных ИС, анализировать требования основных законов и нормативных документов в области безопасности ИС.<br>Владеть:<br>навыками выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированных систем. | основные принципы построения комплексной системы защиты ИС.<br>Уметь:<br>принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности ИС.<br>Владеть:<br>методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты ИС, методами расчёта рисков ИБ ИС. |
| | ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности. | Знать:<br>типовые архитектуры, модели, компоненты, интерфейсы, технические характеристики ИС.<br>Уметь:<br>выбирать архитектуры ИС, модели, компоненты, интерфейсы, технические характеристики ИС.<br>Владеть: | Знать:<br>виды и методы проектирования ИС; способы конструирования, принципы проектирования, структуру, стадии и этапы разработки проекта.<br>Уметь: | Знать:<br>методы и способы управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства |

| | | | | |
|---|---|---|---|---|
| | | навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС. | применять методы проектирования ИС; применять методы для управления персоналом и проектом, разрабатывать техническую и конструкторску ю документацию. Владеть: методами и способами проектирования ИС. | разработки проектов, конструкторской и технической документации. Уметь: разрабатывать техническую и конструкторскую документацию, применять программные средства для разработки проектов, конструкторской и технической документации. Владеть: методами и методиками управления персоналом и проектами, применения программных средств разработки проектов, конструкторской и технической документации. Знать: использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности. Владеть: |
| | ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности. | Знать: основные принципы организации технического, программного и информационного обеспечения защищенных ИС. Уметь: осуществлять выбор функциональной структуры системы обеспечения информационной безопасности, обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. Владеть: навыками управления информационной безопасностью ИС, освоения, внедрения | Знать: методы концептуального проектирования технологий обеспечения информационно й безопасности; основные нормативные правовые акты в области информационно й безопасности и защиты информации. Уметь: организовывать работы по совершенствова нию, модернизации и унификации технологий обеспечения | |

| | | | | |
|---|---|---|---|---|
| | ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем. | и сопровождения документации, в том числе и в команде.<br><br>Знать:<br>этапы построения системы информационной безопасности ИС, условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации.<br>Уметь:<br>применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы.<br>Владеть:<br>навыками анализа защищенности объекта информатизации. | информационной безопасности, осуществлять выбор функциональной структуры системы обеспечения информационной безопасности.<br>Владеть:<br>навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов.<br>Знать:<br>классификацию угроз, основные направления защиты информации на объекте, последствия и виды несанкционированных действий с информацией, классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, оценки состояния степени защищённости информации. | знаниями в области правового обеспечения информационной безопасности и навыками правового применения нормативного законодательства в данной сфере; поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы.<br><br>Знать:<br>методы и методики оценки рисков информационной безопасности при использовании программных средств и информационных систем управления, модели, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз.<br>Уметь:<br>использовать |

| | | | | |
|---|---|---|---|---|
| | | | Уметь: применять типовые методики для получения характеристик рисков и угроз. Владеть: методами проведения анализа угроз информационной безопасности; разделения рисков на приемлемые и неприемлемые. | основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками. Владеть: навыками оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками, разработки моделей угроз и нарушителей информационной безопасности ИС. |
| ОПК-5 | ОПК-5.1 Проводит патентные исследований, объектом которых могут являться объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы | Знать: методы и методики проведения и обработки результатов экспериментальных исследований. Уметь: применять требования стандартов и ГОСТов для проведения патентных исследований. Владеть: навыками обработки данных экспериментальных исследований и оформления | Знать: методы проведения обработки и оформления отчётной научно-технической документации ОНТД. Уметь: применять требования разработки содержательной части и оформления ОНТД, в том числе отчётов о проведении патентные | Знать: методы проведения обработки и оформления отчётной научно-технической документации, требования руководящих документов, ГОСТов. Уметь: выбирать правильный метод обработки экспериментальных данных и оценивать его результаты, соблюдать правила оформления |

