

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 21.01.2024 12:53:48

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе дисциплины «Методы и средства защиты информации в системах электронного документооборота»

Цель преподавания дисциплины

Целью преподавания дисциплины «Методы и средства защиты информации в системах электронного документооборота» является формирование представления об электронном документе как новой сущности в правовых отношениях, предоставление студентам систематизированного подхода к проблеме использования систем электронного документооборота (ЭДО) и информационных систем (ИС) на основе предоставленных базовых сведений. Курс знакомит студентов с понятиями и методами защищенного ЭДО и направлен на приобретение студентами глубоких и всесторонних знаний по современным методам разработки и использования систем в области финансового документооборота с обеспечением юридической значимости обрабатываемой информации.

Задачи изучения дисциплины

- привитие обучаемым основ культуры обеспечения ИБ;
- формирование у обучающихся понимания роли процессов управления в обеспечении ИБ организаций, объектов и систем;
- ознакомление обучающихся с основными методами управления ИБ организаций, объектов и систем;
- обучение различным методам реализации процессов управления ИБ, направленных на эффективное управление ИБ конкретной организации.

Компетенции, формируемые в результате освоения дисциплины

Способен формировать проектные решения по созданию и модернизации защищённых информационных систем (ПК-1);

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах (ПК-2);

Способен управлять персоналом, обслуживающим защищённые информационные системы (ПК-6);

Способен контролировать защищённость информационных систем (ПК-9).

Разделы дисциплины

- 1 Введение «Методы и средства защиты информации в системах электронного документооборота»
- 2 Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.
- 3 Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.
- 4 Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.
- 5 Развитие международного законодательства в области защиты информации и информационной безопасности.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики


М.О. Таныгин
(подпись, инициалы, фамилия)

« 30 » 06 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты информации в системах электронного
документооборота
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Защищённые информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
очная, очно-заочная, заочная

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета (протокол № «26» 02 2024 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности № «30» 08 2024 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы к.т.н., доцент _____ Таныгин М.О.
(ученая степень и ученое звание, Ф.И.О.)

/Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ №11 от 30.06.2022 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «29» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета 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 «Методы и средства защиты информации в системах электронного документооборота» является формирование представления об электронном документе как новой сущности в правовых отношениях, предоставление студентам систематизированного подхода к проблеме использования систем электронного документооборота (ЭДО) и информационных систем (ИС) на основе предоставленных базовых сведений. Курс знакомит студентов с понятиями и методами защищенного ЭДО и направлен на приобретение студентами глубоких и всесторонних знаний по современным методам разработки и использования систем в области финансового документооборота с обеспечением юридической значимости обрабатываемой информации.

1.2 Задачи изучения дисциплины

Задачи изучения учебной дисциплины:

- привитие обучаемым основ культуры обеспечения ИБ;
- формирование у обучаемых понимания роли процессов управления в обеспечении ИБ организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления ИБ организаций, объектов и систем;
- обучение различным методам реализации процессов управления ИБ, направленных на эффективное управление ИБ конкретной организации.

Таким образом, дисциплина «Методы и средства защиты информации в системах электронного документооборота» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

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

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код комп-ии</i>	<i>наименование компетенции</i>		
ПК-1	Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	<p>Знать: Методику анализа проектной документации, выявляя ее составляющие и связи между ними.</p> <p>Уметь: Анализировать проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними.</p> <p>Владеть (или Иметь опыт деятельности): Навыками сбора, анализа и обработки информации о проектных документах на средства защиты информации.</p>
		ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем	<p>Знать: Методику анализа проектной документации, включая техническую и проектную документацию по вопросам создания защищённых информационных систем выявляя ее составляющие и связи между ними.</p> <p>Уметь: Анализировать техническую и проектную документацию по вопросам</p>

		создания защищённых информационных систем. Владеть (или Иметь опыт деятельности): Навыками сбора, анализа и обработки информации, включая проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними.
	ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации	Знать: Методику анализа характеристики проектируемых решений с требованиями защиты информации. Уметь: Анализировать характеристики проектируемых решений с требованиями защиты информации. Владеть (или Иметь опыт деятельности): Навыками сбора, анализа и обработки информации о характеристике проектируемых решений с требованиями защиты информации.
	ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	Знать: Методику анализа конфигурации и состава защищённых информационных систем. Уметь: Анализировать конфигурацию и состав защищённых информационных систем. Владеть (или Иметь опыт деятельности): навыками формирования конфигурации и состава защищённых информационных систем

