МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«20» сентября 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы
Обеспечение информационной безопасности распределенных информационных систем
наименование направленности (профиля) подготовки (специализации)

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
3.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
5.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
6.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1 Цели освоения дисциплины

Целью изучения дисциплины «Защита электронного документооборота» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации в системах электронного документооборота, анализом возможных угроз в информационной сфере и адекватных мер по их нейтрализации, совершенствование практических навыков по организации защиты информации в организациях, в том числе на предприятии и в учреждениях.

2 Место дисциплины в структуре образовательной программы подготовки специалиста

Дисциплина «Защита электронного документооборота» входит в вариативную часть блока 1 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Криптографические методы защиты информации», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Безопасность операционных систем».

Знания (умения, навыки), полученные при изучении данной дисциплины будут использоваться в научно-исследовательской работе, при прохождении производственной практики и выполнении ВКР.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «*Защита электронного документооборота*» обучающийся должен обладать следующими компетенциями: ПК-24; ПК-28; ПСК-7.5

Структурный элемент компетенции	**Планируемые результаты обучения**
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	− принципы построения и функционирования, примеры реализаций систем электронного документооборота; -методы и средства проектирования систем электронного документооборота; - основные принципы построения защищенных информационных систем, электронного документооборота; –критерии оценки защищенности систем электронного документооборота, источники угроз и нормативные документы; - информационные технологии, используемые в автоматизированных системах; - нормативные правовые акты в области защиты информации; − возможности, классификацию и область применения макрообработки;
Уметь:	-применять современные информационные технологии для прохождения, обработки, учета и рассылки документов внутри организации с учетом требований информационной безопасности; -разрабатывать техническую документацию для систем защиты электронного документооборота; -готовить научно-технические отчеты, обзоры, публикации по теме предметной области;
Владеть:	-навыками применения современных информационных технологий для прохождения, обработки, учета документов внутри организации с учетом требований информационной безопасности; навыками разработки технической документации для систем защитыэлектронного документооборота; -навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области;
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	

Структурный элемент компетенции	**Планируемые результаты обучения**
Знать	-основные методы управления информационной безопасностью; -процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы; принципы формирования политики информационной безопасности автоматизированных систем
Уметь:	- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации;
Владеть:	-навыками построения моделей угроз системы электронного документооборота; -методами управления информационной безопасностью для решения задач управления информационной безопасностью систем электронного документооборота; - навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем;
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	
Знать	-мероприятия по обеспечению безопасности распределенных информационных систем; методы организации работы по обеспечению защиты информации в распределенных информационных системах; -организационные меры по защите информации с системах ЭДО; -законодательные акты, стандарты по защите информации в системах ЭДО;
Уметь:	-выбирать методы и подходы к проектированию средств защиты СЭДО на предприятии; -выявлять особенности и формировать требования безопасности к системе организации коллективной работы с документами в режиме совместного доступа и передачи их на исполнение по электронной почте или по локальной сети; -составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы
Владеть:	-навыками администрирования систем электронного документооборота; -методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов; -научными основами и современными методиками обеспечения безопасности распределенной информационной системы

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет **4** зачетных единиц **144** акад. часов, в том числе:

- контактная работа – 72 акад. часов:
  - аудиторная – 68 акад. часов;
  - внеаудиторная – 4 кад. часов
- самостоятельная работа – 36,3 акад. часов;
- подготовка к экзамену – 35,7 акад. часа

Раздел/ тема дисциплины	**Аудиторная контактная работа (в акад. часах)**		сам ост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	лекции	практич. занятия				
Тема 1. Функции, задачи и особенности электронного документооборота. Тема 1.1 Основные понятия и принципы электронного документооборота. Теоретические и организационные основы создания систем электронного документооборота организации.	1	1	1,3	Поиск дополнительной информации по заданной теме	Опрос, тестирование	ПК-24 -зу
Тема 1.2. Методологические основы разработки информационной системы электронного документооборота.	0,5		1	Самостоятельное изучение учебной и научно литературы. ИДЗ	Опрос, тестирование, проверка ИДЗ	ПК-24 -зу ПК-28-з
Тема 1.3 Классификация систем электронного документооборота.	0,5		1	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Опрос, тестирование	ПК-24 -зув ПК-28-зу
Тема 2. Классификация угроз СЭД . Тема 2.1. Угроза конфиденциальности. Угроза доступа рабочих мест. Угроза доступа сервера ОС. Угроза сервера СЭД. Угроза перехвата каналов связи.	2	1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Опрос, тестирование, проверка ИДЗ	ПК-24 -зув ПК-28-зув
Тема 2.2.Угрозы целостности и доступности СЭДО. Угроза доступа сервера ОС. Угроза сервера СЭД. Контроль целостности электронного документа.	2	1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Опрос, коллоквиум	ПК-24 -зув ПК-28-зув
Тема 3. Источники угроз СЭДО. Внешние и внутренние источники угроз. Методы и средства защиты от внешних и внутренних угроз по всем категориям уязвимостей. Тема 3.1. Соответствие видов угроз и процессов обработки информации в ЭДО	2	2/1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Опрос, коллоквиум	ПК-24 -зув ПК-28-зув ПСК-7.5-з
Тема 3.2.Анализ источников угроз. Исследование угроз и	4	4/1	3	Самостоятельное изучение учебной и научно литературы,	Обсуждение, семинар,	ПСК-7.5-зув