| | | | | |
|---|---|---|---|---|
| | для ЭВМ и базы данных и др.), ноу-хау и пр.<br><br>ОПК-5.2 Составляет отчеты о научных исследованиях. | отчётной научно-технической документации (ОНТД).<br><br>Знать: требования руководящих документов, ГОСТов проведения НИР. Уметь: разрабатывать ОНТД в соответствии с требованиями руководящих документов. Владеть: навыками обработки данных экспериментальных исследований и оформления ОНТД. | исследований. Владеть: навыками анализа научной документации.<br><br>Знать: методы и методики проведения научных исследований и обработки результатов экспериментальных исследований. Уметь: разрабатывать ОНТД в соответствии с требованиями ГОСТов на проведение НИР. Владеть: навыками анализа научной документации. | докладов, статей по результатам исследований. Владеть: навыками проведения патентных и научных исследований в соответствии с требованиями ГОСТов, нормативных и руководящих документов.<br>Знать: методы анализа, обработки научного материала и оформления отчётной научно-технической документации. Уметь: применять методы анализа, обработки научного материала и оформления отчётной научно-технической документации ОНТД. Владеть: навыками разработки отчётов о проведении патентных и научных исследований в соответствии с требованиями ГОСТов на НИР, нормативных и руководящих документов. |

**7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в**

**процессе освоения основной профессиональной образовательной программы**

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

| № п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|---|---|---|---|---|---|---|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Основные понятия и анализ угроз информационной безопасности | УК-2, УК-3, УК-6 | Лекция, СРС | Вопросы для устного опроса | 1-3 | Согласно таблице 7.2 |
| 2 | Проблемы информационной безопасности сетей | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, СРС | Вопросы для устного опроса | 4-14 | Согласно таблице 7.2 |
| 3 | Политика безопасности | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, СРС, лабораторная работа №1 | Вопросы для устного опроса<br>КВЗЛР №1 | 15-17<br>1-4 | Согласно таблице 7.2 |
| 4 | Криптографическая защита информации | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, практические работы №1 №2, СРС | Вопросы для устного опроса<br>КВЗПР №1<br>КВЗПР №2 | 18-24<br>1 – 3<br>1 – 3 | Согласно таблице 7.2 |
| 5 | Технологии аутентификации | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, СРС | Вопросы для устного опроса | 25-30 | Согласно таблице 7.2 |
| 6 | Технологии межсетевых экранов | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, СРС | Вопросы для устного опроса | 31-33 | Согласно таблице 7.2 |
| 7 | Технологии защиты от вирусов | УК-2, УК-3, УК-6, ОПК-3, | Лекция, Практическая работа | Вопросы для устного опроса<br>КВЗПР №3, ТКР, | 34-41<br>1-5 | Согласно таблице 7.2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | ОПК-5 | №3, выполнение этапов курсовой работы, СРС | КРКр | | |
| 8 | Требования к системам защиты информации | УК-2, УК-3, УК-6 | Лекция, лабораторные работы №2,3, выполнение этапов курсовой работы, СРС | Вопросы для устного опроса<br>КВЗЛР №2, КВЗЛР №3, ТКР, КРКр | 42-46<br>1-4<br>1-4 | Согласно таблице 7.2 |
| 9 | Основы правового обеспечения защиты информации | УК-2, УК-3, УК-6, ОПК-3, ОПК-5 | Лекция, Практическая работа №4, выполнение этапов курсовой работы, СРС | Вопросы для устного опроса<br>КВЗПР №4, ТКР, КРКр | 47-60<br>1-4 | Согласно таблице 7.2 |

СРС – самостоятельная работа студента,
КВЗЛР – контрольные вопросы для защиты лабораторных работ,
КВЗПР - контрольные вопросы для защиты практических работ,
ТКР – темы курсовых работ,
КРКр – критерии оценки курсовых работ

## Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности автоматизированных систем.
3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Контрольные вопросы для защиты лабораторной работы №1:

«Система аудита информационной безопасности ГИС».

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие ИБ в России
6. Какой состав и организационная структура системы обеспечения информационной безопасности?
7. В чем заключается стандарт ISO 17799?
8. Опишите методику анализа рисков.

Контрольные вопросы для защиты практической работы №2

Определение показателей защищенности информации при несанкционированном доступе.

1. В чем заключаются основные принципы проектирования защищённых систем?
2. Перечислите показатели качества процесса проектирования.
3. Постановка проблемы комплексного обеспечения информационной безопасности защищённых систем.
4. Основы методологии многовариантного планирования процесса проектирования.
5. Методы и методики проектирования комплексных систем информационной безопасности от несанкционированного доступа.
6. Методы и методики оценки качества комплексных систем информационной безопасности.