ПК-2	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах	ПК-2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	<p>Знать: Методику анализа управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах</p> <p>Уметь: Анализировать управление работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах</p> <p>Владеть (или Иметь опыт деятельности): навыками управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах</p>
		ПК-2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах	<p>Знать: Методику анализа комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах</p> <p>Уметь: Анализировать комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах</p> <p>Владеть (или Иметь опыт деятельности): комплексом мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах</p>

		<p>ПК-2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем</p>	<p>Знать: Методику анализа управления процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем</p> <p>Уметь: Анализировать управление процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем</p> <p>Владеть (или Иметь опыт деятельности): навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем</p>
		<p>ПК-2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах</p>	<p>Знать: Методику анализа разработки организационно-распорядительных документов, регламентирующие порядок эксплуатации защищённых информационных системах</p> <p>Уметь: Анализировать организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах</p> <p>Владеть (или Иметь опыт деятельности): навыками в разработке организационно-распорядительных документов, регламентирующие порядок эксплуатации защищённых информационных системах</p>

ПК-6	Способен управлять персоналом, обслуживающим защищённые информационные системы	ПК-6.1 Формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы	<p>Знать: Методику анализа формирования цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы</p> <p>Уметь: Анализировать цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы</p> <p>Владеть (или Иметь опыт деятельности): навыками в формировании цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы</p>
		ПК-6.2 Формулирует трудовые задачи при проведении работ по развитию, модернизации защищённой информационно й системы	<p>Знать: Методику анализа формирования трудовых задач при проведении работ по развитию, модернизации защищённой информационной системы</p> <p>Уметь: Анализировать трудовые задачи при проведении работ по развитию, модернизации защищённой информационной системы</p> <p>Владеть (или Иметь опыт деятельности): навыками в формировании трудовых задачи при проведении работ по развитию, модернизации защищённой информационной системы</p>
		ПК-6.3 Формирует требования, предъявляемые потребителями к программным, программно-аппаратным и техническим	<p>Знать: Методику анализа формирующие требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации</p> <p>Уметь: Анализировать требования, предъявляемые</p>

		<p>средствам и системам защиты информации</p>	<p>потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации</p> <p>Владеть (или Иметь опыт деятельности): навыками формирования требований, предъявляемых потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации</p>
		<p>ПК-6.4</p> <p>Определяет порядок действий проведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p>	<p>Знать: Методику анализа порядка действий при проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p> <p>Уметь: Анализировать порядок действий при проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p> <p>Владеть (или Иметь опыт деятельности): навыками определения порядка действий проведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p>
		<p>ПК-6.5</p> <p>Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых</p>	<p>Знать: Методику анализа формирования отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации</p> <p>Уметь: Анализировать отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических</p>

		к системам защиты информации	документов, предъявляемых к системам защиты информации Владеть (или Иметь опыт деятельности): навыками в формировании отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации
ПК-9	Способен контролировать защищённость информационных систем	ПК-9.1 Разрабатывает методику оценки уровня защищённости информационной системы	Знать: Методику анализа оценки уровня защищённости информационной системы Уметь: Анализировать методику оценки уровня защищённости информационной системы Владеть (или Иметь опыт деятельности): методикой оценки уровня защищённости информационной системы
		ПК-9.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам	Знать: Методику анализа проведения оценки соответствия уровня защищённости требованиям политики безопасности и нормативным документам Уметь: Анализировать оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам Владеть (или Иметь опыт деятельности): навыками в проведении оценки соответствия уровня защищённости требованиям политики безопасности и нормативным документам