Раздел/ тема дисциплины	**Аудиторная контактная работа (в акад. часах)**		сам ост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	лекции	практич. занятия				
проектирование модели разграничения прав доступа для систем электронного документооборота.				работа с материалами образовательного портала., Выполнение ИДЗ	проверка ИДЗ	
Тема 3.3.Модель угроз ИБ при обработке информации в СЭДО	2	2/1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Обсуждение, семинар	ПСК-7.5-зув
Тема 4. Проблемы аутентификации пользователей СЭД. Тема 4.1. Разграничение прав доступа к объектам. Ограничение доступа на интерфейсном уровне.	2	4/2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала, ИДЗ	Обсуждение, семинар, проверка ИДЗ	ПК-28-з ПСК-7.5-з
Тема 4.2 Задание доступа на уровне серверной базы данных. Разграничение доступа к различным частям документов	2	2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Обсуждение, семинар	ПК-28-зув ПСК-7.5-зу
Тема 5. Концептуальная модель аппаратной защиты технологии электронного обмена информацией. Применение аппаратных средств защиты информации в системах электронного документооборота.	2	3/2	3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Опрос, тестирование	ПК-28-зу ПСК-7.5-зу
Тема 5. Системы предотвращения утечек информации.	2	4/3	3	Самостоятельное изучение учебной и научной литературы	Опрос, тестирова ние	ПК-28 -зув ПСК-7.5-з
Тема 5.1Обзор и сравнение российских и зарубежных dlp-систем. Идентификация и профайлинг пользователей пользователей	1		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала, ИДЗ	Обсуждение, семинар, проверка ИДЗ	ПК-28 -зув ПСК-7.5-зув
Тема 5.2. Создание правил безопасности. Фильтрация трафика при перехвате. Организация защищенной системы электронной почты. Цифровые отпечатки.	1	4/2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Обсуждение, семинар	ПК-28 -зув ПСК-7.5-зув

Раздел/ тема дисциплины	**Аудиторная контактная работа (в акад. часах)**		сам ост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	лекции	практич. занятия				
Оценка эффективности защиты СЭД. Оценка по экономической эффективности. Методы оценки по интегральному эффекту («линейная свертка» частных показателей, методы теории нечетких множеств). Оптимизационные задачи выбора СЗИ СЭДО	4	2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка к практическим занятиям.	Опрос, коллоквиум	ПК-24 -зув ПК-28 -зув ПСК-7.5-зув
Тема 6. Проектирование и внедрение защищенного электронного документооборота. Тема 6.1. Особенности эксплуатации защищенных систем электронного документооборота. Обоснование оптимальное сочетание взаимосвязанных организационных, программных, аппаратных и иных средств СЗИ.	4	2//2	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС	Опрос, тестирование, проверка ИДЗ	ПК-24 -зув ПК-28 -зув ПСК-7.5-зув
Тема 6.2. Анализ эффективности и разработка мер по развитию и совершенствованию СЗИ СЭД.	2	2	1	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Опрос, коллоквиум	ПК-24 -зув ПК-28 -зув ПСК-7.5-зув
Экзамен				Подготовка к экзамену	**35,7**	
Итого по дисциплине	**34**	**34/14**	**36,3**			

5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Защита электронного документооборота» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

- ***обзорные лекции*** – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- ***информационные*** – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;
- ***лекции-визуализации*** – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;
- ***Семинар.***
- ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

- ***проблемная*** - для развития исследовательских навыков и изучения способов решения задач.
- ***лекции с заранее запланированными ошибками*** – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.
- ***Практическое занятие в форме практикума*** – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.
- ***Практическое занятие на основе кейс-метода*** – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации

Формы учебных занятий с использованием игровых технологий:

- ***Учебная игра*** **–** форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.
- ***Деловая игра*** – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения

