Аннотация к рабочей программе дисциплины «Управление информационной безопасностью телекоммуникационных систем»

Цель преподавания дисциплины

Целью преподавания дисциплины «Управление информационной безопасностью телекоммуникационных систем» 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 осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1).

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

Способен при решении профессиональных задач организовывать защиту

информации ограниченного доступа в соответствии снормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности РоссийскойФедерации, Федеральной службы по техническому и экспортному контролю (ОПК-6).

Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасностителекоммуникационных систем и сетей (ОПК-9.1).

Разделы дисциплины

1 Основные понятия и анализ угроз информационной безопасности
2 Проблемы информационной безопасности сетей
3 Политика безопасности
4 Криптографическая защита информации
5 Технологии аутентификации
6 Технологии межсетевых экранов
7 Технологии защиты от вирусов
8 Требования к системам защиты информации
9 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)

«30» 06 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью телекоммуникационных систем

(наименование дисциплины)

ОПОП ВО 10.05.02Информационная безопасность телекоммуникационных систем

(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Управление безопасностью телекоммуникационных систем и сетей

наименование направленности (профиля, специализации)

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей, одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол № 11 «30» июня 2022 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы
к.т.н., доцент Ефремов М.А.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №_

«__»___20_г., на заседании кафедры_____ .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №_

«__»___ 20_ г., на заседании кафедры_____ .
(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 телекоммуникационных систем» 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-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	***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. ***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

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*		
			нагрузку персонала в соответствии с должностными обязанностями. ***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-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	***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) ***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разрабо-

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*		
			танную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
УК-2	Способен управлять проектом на всех этапах его жизненного цикла.	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. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на

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*		
			соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и изменения в план реализации проекта, устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***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.
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	ОПК-6.1 Разрабатывает модели угроз и модели нарушителя объекта информатизации.	***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

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*		
	службы по техническому и экспортному контролю.		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 программных средств и информационных систем управления, модели, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз. ***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. ***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

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*		
			угроз и нарушителей информационной безопасности ИС.
		ОПК-6.2 Формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа.	***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. ***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. ***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

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*		
			документации.
ОПК-9.1	Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей.	ОПК-9.1.1 Составляет отчеты по результатам проверок защищенности телекоммуникационных систем и сетей.	***Знать:*** требования руководящих документов, ГОСТов проведения НИР, методы и методики проведения проверок защищенности телекоммуникационных систем и сетей и обработки их результатов, методы анализа, обработки отчетов и оформления отчётной научно-технической документации (ОНТД). ***Уметь:*** разрабатывать ОНТД в соответствии с требованиями руководящих документов, ГОСТов на проведение НИР, применять методы анализа, обработки отчетов проверок и оформления отчётной научно-технической документации (ОНТД). ***Владеть:*** навыками обработки данных отчетов проверок и оформления ОНТД, анализа технической документации, разработки отчётов о проведении проверок защищенности телекоммуникационных систем и сетей в соответствии с требованиями ГОСТов на НИР, нормативных и руководящих документов.
		ОПК-9.1.2 Выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей.	***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

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*		
			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) ***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. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
		ОПК-9.1.3 Разрабатывает рекомендации по эксплуатации системы защиты информации.	***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** навыками

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*		
			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.
		ОПК-9.1.4 Оценивает рисков, связанных с осуществлением угроз 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

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*		
			основных законов и нормативных документов в 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. ***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.

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 специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, направленность (профиль, специализация) «Управление безопасностью телекоммуникационных систем и сетей. Дисциплина изучается на 5 курсе во 9 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.), 108 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	-
практические занятия	36
Самостоятельная работа обучающихся (всего)	35,9
Контроль (подготовка к экзамену)	-
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные криптосистемы 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 аутентификация 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 распределенные 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 информационной безопасности	4	-	-	У-1-5 МУ-1	УО - 2	УК-1 УК-2 ОПК-6 ОПК-9.1
2	Проблемы информационной безопасности сетей	4	-	-	У-1-5 МУ-1	УО - 4	УК-1 УК-2 ОПК-6 ОПК-9.1
3	Политика безопасности	4	-	-	У-1-5 МУ-1	УО-6	УК-1 УК-2 ОПК-6 ОПК-9.1
4	Криптографическая защита информации	4	-	1,2	У-1-5 МУ-1-5	УО – 8 ЗПР – 4,8	УК-1 УК-2 ОПК-6 ОПК-9.1
5	Технологии аутентификации	4	-	-	У-1-5 МУ-1	УО -10	УК-1 УК-2 ОПК-6 ОПК-9.1
6	Технологии межсетевых экранов	4	-	-	У-1-5 МУ-1	УО -12	УК-1 УК-2 ОПК-6 ОПК-9.1
7	Технологии защиты от вирусов	4	-	3	У-1-5 МУ-1-5	УО, ЗПР	УК-1 УК-2 ОПК-6 ОПК-9.1
8	Требования к системам защиты информации	4	-	-	У-1-5 МУ-1	УО – 16	УК-1 УК-2 ОПК-6 ОПК-9.1
9	Основы правового обеспечения защиты	4	-	4	У-1-5 МУ-1-5	УО, ЗПР -18	УК-1 УК-2 ОПК-6