		ПК-9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы	<p>Знать: Методику анализа разработки системы мероприятий по оценке уровня защищённости информационной системы</p> <p>Уметь: Анализировать систему мероприятий по оценке уровня защищённости информационной системы</p> <p>Владеть (или Иметь опыт деятельности): навыками в разработке систем мероприятий по оценке уровня защищённости информационной системы</p>
		ПК-9.4 Определяет уязвимости защищённости телекоммуникационных систем и сетей	<p>Знать: Методику анализа уязвимости защищённости телекоммуникационных систем и сетей</p> <p>Уметь: Анализировать уязвимости защищённости телекоммуникационных систем и сетей</p> <p>Владеть (или Иметь опыт деятельности): навыками определения уязвимости защищённости телекоммуникационных систем и сетей</p>

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «» входит в базовую часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01.Информационная безопасность профиль «Защищённые информационные системы». Дисциплина «Методы и средства защиты информации в системах электронного документооборота» изучается на 2 курсе в 3 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 трудоёмкость (объём) дисциплины составляет 4 зачётные единицы, 144 часа

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоёмкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	
Самостоятельная работа обучающихся (всего)	34.85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

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	Раздел (тема) Дисциплины	Содержание
1.	Введение «Методы и средства защиты информации в системах электронного документооборота»	Введение в дисциплину. Основные понятия и принципы электронного документооборота. Предмет, цель и задачи курса. Основные термины и определения. Этапы документооборота. Представление о системе

		электронного документооборота. Требования к системам электронного документооборота.
2.	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	Методы и средства защиты информации в СЭД. Основные виды защищаемой информации в системе электронного документооборота, виды документов ограниченного доступа. Уровни конфиденциальности. Угрозы безопасности информации в системах электронного документооборота. Основные требования и меры по защите информации. Защита от вредоносных программ.
3.	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.	Электронный регламент управления организацией. Проблема стандартизации метаданных и форматов в контексте реализации проекта «Электронного правительства». Юридическая сила электронного документа. Проблема защиты информации и информационной безопасности в системах электронного документооборота. Защита персональных данных в информационных системах. Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ.
4.	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	Защита электронных документов: целостность и конфиденциальность. Угрозы. Шифрование информации. Электронная подпись. Комплексный метод защиты. Проблемы распределения и хранения ключей. Организационные мероприятия.
5.	Развитие международного законодательства в области защиты информации и информационной безопасности.	Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ. Общегосударственные информационные системы. Федеральные целевые программы в области внедрения электронного документооборота.

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ Пп /п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек., час	№ лб.	№п р.			
1	2	3	4	5	6	7	8
1.	Введение «Методы и средства защиты информации в системах электронного документооборота»	6	-	1	У - 1-5 МУ – 1-5	С, ЗПР (1-2)	ПК-1, ПК-2, ПК-6, ПК-9.
2.	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	6	-	2	У - 1-5 МУ – 1-5	С, ЗПР (3-6)	ПК-1, ПК-2, ПК-6, ПК-9.
3.	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.	8	-	3	У - 1-5 МУ – 1-5	С, ЗПР (6-8)	ПК-1, ПК-2, ПК-6, ПК-9.
4.	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	8	-	4	У - 1-5 МУ – 1-5	С, ЗПР (8-10)	ПК-1, ПК-2, ПК-6, ПК-9.
5.	Развитие международного законодательства в области защиты информации и информационной безопасности.	8	-	5	У - 1-5 МУ – 1-5	С, ЗПР (11-12)	ПК-1, ПК-2, ПК-6, ПК-9.
	Итого	36	-	-			

С – собеседование, ЗПР – защита практической работы

4.2 Лабораторные работы и практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Семинар на тему «Механизмы обеспечения информационной безопасности электронных документов»	6
2.	Семинар на тему «Защищенные системы электронного	6

	документооборота»	
3.	Семинар на тему «Применение электронной подписи в системах электронного документооборота»	8
4.	Практическое занятие «Настройка межсетевое взаимодействия»	8
5.	Практическое занятие «ViPNet Деловая почта»	8
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение в спецкурс «Методы и средства защиты информации в системах электронного документооборота»	1-3 недели	6
2.	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	4-7 недели	6
3.	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации	8-11 недели	6
4.	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	12-15 недели	8
5.	Развитие международного законодательства в области защиты информации и информационной безопасности.	15-18 недели	8,85
Итого			34,85

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;
 - путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
 - путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных работ.
- типографией университета:
- путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;
 - путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

Образовательные технологии.