- ***Творческий проект*** – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

- ***Информационный проект*** – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

Формы учебных занятий с использованием информационно-коммуникационных технологий:

- ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
- ***Практическое занятие в форме презентации*** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

- ***методы IT***
  - Подготовка и проведение лабораторных работ по поиску информации в сетях. Задание критериев поиска информации. Работа с поисковыми системами университета и внешними ресурсами.
  - Подготовка и проведение лабораторных работ по Архивации данных с целью дальнейшего использования в средствах телекоммуникационных технологий: электронной почте, чате, телеконференции т.д.
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий.
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
  - Компьютерный практикум.
- ***работа в команде***
  - Работа с элементами «Семинар», «Форум», «Обсуждение» на образовательном портале.
- ***case-study***
  - Разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
- ***проблемное обучение***
  - Подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.
- ***учебная дискуссия***
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- ***использование тренингов***
  - Подготовка и проведение демонстрационных, тематических и итоговых компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Защита электронного документооборота» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные индивидуальные домашние задания (ИДЗ):

Тема1. 1) Анализ системы документооборота предприятия Задание: сформировать комплекс требований к системе защиты ЭДО, на основе анализа состояния документооборота организации; рассмотреть перечень информационных активов организации и коммуникационную структуру информационных потоков.

2) Проанализировать наиболее распространенные СЭД на российском рынке на наличие встроенных сертифицированных СЗИ.

Тема 2. Классификация угроз СЭД. 1)Составить перечень угроз СЭД, по объекту воздействия (объектом воздействия является инфраструктура информационных систем), используя данные банка угроз ФСТЭК,
2)Составить перечень уязвимостей СЭД(на примере 1С) с сетевым способом получения доступа.

Тема 4.1. Исследование угроз и проектирование модели разграничения прав доступа для систем электронного документооборота.
Задание: на языке программирования высокого уровня, написать программу, которая будет реализовывать матрицу доступа позволит изменять уровни доступа пользователей (субъектов) и степени секретности файлов (объектов). Написать отчет о выполненной работе, в котором отразить: блок-схему алгоритма программы, исходный текст программы и описание порядка работы в ней.

Тема 9. Контроль информационных потоков. Контроль почтовых серверов. Контроль архивов и документов, защищенных паролем.. Поиск по регулярным выражениям. (DLP-система SecureTower).

Тема 4.2 Задание: Применение системы Страж NT для защиты в части реализации мандатной модели разграничения доступа.

1) в соответствии с политикой безопасности назначить каждому пользователю уровень допуска при помощи «Менеджер пользователей» программы «Управление СЗИ
2) для прикладных программ, предназначенных для обработки защищаемых ресурсов, разрешить режим запуска и установить значение допуска при помощи окна «Администратор ресурсов» программы «Управление СЗИ»;
3) в соответствии с политикой безопасности определить защищаемые ресурсы и присвоить им гриф секретности также при помощи «Администратора ресурсов».

Тема 5.2. Создание правил безопасности. Фильтрация трафика при перехвате. Цифровые отпечатки.
Задание: отобразить типовые схемы для мониторинга перехвата— серверный и агентский. Настроить базу данных перехвата трафика на сервере. Настроить перехват непосредственно на рабочих станциях. Выявить, способ перехвата позволяет значительно расширить перехватываемые каналы, охватить большинство мессенджеров и веб-трафик по протоколу HTTPS.

Тема 6 Задача: Разработать техническое задание на создание проекта защиты СЭД

1) описание программно-технических решений для создания системы защиты в соответствии с требованиями Технического задания.

2) разработка общих решений по системе и её частям, функционально-алгоритмической структуре системы, по функциям персонала и организационной структуре, по структуре технических средств, по организации и ведению информационной базы.

3) Теоретические вопросы к экзамену

1. Основные принципы построения системы электронного документооборота. Стандарты в области проектирования электронного документооборота ИС.
2. Архитектуры и способы построения СЭД. Современные программные средства электронного документооборота.
3. Выявленные уязвимости СЭДО. Выбор средств защиты. Обосновать взаимосвязь между методами и средствами защиты информации
4. Определение и источники основных преднамеренных угроз ЭД. Способы проникновения компьютерных вирусов в корпоративные сети.