	информации						ОПК-9.1
	Всего	36					

УО – устный опрос, ЗПР – практическая работа.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№ п/п	Наименование практической работы	Объем, час.
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	8
2	Определение показателей защищенности информации при несанкционированном доступе.	8
3	Критерии оценки и выбора CASE-средств.	10
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	10
Итого		36

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	3,9
2	Проблемы информационной безопасности сетей	4 неделя	4
3	Политика безопасности	6 неделя	4
4	Криптографическая защита информации	8 неделя	4
5	Технологии аутентификации	10 неделя	4
6	Технологии межсетевых экранов	12 неделя	4
7	Технологии защиты от вирусов	14 неделя	4
8	Требования к системам защиты информации	16 неделя	4
9	Основы правового обеспечения защиты информации	18 неделя	4
Итого			35,9

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 обо-

рудованием 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 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	Практическое занятие №1. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	Анализ конкретных ситуаций	4
2	Практическое занятие №2. Определение показателей защищенности информации при несанкционированном доступе.	Анализ конкретных ситуаций	4
3	Практическое занятие №3. Критерии оценки и выбора CASE-средств.	Анализ конкретных ситуаций	4
4	Практическое занятие №4. Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	Анализ конкретных ситуаций	6
Итого			18

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-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Системы искусственного интеллекта		Управление информационной безопасностью телекоммуникационных систем
УК-2. Способен управлять проектом на всех этапах его жизненного цикла.	Управление разработкой систем безопасности		Управление информационной безопасностью телекоммуникационных систем
ОПК-6. Способен при решении профессиональных задач	Организационное и правовое обеспечение информационной безопасности Управление информационной безопасно-		Производственная эксплуатационная практика

организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	стью телекоммуникационных систем	
ОПК-9.1. Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей.	Управление информационной безопасностью телекоммуникационных систем	Производственная эксплуатационная практика

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, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	***Знать:*** требования к разработке проектной и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, архитектуру и состав типовых защищённых ИС, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке. ***Уметь***: организовать выполнение работ в рамках проекта по разработке защищённых ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке защищённых ИС, расчёта нагрузки персонала в соответствии с должностными обязанностями.	***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, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, основные требования к системам защиты информации. ***Уметь***: организовать выполнение работ в рамках проекта по разработке защищённых ИС, контролировать выполнение задач персоналом на соответствие	***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. ***Уметь***: организовать выполнение работ в рамках проекта по разработке защищённых ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и планово-

			требованиям ТЗ, других нормативных и планово-экономических документов, разрабатывать плановые документы, сетевые графики. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке защищённых ИС, других нормативных документов; разработки плановых документов, сетевых графиков, расчёта нагрузки персонала в соответствии с должностными обязанностями.	экономических документов, разрабатывать плановые документы, сетевые графики, рассчитывать нагрузку персонала в соответствии с должностными обязанностями. ***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-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, программных средств, параметры и характеристики покупных комплектующих изделий, параметры и характеристики сетевого оборудования, функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проекти-	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ, программных средств, параметры и характеристики покупных комплектующих изделий, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС,	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты

		рованию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС.	задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.	и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию защищённых 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. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.

УК-2 Способен управлять проектом на всех этапах его жизненного цикла.	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, должностные обязанности руководителя проекта и инженерно-технического персонала, основные требования к системам защиты информации. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, своевременно вносить коррективы в разработанную документацию и изменения в план реализации проекта. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке прикладных ИС, применения средств контроля и мониторинга бесперебойного функционирования защищённых ИС.	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, 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***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно	***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. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и

			вносить коррективы в разработанную документацию и изменения в план реализации проекта. ***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; применения средств контроля и мониторинга бесперебойного функционирования защищённых ИС.	юридических документов, своевременно вносить коррективы в разработанную документацию и изменения в план реализации проекта, устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***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.
ОПК-6. Способен при решении профессиональных за-	ОПК-6.1 Разрабатывает модели угроз и модели нару-	***Знать:*** этапы построения системы информационной безопасности ИС, условия и факторы,	***Знать:*** этапы построения системы информационной безопасности ИС,	***Знать:*** этапы построения системы информационной безопасности ИС, условия и факторы,