Реализация компетентного 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 не предусмотрено использование интерактивных технологий.

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 практических и (или) лабораторных 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

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен формировать проектные решения по созданию и модернизации защищённых информационных систем (ПК-1)	Технологии распределённых реестров Безопасность распределённых систем	Методы и средства защиты информации в системах электронного документооборота Теоретические основы компьютерной безопасности Управление разработкой систем безопасности	
Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах (ПК-2)	Организация работ по обеспечению безопасности в информационных системах	Технологии распределённых реестров Безопасность распределённых систем Производственная технологическая практика	
Способен управлять персоналом, обслуживающим защищённые информационные системы (ПК-6)	Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности		Производственная преддипломная практика
Способен контролировать защищённость информационных систем (ПК-9)	Методы и средства защиты информации в системах электронного документооборота Оценка защищённости информационных систем		Производственная проектно-технологическая практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (указываемся название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисциплиной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-1 / завершающий	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	Знать: Методику проектной документации. Уметь: Анализировать проектные документы на средства защиты информации. Владеть: Навыками сбора, информации о проектных документах на средства защиты информации.	Знать: Методику анализа проектной документации. Уметь: Анализировать проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему. Владеть: Навыками сбора, информации о проектных документах на средства защиты информации.	Знать: Методику анализа проектной документации, выявляя ее составляющие и связи между ними. Уметь: Анализировать проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними. Владеть: Навыками сбора, анализа и обработки информации о проектных документах на средства защиты информации.
	ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых	Знать: Методику анализа проектной документации по вопросам создания защищённых	Знать: Методику анализа проектной документации касающейся техническую документацию по	Знать: Методику анализа проектной документации касающейся техническую и проектную документацию по

	информационных систем	<p>информационных систем выявляя ее составляющие и связи между ними.</p> <p>Уметь: Анализировать документацию по вопросам создания защищённых информационных систем.</p> <p>Владеть: Навыками сбора, информации касающуюся проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними.</p>	<p>вопросам создания защищённых информационных систем выявляя ее составляющие и связи между ними.</p> <p>Уметь: Анализировать техническую документацию по вопросам создания защищённых информационных систем.</p> <p>Владеть: Навыками сбора, анализа и информации касающуюся проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними.</p>	<p>вопросам создания защищённых информационных систем выявляя ее составляющие и связи между ними.</p> <p>Уметь: Анализировать техническую и проектную документацию по вопросам создания защищённых информационных систем.</p> <p>Владеть: Навыками сбора, анализа и обработки информации касающуюся проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей как систему, выявляя ее составляющие и связи между ними.</p>
ПК-1.3	Сопоставляет характеристики проектируемых решений с требованиями защиты информации	<p>Знать: Методику анализа характеристики проектируемых решений.</p> <p>Уметь: Анализировать характеристики проектируемых решений.</p> <p>Владеть: Навыками сбора информации о характеристике проектируемых решений с требованиями</p>	<p>Знать: Методику анализа характеристики проектируемых решений с требованиями защиты информации.</p> <p>Уметь: Анализировать характеристики проектируемых решений с требованиями защиты информации.</p> <p>Владеть:</p>	<p>Знать: Методику анализа характеристики проектируемых решений с требованиями защиты информации.</p> <p>Уметь: Анализировать характеристики проектируемых решений с требованиями защиты информации.</p> <p>Владеть: Навыками</p>