Темы курсовых работ:

Проектирование защищенной информационной системы для предприятий нефтегазовой отрасли.

Проектирование защищенной информационной системы для органов местного самоуправления.

Проектирование защищенной информационной системы для предприятий банковской сферы.

Проектирование защищенной информационной системы для муниципальных предприятий.

Проектирование защищенной информационной системы для машиностроительной отрасли.

Проектирование защищенной информационной системы для энергетической отрасли.

Проектирование защищенной информационной системы для военизированной отрасли.

Проектирование защищенной информационной системы для строительной отрасли.

Проектирование защищенной информационной системы для металлургической отрасли.

Проектирование защищенной информационной системы для жилищно-коммунального хозяйства.

Разработка модели угроз образовательного учреждения.

Разработка модели угроз образовательного учреждения.

Разработка модели угроз медицинского учреждения.

Разработка модели угроз муниципального учреждения.

Разработка модели угроз коммерческой организации.

Разработка модели угроз банка.

Требования к структуре, содержанию, объёму, оформлению курсовых работ, процедуре защиты, а также критерии оценки определены в:

- стандарте СТУ 04.02.030-2017 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению»;

- положение П 02.016-2018 «О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающихся образовательных программ»;

- методических указаниях по выполнению курсовой работы.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

*Промежуточная аттестация* по дисциплине проводится в форме зачёта. Зачёт проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых

заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

*Умения, навыки (или опыт деятельности) и компетенции* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

## Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Руководитель, оценивая результаты создания системы безопасности, прежде всего, должен обратить внимание на:

А) Экономический эффект от внедрения системы.

Б) Функциональную полноту, адаптивность, корректность работы системы.

В) Эффективность использования системой существующей инфраструктуры.

Г) Степень достижения поставленных целей.

Задание в открытой форме:

1. Элементом архитектуры системы безопасности организации является…….

2. Архитектура информационных систем организации включает в себя……..

3. Формальное описание архитектуры предприятия впервые было сформулировано в……...

4. В системном проектировании существуют следующие уровни представления архитектуры ……

Задание на установление правильной последовательности.

Установите последовательность этапов проектирования и разработки защищённой ИС:

1. Внедрение

2. Эксплуатация и модификация

3. Разработка

4. Выявление требований

Задание на установление соответствия:

между ИТ- ресурсами защищённой ИС и описаниями функционирования её элементов

| | | | |
|---|---|---|---|
| 1 | Информация | А | Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию |
| 2 | Инфраструктура | Б | Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которые используются для принятия управленческих решений |
| 3 | Персонал | В | Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений |

| | | | |
|---|---|---|---|
| 4 | Приложения | Г | Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам |

между способами и видами информации

| | | | |
|---|---|---|---|
| 1 | По способу кодирования | А | Цифровая, аналоговая |
| 2 | По способу представления | Б | Визуальная, звуковая, документ |
| 3 | По способу обработки | В | Текстовая, графическая, числовая |
| 4 | По способу восприятия | Г | Непрерывная, дискретная |

Компетентностно-ориентированная задача:

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 100 узлов.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

### 7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|---|---|---|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Устный опрос по темам 1-3 | 1 | Доля правильных ответов от 50% до 90% | 2 | Доля правильных ответов более 90% |
| Устный опрос по темам 4-6 | 1 | Доля правильных ответов от 50% до 90% | 2 | Доля правильных ответов более 90% |
| Устный опрос по темам 7-9 | 1 | Доля правильных ответов от 50% до 90% | 2 | Доля правильных ответов более 90% |
| Практическая работа № 1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение» | 3 | Выполнил, доля правильных ответов от 50% до 90% | 7 | Выполнил, доля правильных ответов более 90% |
| Практическая работа № 2 «Определение показателей защищенности информации при несанкционированном доступе» | 3 | Выполнил, доля правильных ответов от 50% до 90% | 7 | Выполнил, доля правильных ответов более 90% |
| Практическая работа № 3 «Критерии оценки и выбора CASE-средств» | 3 | Выполнил, доля правильных ответов от 50% до 90% | 7 | Выполнил, доля правильных ответов более 90% |
| Лабораторная работа №1 «Система аудита информационной безопасности ГИС» | 4 | Выполнил, доля правильных ответов от 50% до 90% | 7 | Выполнил, доля правильных ответов более 90% |
| Лабораторная работа №2 «Решение ситуационных задач (кейсов)» | 4 | Выполнил, доля правильных ответов от 50% до 90% | 7 | Выполнил, доля правильных ответов более 90% |
| Лабораторная работа №3 «Основные методы управления | 4 | Выполнил, доля правильных ответов от 50% до | 7 | Выполнил, доля правильных ответов более 90% |