дач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	шителя объекта информатизации.	приводящие к нарушению целостности, доступности и конфиденциальности информации, классификацию угроз, основные направления защиты информации на объекте, классификацию нарушителей, методы и методики оценки рисков информационной безопасности при использовании программных средств и информационных систем управления. ***Уметь:*** применять известные методики оценки угроз, применять типовые методики для получения характеристик рисков и угроз, использовать основные модели оценки рисков для получения количественных и качественных оценок рисков. ***Владеть:*** навыками анализа защищенности объекта информатизации, оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками.	условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации, классификацию угроз, основные направления защиты информации на объекте, , классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, модели, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз. ***Уметь:*** применять известные методики оценки угроз, анализировать и классифицировать угрозы, использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и про-	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 программных средств и информационных систем управления, модели, методы и методики оценки угроз и уязвимостей, инструментальные средства анализа угроз. ***Уметь:*** применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы, применять типовые методики для по-

			ектирования системы управления рисками. ***Владеть:*** навыками анализа защищенности объекта информатизации, оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками, разработки моделей угроз и нарушителей информационной безопасности ИС.	лучения 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. ***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-6.2 Формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа.	***Знать:*** типовые архитектуры, модели, компоненты, интерфейсы, методы и способов управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства разработки проектов, конструкторской и	***Знать:*** типовые архитектуры, модели, компоненты, интерфейсы, технические характеристики ИС; способы конструирования, принципы проектирования, структуру, стадии и этапы разработ-	***Знать:*** типовые архитектуры, модели, компоненты, интерфейсы, технические характеристики ИС, виды и методы проектирования ИС; способы конструирования, принципы проектирования, структуру, стадии и этапы разработки

		технической документации. ***Уметь:*** выбирать архитектуры ИС, характеристики ИС, разрабатывать техническую и конструкторскую документацию, конструкторской и технической документации. ***Владеть:*** навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС, применения программных средств разработки проектов.	ки проекта, методы и способов управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства разработки проектов, конструкторской и технической документации. ***Уметь:*** выбирать архитектуры ИС, модели, компоненты, интерфейсы, технические характеристики ИС, разрабатывать техническую и конструкторскую документацию, конструкторской и технической документации. ***Владеть:*** навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС, методами и методиками управления персоналом и проектами, применения программных средств разработки проектов, конструкторской и технической документации.	проекта, методы и способов управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства разработки проектов, конструкторской и технической документации. ***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. ***Владеть:*** навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС, методами и способами проектирования ИС; методами и методиками управления персоналом и проектами, применения программ-

				ных средств разработки проектов, конструкторской и технической документации.
ОПК-9.1 Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей.	ОПК-9.1.1 Составляет отчеты по результатам проверок защищенности телекоммуникационных систем и сетей.	***Знать:*** требования руководящих документов, ГОСТов проведения НИР, методы и методики проведения проверок защищенности телекоммуникационных систем и сетей и обработки их результатов. ***Уметь:*** составлять отчеты в соответствии с требованиями руководящих документов, ГОСТов на проведение НИР. ***Владеть:*** навыками обработки данных отчетов проверок и оформления отчетов.	***Знать:*** требования руководящих документов, ГОСТов проведения НИР, методы и методики проведения проверок защищенности телекоммуникационных систем и сетей и обработки их результатов, методы анализа, обработки отчетов и оформления отчётной научно-технической документации (ОНТД). ***Уметь:*** разрабатывать ОНТД в соответствии с требованиями руководящих документов, обработки отчетов проверок и оформления отчётной научно-технической документации (ОНТД). ***Владеть:*** навыками обработки данных отчетов проверок и оформления ОНТД, разра-	***Знать:*** требования руководящих документов, ГОСТов проведения НИР, методы и методики проведения проверок защищенности телекоммуникационных систем и сетей и обработки их результатов, методы анализа, обработки отчетов и оформления отчётной научно-технической документации (ОНТД). ***Уметь:*** разрабатывать ОНТД в соответствии с требованиями руководящих документов, ГОСТов на проведение НИР, применять методы анализа, обработки отчетов проверок и оформления отчётной научно-технической документации (ОНТД). ***Владеть:*** навыками обработки данных отчетов проверок и оформления ОНТД, анализа технической документации, разработки отчётов о проведении проверок защищенности

			ботки отчётов о проведении проверок защищенности телекоммуникационных систем и сетей в соответствии с требованиями ГОСТов на НИР, нормативных и руководящих документов.	телекоммуникационных систем и сетей в соответствии с требованиями ГОСТов на НИР, нормативных и руководящих документов.
	ОПК-9.1.2 Выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, требования к разработке программных средств, спецификации комплектующих компьютерных средств, функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ; требования к разработке программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, контракта; про-	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных 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) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять кон-