		защиты информации.	Навыками сбора, анализа и обработки информации о характеристике проектируемых решений с требованиями защиты информации.	сбора, анализа и обработки информации о характеристике проектируемых решений с требованиями защиты информации.
	ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	Знать: Методику анализа конфигурации. Уметь: Анализировать конфигурацию. Владеть: навыками формирования конфигурации.	Знать: Методику анализа состава защищённых информационных систем. Уметь: Анализировать состав защищённых информационных систем. Владеть: навыками формирования состава защищённых информационных систем.	Знать: Методику анализа конфигурации и состава защищённых информационных систем. Уметь: Анализировать конфигурацию и состав защищённых информационных систем. Владеть: навыками формирования конфигурации и состава защищённых информационных систем.
ПК-2 / завершающий	ПК-2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	Знать: Методику управления работой специалистов по созданию и эксплуатации средств защиты информации Уметь: <i>управлять</i> работой специалистов по созданию и эксплуатации средств защиты информации Владеть: навыками управления работой специалистов по созданию и эксплуатации	Знать: Методику управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах Уметь: <i>управлять</i> работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах Владеть:	Знать: Методику анализа управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах Уметь: Анализировать управление работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах Владеть: навыками

		средств защиты информации	навыками управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах
ПК-2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах		Знать: Методику анализа комплекса мер для защиты в защищённых информационных системах Уметь: определять комплекс мер для защиты в защищённых информационных системах Владеть: комплексом мер для защиты в защищённых информационных системах	Знать: Методику анализа комплекса мер для защиты в защищённых информационных системах Уметь: Анализировать комплекс мер для защиты в защищённых информационных системах Владеть: комплексом мер для защиты в защищённых информационных системах	Знать: Методику анализа комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах Уметь: Анализировать комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах Владеть: комплексом мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах
ПК-2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем		Знать: Методику анализа управления процессом анализа моделей угроз Уметь: Анализировать управление	Знать: Методику анализа управления процессом разработки моделей угроз Уметь: Анализировать управление	Знать: Методику анализа управления процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем

	ых систем	процессом анализа моделей угроз Владеть: навыками управления процессом анализа моделей угроз	процессом разработки моделей угроз Владеть: навыками управления процессом разработки моделей угроз	Уметь: Анализировать управление процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем Владеть: навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем
	ПК-2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	Знать: Методику разработки организационно-распорядительных документов Уметь: понимать организационно-распорядительные документы Владеть : навыками анализа организационно-распорядительных документов	Знать: Методику анализа разработки организационно-распорядительных документов Уметь: Анализировать организационно-распорядительные документы Владеть : навыками разработки организационно-распорядительных документов	Знать: Методику анализа разработки организационно-распорядительных документов, регламентирующие порядок эксплуатации защищённых информационных системах Уметь: Анализировать организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах Владеть : навыками разработки организационно-распорядительных документов, регламентирующие порядок эксплуатации защищённых информационных

				системах
ПК-6 / завершаю щий	ПК-6.1 Формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающе го информационн ые системы	Знать: Методику анализа формирования персонала Уметь: Анализировать цели, персонала, обслуживающего информационные системы Владеть: навыками в области теории персонала, обслуживающего информационные системы	Знать: Методику анализа формирования цели персонала, обслуживающего информационные системы Уметь: Анализировать цели, персонала, обслуживающего информационные системы Владеть: навыками в формировании цели, персонала, обслуживающего информационные системы	Знать: Методику анализа формирования цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы Уметь: Анализировать цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы Владеть: навыками в формировании цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы
	ПК-6.2 Формулирует трудо вые задачи при проведении работ по развитию, модернизации защищённой информационн ой системы	Знать: Методику трудо вых задачи при проведении работ по развитию защищённой информационной системы Уметь: Анализировать трудо вые задачи при проведении работ по развитию защищённой информационной системы Владеть: навыками анализа трудо вых задачи при проведении работ по	Знать: Методику трудо вых задачи при проведении работ по развитию, модернизации защищённой информационной системы Уметь: Анализировать трудо вые задачи при проведении работ по развитию, модернизации защищённой информационной системы Владеть: навыками анализа трудо вых задачи	Знать: Методику анализа формирования трудо вые задачи при проведении работ по развитию, модернизации защищённой информационной системы Уметь: Анализировать трудо вые задачи при проведении работ по развитию, модернизации защищённой информационной системы Владеть: формированием трудо вых задач при