| | | | | |
|---|---|---|---|---|
| информационной безопасностью в ГИС» | | 90% | | |
| Итого | 24 | | 48 | |
| Посещаемость | 0 | | 16 | |
| Зачёт | 0 | | 36 | |
| Итого | 24 | | 100 | |

*Для промежуточной аттестации обучающихся*, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

## 8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

### 8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. : ил., табл. - Библиогр.: с. 188-195. - ISBN 978-5-7681-1196-0 : 290.00 р. - Текст : непосредственный.

2. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков ; Министерство науки и высшего образования Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с. : ил. - URL: http://biblioclub.ru/index.php?page=book&id=561238. (дата обращения 02.09.2021) . - Режим доступа: по подписке. – Текст : электронный.

3. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем [Электронный ресурс] : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. - 128 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=598665.

### 8.2 Дополнительная учебная литература

4. Безбогов, А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. – Режим доступа : http://window.edu.ru/resource/546/38546. - Текст: электронный.

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для студентов вузов, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с. – Текст : непосредственный.

6. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М. : Академия, 2009. - 416 с. – Текст : непосредственный.

7. Аверченков, В. И. Служба защиты информации: организация и управление : [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 02.09.2021). – Режим доступа: по подписке. - Текст : электронный.

8. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 02.09.2021). – Режим доступа: по подписке. – Текст : электронный.

9. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. П. Фисун. - Курск : ЮЗГУ, 2013 - Ч. 1 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 150 с.

10. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. П. Фисун. - Курск : ЮЗГУ, 2013 - Ч. 2 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 303 с.

### 8.3 Перечень методических указаний

1. Управление информационной безопасностью : методические указания по выполнению самостоятельных работ направления подготовки бакалавриата 10.03.01 «Информационная безопасность» для студентов всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 48 с. - Загл. с титул. экрана. - Текст : электронный.

2. Решение ситуационных задач (кейсов) : методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 7 с. - Загл. с титул. экрана. - Текст : электронный.

3. Основные методы управления информационной безопасностью в ГИС : методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 20 с. - Загл. с титул. экрана. - Текст : электронный.

4. Система аудита информационной безопасности ГИС : методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 14 с. - Загл. с титул. экрана. - Текст : электронный.

5. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 16 с.

6. Определение показателей защищенности информации при несанкционированном доступе [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 7 с.

7. Критерии оценки и выбора CASE-средств [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т; сост.: А. Л. Марухленко. – Курск : ЮЗГУ, 2017. - 10 с.

8. Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

9. Информационная безопасность : методические указания для самостоятельной работы по изучению дисциплины для направления подготовки (специальности) 02.03.03 «Математическое обеспечение и администрирование информационных систем» / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Курск : ЮЗГУ, 2021. - 17 с. - Загл. с титул. экрана. - Текст : электронный.

### 8.4 Другие учебно-методические материалы

**Периодические издания:**

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.» - http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компью терные системы» - http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

## 9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft [официальный сайт].
8. http://www.consultant.ru Компания «Консультант Плюс» [официальный сайт].

## 10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Управление информационной безопасностью» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические и лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Управление информационной безопасностью»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и

конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Управление информационной безопасностью» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Управление информационной безопасностью» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

## 11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программа анализа и управления информационными рисками “Гриф”.(свободное ПО).

Программа хранения паролей Password Commander (свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LAN-guard Network Security Scanner.

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр:

ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+

## 13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

*Для лиц с нарушением слуха* возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

*Для лиц с нарушением зрения* допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

*Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата,* на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

## 14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

| Номер изменения | Номера страниц | | | | Всего страниц | Дата | Основание для изменения и подпись лица, проводившего изменения |
|---|---|---|---|---|---|---|---|
| | Изме-нённых | Заменённых | Аннулированных | новых | | | |
| | | | | | | | |