			верять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:***, навыками контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.	троль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
	ОПК-9.1.3 Разрабатывает рекомендации по эксплуатации системы защиты информации.	***Знать:*** отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС,	***Знать:*** отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** навыками организации и управления внедрением, отладкой и	***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием

			развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС,	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.
	ОПК-9.1.4 Оценивает рисков, связанных с осуществлением угроз безопасности.	***Знать:*** классификацию, виды и типы угроз безопасности ИС, основные компоненты ИС, состав, требования основных законов и нормативных документов в области безопасности ИС; методы, способы и методики анализа рисков безопасности ИС; классификацию основных источников угроз, комплекс мероприятий, основные принципы построения комплексной системы защиты ИС. ***Уметь:*** определять угрозы безопасности ИС, определять возможные риски нарушения безопасности функционирования ИС; определять основные источники угроз, направленные на повышение защищенности и снижения рисков нарушения безопасности ИС. ***Владеть:*** навыками анализа защищенно-	***Знать:*** классификацию, виды и типы угроз безопасности 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 построе-	***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; ос-

		сти ИС.	ния комплексной системы защиты ИС. ***Уметь:*** определять угрозы безопасности ИС, определять возможные риски нарушения безопасности функционирования ИС; анализировать требования основных законов и нормативных документов в области безопасности ИС; ***Владеть:*** навыками анализа защищенности ИС; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности ИС, 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	новные 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 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. ***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

			мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем.	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.

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-1, УК-2, ОПК-6, ОПК-9.1	Лекция, СРС	Вопросы для устного опроса	1-3	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, СРС	Вопросы для устного опроса	4-14	Согласно таблице 7.2
3	Политика безопасности	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, СРС,	Вопросы для устного опроса	15-17	Согласно таблице 7.2
4	Криптографическая защита информации	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, практические работы №1 №2, СРС	Вопросы для устного опроса КВЗПР №1 КВЗПР №2	18-24 1 – 3 1 – 3	Согласно таблице 7.2
5	Технологии аутентификации	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, СРС	Вопросы для устного опроса	25-30	Согласно таблице 7.2
6	Технологии межсетевых экранов	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, СРС	Вопросы для устного опроса	31-33	Согласно таблице 7.2
7	Технологии защиты от вирусов	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, Практическая работа №3, выполнение эта-	Вопросы для устного опроса КВЗПР №3,	34-41 1-5	Согласно таблице 7.2

			пов курсовой работы, СРС			
8	Требования к системам защиты информации	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, лабораторные работы №2,3, выполнение этапов курсовой работы, СРС	Вопросы для устного опроса	42-46	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	УК-1, УК-2, ОПК-6, ОПК-9.1	Лекция, Практическая работа №4, выполнение этапов курсовой работы, СРС	Вопросы для устного опроса КВЗПР №4,	47-60 1-4	Согласно таблице 7.2

СРС – самостоятельная работа студента,
КВЗПР - контрольные вопросы для защиты практических 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 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.

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, произ-

водственных 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	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 4-6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 7-9	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа № 1 «Оценка показателей качества функционирования ком-	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%

плексной системы защиты информации на предприятии: физическое проникновение»				
Практическая работа № 2 «Определение показателей защищенности информации при несанкционированном доступе»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа № 3 «Критерии оценки и выбора CASE-средств»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа № 4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.»	6	Выполнил, доля правильных ответов от 50% до 90%	10	Выполнил, доля правильных ответов более 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. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков ; Южный федеральный университет ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с. - URL: http://biblioclub.ru/index.php?page=book&id=561238. (дата обращения 16.02.2023). - Режим доступа: по подписке. – Текст : электронный.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : 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 "Программ-

ное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с. – Текст : непосредственный.

5. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 – Ч. 1. – 150 с. - Текст : электронный.

6. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - Ч. 2. - 303 с.- Текст : электронный.

8.3 Перечень методических указаний

1. Управление информационной безопасностью : методические указания по выполнению самостоятельных работ 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. - 17 с. - Текст : электронный.

2. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение : 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. - Текст : электронный.

3. Определение показателей защищенности информации при несанкционированном доступе : 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. - Текст : электронный.

4. Критерии оценки и выбора CASE-Средств : методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Текст : электронный.

5. Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности : 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. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. - 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 телекоммуникационных систем» 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 телекоммуникационных систем»: 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 телекоммуникационных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Управление информационной безопасностью телекоммуникационных систем» - 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 LANguard 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: ноутбукASUSX50VLPMD-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: обу-

чающийся 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
	Измененных	Заменённых	Аннулированных	новых			