		развитию защищённой информационной системы	при проведении работ по развитию, модернизации защищённой информационной системы	проведении работ по развитию, модернизации защищённой информационной системы
ПК-6.3 Формирует требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации	Знать: Методику анализа формирующие требования, предъявляемые потребителями к программно-аппаратным и техническим средствам Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным и техническим средствам Владеть: навыками формирования требований, предъявляемых потребителями к программно-аппаратным и техническим средствам	Знать: Методику анализа формирующие требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным и техническим средствам Владеть: навыками формирования требований, предъявляемых потребителями к программным, программно-аппаратным и техническим средствам	Знать: Методику анализа формирующие требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным и техническим средствам Владеть: навыками формирования требований, предъявляемых потребителями к программным, программно-аппаратным и техническим средствам	Знать: Методику анализа формирующие требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным и техническим средствам Владеть: навыками формирования требований, предъявляемых потребителями к программным, программно-аппаратным и техническим средствам
ПК-6.4 Определяет порядок действий проведения процедур сертификации	Знать: Методику анализа порядка действий проведения процедур и аттестации систем защиты и	Знать: Методику анализа порядка действий проведения процедур и аттестации средств и систем	Знать: Методику анализа порядка действий проведения процедур и аттестации средств и систем	Знать: Методику анализа порядка действий проведения процедур сертификации и аттестации средств и

	и аттестации средств и систем защиты и объектов информатизации	<p>объектов информатизации</p> <p>Уметь: Анализировать порядок действий проведении процедур и аттестации систем защиты и объектов информатизации</p> <p>Владеть: навыками анализа порядка действий проведении процедур сертификации систем защиты и объектов информатизации</p>	<p>защиты и объектов информатизации</p> <p>Уметь: Анализировать порядок действий проведении процедур и аттестации средств и систем защиты и объектов информатизации</p> <p>Владеть: навыками анализа порядка действий проведении процедур сертификации средств и систем защиты и объектов информатизации</p>	<p>систем защиты и объектов информатизации</p> <p>Уметь: Анализировать порядок действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p> <p>Владеть : навыками анализа порядка действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации</p>
ПК-6.5 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации	<p>Знать: Методику анализа формирования отчётов по изменению за выбранный период времени требований нормативных правовых актов</p> <p>Уметь: Анализировать отчёты по изменению за выбранный период времени требований нормативных правовых актов</p> <p>Владеть: навыками в формировании отчётов по изменению за выбранный период времени требований нормативных</p>	<p>Знать: Методику анализа формирования отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов</p> <p>Уметь: Анализировать отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов</p> <p>Владеть: навыками в формировании</p>	<p>Знать: Методику анализа формирования отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации</p> <p>Уметь: Анализировать отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты</p>	<p>Знать: Методику анализа формирования отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации</p> <p>Уметь: Анализировать отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты</p>

		правовых актов	отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов	информации Владеть: навыками в формировании отчётов по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации
ПК-9 / завершающих	ПК-9.1 Разрабатывает методику оценки уровня защищённости информационной системы	Знать: Методику анализа формирования персонала Уметь: Анализировать цели, персонала, обслуживающего информационные системы Владеть: навыками и теорией персонала, обслуживающего информационные системы	Знать: Методику анализа формирования цели персонала, обслуживающего информационные системы Уметь: Анализировать цели, персонала, обслуживающего информационные системы Владеть: навыками формирования цели, персонала, обслуживающего информационные системы	Знать: Методику анализа формирования цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы Уметь: Анализировать цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы Владеть: навыками формирования цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы
	ПК-9.2 Проводит оценку соответствия уровня защищённости требованиям политики	Знать: Методику формирования трудовых задач при проведении работ по развитию защищённой информационной	Знать: Методику анализа формирования трудовые задачи при проведении работ по развитию защищённой	Знать: Методику анализа формирования трудовые задачи при проведении работ по развитию, модернизации защищённой