5. Защита методом управления доступом. Идентификация и аутентификация. Роль аутентификации в организации защиты документооборота при использовании открытых сетей связи Средства управления доступом. Обосновать взаимосвязь между методами и средствами управления доступом.
6. Принципы работы и возможности dlp-систем. Сравнить существующие российские и зарубежные dlp-системы.
7. Организация электронного архива документов и комплекс мер защиты электронной документации.
8. Юридические проблемы защиты электронного документооборота.
9. Визирование ЭЦП версии присоединенного файла. Удаление документов. Какой вид угроз информационной безопасногсти СЭД перекрывается с помощью криптографических методов защиты.
10. Аппаратные средства защиты корпоративных информационных систем и СЭД.
11. Уязвимости СЭД, использующих общедоступные каналы связи(защиты каналов связи на сетевом уровне, защиты периметра файерволами).
12. Критерии оценки защищенности систем электронного документооборота
13. Нормативные правовые акты в области защиты информации в СЭД.
14. СЭДО как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
15. Содержание и порядок деятельности персонала по эксплуатации защищенных СЭДО

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		
Знать	− принципы построения и функционирования, примеры реализаций систем электронного документооборота; -методы и средства проектирования систем электронного документооборота; - основные принципы построения защищенных информационных систем, электронного документооборота; –критерии оценки защищенности систем электронного документооборота, источники угроз и нормативные документы; - информационные технологии, используемые в автоматизированных системах; − возможности, классификацию и область применения макрообработки;	**Перечень теоретических вопросов:** 1. Основные принципы построения системы электронного документооборота. 2. Принципы построения систем и средств защиты информационных систем, электронного документооборота 16. Современные программные средства электронного документооборота 17. Архитектуры и способы построения СЭД. 18. Сравнение российских систем ЭД. Встроенные СЗИ СЭД. 19. Критерии оценки защищенности систем электронного документооборота 20. Нормативные правовые акты в области защиты информации в СЭД.

Уметь:	-применять современные информационные технологии для прохождения, обработки, учета и рассылки документов внутри организации с учетом требований информационной безопасности; -разрабатывать техническую документацию для систем защиты электронного документооборота; -готовить научно-технические отчеты, обзоры, публикации по теме предметной области;	**Задача:** На основании актуального перечня информационных активов малого предприятия и его коммуникационной архитектуры, сформировать список требований к системе защиты ЭДО, на основе составленных требований составить перечень СЭДО, удовлетворяющих требованиям информационной безопасности.
Владеть:	-навыками применения современных информационных технологий для прохождения, обработки, учета документов внутри организации с учетом требований информационной безопасности; навыками разработки технической документации для систем защитыэлектронного документооборота; -навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области;	**Задача:** в соответствии с некоторой утвержденной политикой безопасности произвести основные настройки и установки системы предотвращения утечек информации (на примере системы Secure Tower).

ПК-28 способностью управлять информационной безопасностью автоматизированной системы

Знать	-основные методы управления информационной безопасностью; -процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы; принципы формирования политики информационной безопасности автоматизированных систем	**Перечень теоретических вопросов:** 1. Перечислить комплекс мер защиты электронной документации 2. Визирование ЭЦП версии присоединенного файла. Удаление документов. 4.Определение и источники основных преднамеренных угроз 3. Способы проникновения компьютерных вирусов в корпоративные сети. 4. Ввзаимосвязь между методами и средствами защиты информации 5. Защита методом управления доступом 6. Защита и надежность методов идентификации и аутентификации. Роль аутентификации в организации защиты документооборота при использовании открытых сетей связи. 7. Какой вид угроз информационной безопасногсти СЭД перекрывается с помощью криптографических методов защиты. 8. Организация защиты электронного архива документов. 9. Офисные устройства по обработке конфиденциальной информации:
Уметь:	- разрабатывать предложения по совершенствованию системы	**Задача:** На основе анализа текущего

	управления информационной безопасностью автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации;	состояния электронного документооборота предприятия, разработать предложения защиты системы электронного документооборота с несколькими вариантами, краткий анализ этих вариантов и рекомендации по выбору.
Владеть:	-навыками построения моделей угроз системы электронного документооборота; -методами управления информационной безопасностью для решения задач управления информационной безопасностью систем электронного документооборота; - навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем;	**Задача:** Определить и сформулировать основные угрозы в СЭДО в зависимости от специфики ее работы. Обосновать выбор средств защиты по каждому виду угроз.

ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

Знать	-мероприятия по обеспечению безопасности распределенных информационных систем; -методы организации работы по обеспечению защиты информации в распределенных информационных системах; -организационные меры по защите информации с системах ЭДО; -законодательные акты, стандарты по защите информации в системах ЭДО;	**Перечень теоретических вопросов:** 1. Проектирование системы защиты документооборота –основные задачи, этапы, проблемы. 2. Проблемы создания систем защищенного документооборота. 3. Организационные меры защиты электронной документации 4. Принципы работы и возможности dlp-систем. 5. Сравнить существующие российские и заруюежные dlp-системы. 6. Законодательные акты, стандарты по защите информации в системах ЭДО 7. Юридические проблемы защиты электронного документооборота. 8. СЭДО как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности 9. Содержание и порядок деятельности персонала по эксплуатации защищенных СЭДО
Уметь:	-выбирать методы и подходы к проектированию средств защиты СЭДО на предприятии; -выявлять особенности и формировать требования безопасности к системе	**Задача:** В соответствии с данной политикой безопасности и информационными ресурсами предприятия разработать матрицу и защиты информации в типовой ИС.

	организации коллективной работы с документами в режиме совместного доступа и передачи их на исполнение по электронной почте или по локальной сети; -составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы	
Владеть:	-навыками администрирования систем электронного документооборота; -методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов; -научными основами и современными методиками обеспечения безопасности распределенной информационной системы	**Задача:** На основе ТЗ разработать эскизный проект системы защиты информации для дальнейшего выполнения работ по созданию КСЗИ, в соответствии с ГОСТ 34.201-89)

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку «***отлично***» – обучающийсядолжен показать высокий уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободно и правильно обосновывать принятые решения;

– на оценку «***хорошо***» – обучающийсядолжен показать средний уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике;

– на оценку «***удовлетворительно***» – обучающийсядолжен показать пороговый уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

– на оценку «***неудовлетворительно***» – обучающийсяне может показать знания на уровне воспроизведения и объяснения информации, не умеет использовать полученные знания при решении типовых практических задач.

8 **Учебно-методическое и информационное обеспечение дисциплины (модуля)**

а) Основная литература:

1. Электронное правительство. Электронный документооборот. Термины и определения: Учебное пособие / С.Ю. Кабашов. - М.: НИЦ ИНФРА-М, 2013. - 320 с.: 60x90 1/16. - ISBN 978-5-16-006835-0 – Режим доступа: http://znanium.com/bookread2.php?book=410730 - Заглавие с экрана.
2. Баранкова И. И. Техническая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true. - Макрообъект.

3. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true. - Макрообъект. - ISBN 978-5-9967-1031-7.

б)Дополнительная литература

1. Смирнов Ю.А. Технические средства автоматизации и управления: [Электронный ресурс]:Учебное пособие / Ю.А. Смирнов. - Лань, 2018. - 456 с. - Электронное издание. – Режим доступа: https://e.lanbook.com/reader/book/109629/#1.- Заглавие с экрана.
2. Гражданский Кодекс Российской Федерации (часть четвертая) № 30-ФЗ от 18.12.2006 г. (с изменениями).
3. Закон Российской Федерации «О государственной тайне» № 5485-1 от 21.07.1993 г. (с изменениями).
4. Уголовный Кодекс Российской Федерации № 63-ФЗ от 13.06.1996 г. (с изменениями), статьи 146, 147, 183, 272, 273, 274, 283, 284.
5. Федеральный Закон Российской Федерации «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г. (с изменениями).
6. Федеральный Закон Российской Федерации № 125-ФЗ "Об архивном деле в Российской Федерации" от 22.10.2004 г.
7. Федеральный Закон Российской Федерации № 152-ФЗ «О персональных данных» от 27.07.2006г.
8. Приказ Федеральной архивной службы России № 68 Типовая инструкция по делопроизводству в федеральных органах исполнительной власти.
9. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) "Об информации, информационных технологиях и о защите информации"
10. Федеральный закон от 25 марта 2011 г. № 63-ФЗ «Об электронной подписи».
11. Федеральный закон от 27 июня 2008 г. № 152-ФЗ «О персональных данных».
12. ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения.
13. ГОСТ Р 6.30 2003 Требования к оформлению документов.
14. ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования.

9. Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория	Мультимедийные средства хранения, передачи и представления информации, доска Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021
Аудитория для проведения практических занятий	Мультимедийные средства хранения, передачи и представления информации, доска
Компьютерный класс	Персональные компьютеры с пакетом MS Office и выходом в Интернет Microsoft Open License 42649837, бессрочная
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	DLP- система SecureTower. (Лицензионный ключ (9752920000005A48), бессрочная в рамках договора) СЗИ от НСД Страж NT 3.0№ лицензии: D1B4D8C0F28854B0 бессрочная
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную

Тип и название аудитории	Оснащение аудитории
	информационно-образовательную среду университета.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03. Информационная безопасность автоматизированных систем.Специализация «Обеспечение информационной безопасности распределенных информационных систем».*