	<p>безопасности и нормативным документам</p>	<p>системы Уметь: Анализировать трудовые задачи при проведении работ по модернизации защищённой информационной системы Владеть трудоыми задачами при проведении работ по модернизации защищённой информационной системы</p>	<p>информационной системы Уметь: Анализировать трудовые задачи при проведении работ по модернизации защищённой информационной системы Владеть в формировании трудоыми задачами при проведении работ по модернизации защищённой информационной системы</p>	<p>информационной системы Уметь: Анализировать трудовые задачи при проведении работ по развитию, модернизации защищённой информационной системы Владеть в формировании трудоыми задачами при проведении работ по развитию, модернизации защищённой информационной системы</p>
<p>ПК-9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы</p>	<p>Знать: Методику анализа формирующие требования, предъявляемые потребителями к программно-аппаратным средствам и системам защиты информации Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным средствам и системам защиты информации Владеть: навыками в формировании требований, предъявляемых потребителями к программно-аппаратным средствам и системам защиты</p>	<p>Знать: Методику анализа формирующие требования, предъявляемые потребителями к программно-аппаратным и техническим средствам и системам защиты информации Уметь: Анализировать требования, предъявляемые потребителями к программно-аппаратным и техническим средствам и системам защиты информации Владеть: навыками в формировании требований, предъявляемых потребителями к программно-аппаратным и</p>	<p>Знать: Методику анализа формирующие требования, предъявляемые потребителями к программно-аппаратным и техническим средствам и системам защиты информации Уметь: Анализировать требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации Владеть: навыками в формировании требований, предъявляемых потребителями к программным,</p>	<p>Знать: Методику анализа формирующие требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации Уметь: Анализировать требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации Владеть: навыками в формировании требований, предъявляемых потребителями к программным,</p>

		информации	техническим средствам и системам защиты информации	программно- аппаратным и техническим средствам и системам защиты информации
ПК-9.4 Определяет уязвимости защищённости телекоммуника- ционных систем и сетей	Знать: Методику анализа порядка действий проведении процедур сертификации систем защиты и объектов информатизации Уметь: Анализировать порядок действий проведении процедур сертификации систем защиты и объектов информатизации Владеть: навыками в определении порядка действий при проведении процедур сертификации систем защиты и объектов информатизации	Знать: Методику анализа порядка действий проведении процедур сертификации средств и систем защиты и объектов информатизации Уметь: Анализировать порядок действий проведении процедур сертификации средств и систем защиты и объектов информатизации Владеть: навыками в определении порядка действий при проведении процедур сертификации средств и систем защиты и объектов информатизации	Знать: Методику анализа порядка действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации Уметь: Анализировать порядок действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации Владеть: навыками в определении порядка действий при проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации	

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.	Введение в спецкурс «Методы и средства защиты информации в системах электронного документооборота»	ПК-1, ПК-2, ПК-6, ПК-9.	СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл.7.2
2.	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	ПК-1, ПК-2, ПК-6, ПК-9.	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл.7.2
3.	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.	ПК-1, ПК-2, ПК-6, ПК-9.	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл.7.2
4.	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	ПК-1, ПК-2, ПК-6, ПК-9.	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл.7.2

5.	Развитие международного законодательства в области защиты информации и информационной безопасности.	ПК-1, ПК-2, ПК-6, ПК-9.	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл.7.2
----	---	-------------------------	----------------------------------	-------------	------------	-------------------

ВС- вопросы для собеседования

КВЗПР- контрольные вопросы для защиты практической работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по теме 1: Введение в курс «Методы и средства защиты информации в системах электронного документооборота.

1. Что такое система электронного документооборота?
2. Какая цель и задача курса?
3. Что такое электронно-цифровая подпись?
4. Какие существуют этапы документооборота?
5. Что такое документ?

Контрольные вопросы для защиты практической работы «Методы и средства защиты информации в системах электронного документооборота»

1. Что такое ЕСМ?
2. Что такое система электронного документооборота?
3. Назовите недостатки бумажного документооборота?
4. Что такое документооборот?
5. Назовите преимущества электронного документооборота?

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного 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:

Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

- 1) ФСТЭК России
- 2) ФСБ России
- 3) СВР России
- 4) МВД России
- 5) Роскомнадзор

Задание в открытой форме:

1. Документооборот – это...
2. Аутентификация – это...
3. Проверка подлинности пользователя по предъявленному им идентификатору — это:

Задание на установление правильной последовательности,

При подготовке к внедрению электронного документооборота необходимо

1. Анализ бизнес-процессов организации
2. Анализ возможных конфигураций аппаратно-программных средств, необходимых для внедрения СЭД
3. Состояние используемого оборудования и технологий
4. Разработка информационно-функциональной модели предприятия, реинжиниринг бизнес-процессов

Задание на установление соответствия:

Установите взаимно однозначное соответствие

1.	Целостность	А	свойство информации, гарантирующее, что доступ к информации имеет доступ только определенные лица.
2	Конфиденциальность	Б	свойство информации, гарантирующее, что только определенные лица могут менять информацию.
3	Доступность	В	свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ.

Компетентностно-ориентированная задача:

1) Добавить новый сетевой узел в защищенную сетевую инфраструктуру электронного документооборота. На узле создать 3-х пользователей с различными правами в системе, для двух из них выпустить ключи электронной подписи.

2) Настроить и описать все этапы установления межсетевого взаимодействия между двумя защищенными сетевыми инфраструктурами с электронным документооборотом.

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 «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
Выполнение практической работы №1 «Механизмы обеспечения информационной безопасности электронных документов»	2	Выполнил, доля правильных ответов менее 50%	4	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №2 «Защищенные системы электронного документооборота»	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №3 «Применение электронной подписи в системах электронного документооборота»	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №4 «Настройка межсетевого взаимодействия»	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №5 «ViPNet Деловая почта»	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил и доля правильных ответов более 50%
Собеседование по теме 1	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 2	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 3	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 4	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%

Собеседование по теме 5	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
ИТОГО	24		48	

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 литература

1) Безопасность электронного документооборота : учебное пособие / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 54 с. – URL: <https://biblioclub.ru/index.php?page=book&id=602225> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

2) Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: <https://biblioclub.ru/index.php?page=book&id=79551> (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная литература

3) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. – URL: <https://biblioclub.ru/index.php?page=book&id=276557> (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

4) Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: <https://biblioclub.ru/index.php?page=book&id=208694> (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Настройка межсетевого взаимодействия : методические указания по выполнению лабораторных и практических работ для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, К. Г. Верютина. - Курск : ЮЗГУ, 2019. - 26 с. : ил., табл. - Загл. с титул. экрана. - Текст : электронный.

2) ViPNet Деловая почта : методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Администрирование защищенных телекоммуникационных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, А. А. Чеснокова. - Курск : ЮЗГУ, 2018. - 22 с. : ил. - Загл. с титул. экрана. - Текст : электронный.

3) Первичное развертывание сети ViPNet4 : методические указания по выполнению лабораторных и практических работ для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, К. Г. Верютина. - Курск : ЮЗГУ, 2019. - 42 с. : ил., табл. - Загл. с титул. экрана. - Текст : электронный.

4) Действия при изменениях в структуре сети ViPNet4 : методические указания по выполнению лабораторных и практических работ для студентов укрупненной группы специальностей 10.00.00. / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, К. Г. Верютина. - Курск : ЮЗГУ, 2019. - 27 с. : ил. - Загл. с титул. экрана. - Текст : электронный.

5) Анализ механизмов обеспечения информационной безопасности в системе электронного документооборота : методические указания по выполнению курсовой работы по дисциплине «Методы и средства защиты информации в системах электронного документооборота» для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, А. А. Татаринцева. - Курск : ЮЗГУ, 2017. - 28 с. - Загл. с титул. экрана. - Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

Использование информационных технологий по курсу на данный период предусматривает обязательное использование программного пакета «Консультант плюс», «Гарант».

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Методы и средства защиты информации в системах

электронного документооборота» являются лекции и практические 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 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.

Практическому 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 практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Методы и средства защиты информации в системах электронного документооборота»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов.

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 (собеседовании). 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 немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться, 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 «Методы и средства защиты информации в системах электронного документооборота» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Методы и средства защиты информации в системах электронного документооборота» - 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)

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, открытая среда разработки программного обеспечения Lazarus (Свободное ПО <http://www.lazarus.freepascal.org/>)

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 Тб, монитор Aок 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. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). 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, прочесть 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
	изменённых	заменённых	аннулированных	новых			