Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.15.03 «КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И. Рабочая программа дисциплины: Конфиденциальное делопроизводство и защищенный электронный документооборот. – Королев МО: «Технологический университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.05.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации, документооборота, циркулирующего в ИС предприятия;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности, во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности организации работы по обработке и защите конфиденциальной информации на типовом предприятии;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую основу организации работы сотрудников по обработке и защите конфиденциальной информации;
5. Приобретение студентами первичных навыков по способам обработки и хранения и защиты конфиденциальных документов.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ДОПК-1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;

ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

Основными **задачами** дисциплины являются:

1. Ознакомить студентов с проблемами построения и совершенствования технологии защиты и обработки конфиденциальных документов в условиях применения разнообразных типов носителей документной информации, а также различных средств, способов и систем обработки и хранения конфиденциальных документов;
2. Научить студентов самостоятельно решать поставленные задачи в области организации защиты конфиденциальной информации;

3. Формировать систему знаний у обучающихся по научным, прикладным и методическим аспектам организации выполнения технологических стадий. Процедур и операций с конфиденциальными документами, проектирование рациональной технологической схемы защиты конфиденциального документооборота.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации
- знает технологии проектирования и построения информационных систем
- знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации
- знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками
- знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем
- знает методы анализа процессов для определения актуальных угроз
- знает особенности работы решений по защите информации в информационных процессах и системах
- знает принципы обеспечения информационной безопасности объекта информатизаци ДОПК-
- знает основные категории требований к программным и программно-аппаратным средствам защиты информации
- знает требования по защите автоматизированных систем от НСД
- знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации
- знает отечественные и зарубежные стандарты в области информационной безопасности
- знает как разрабатывать технические задания на создание подсистем информационной безопасности открытых информационных систем
- знает правовые нормы, инструкции и стандарты в области организации документооборота
- знает правовые основы организации защиты государственной тайны и конфиденциальной информации
- знает как разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации
- знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационной безопасности персональных данных
- знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ

Необходимые умения:

- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности
- умеет представлять процессы в формализованном виде на языках моделирования
- умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ
- умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз
- владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации
- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов
- умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение
- умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности

Трудовые действия:

- владеет навыками выявления и устранения угроз информационной безопасности
- владеет навыками реализации политики информационной безопасности
- владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ
- владеет навыками оценки адекватности моделей и анализа результатов моделирования
- владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining
- владеет навыками анализа надежности защиты информационных систем
- владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну
- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ
- владеет навыками проведения лицензирования в области защиты информации

владеет навыками работы с нормативно-правовыми актами

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Конфиденциальное делопроизводство и защищенный электронный документооборот» относится к базовой части основной

профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОПК-1,3,5,6,8.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 4 зачетных единиц, 144 часа.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр 6	Семестр …	Семестр …
Общая трудоемкость	144	144	144		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			

Лабораторные работы (ЛР)	16	16			
Самостоятельная работа	86	86			
Другие виды контактной работы	10	10			
Практическая подготовка	нет	Нет			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2 ч**.**	Т1;Т2	Т1;Т2			
Вид итогового контроля	Экзамен	Экзамен			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	24		24		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	8		8		
Лабораторные работы (ЛР)	4		4		
Самостоятельная работа	118		118		
Другие виды контактной работы	10		10		
Практическая подготовка	нет		Нет		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+ -		+ -		
Вид итогового контроля	Экзамен		Экзамен		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очно/заочное	Практические занятия, час. Очно/заочное	Лаборатор. занятия, час. Очно/заочное	Занятия в интерактивной форме, час. Очно/заочное	Код компетенций
Раздел I. Организация обработки конфиденциальных документов					
Тема 1:Сущность, задачи и особенности конфиденциальной информации	1/0.5	1/1	1/0.2	0.5/1	ДОПК-1,3
Тема 2:Организация конфиденциального делопроизводства	1/0.5	1/0.5	1/0.2	0.5/1	ДОПК-1,3
Тема3:Документирование конфиденциальной информации	1/0.5	1/0.5	1/0.2	0.5/1	ДОПК-1,3
Тема 4: Учет конфиденциальных документов	1/0.5	1/0.5	1/0.2	0.5/1	ДОПК-1,3
Тема 5: Организация конфиденциального документооборота	1/0.5	1/0.5	1/0.2	0.5/1	ДОПК-1,3
Раздел II. Технологии защиты конфиденциальных документов					
Тема 6: Размножение конфиденциальных документов	1/0.5	1/0.5	1/0.3	0.5/1	ДОПК-1,3
Тема 7: Составление номенклатур конфиденциального документооборота	1/0.5	1/0.5	1/0.3	0.5/4	ДОПК-1,3
Тема 8: Подготовка КД для архивного хранения и уничтожения	1/0.5	1/0.5	1/0.3	0.5/1	ДОПК-1,3
Тема 9: Режим хранения конфиденциальной информации и обращение с ней	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Тема 10: Проверка наличия конфиденциальных документов	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Раздел III. Обеспечение режима конфиденциальности безопасного допуска к информационным ресурсам					

Тема 11. Понятие и особенности СЭДО	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Тема 12. Составление номенклатуры дел, формирование и оформление конфиденциальных дел	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Раздел IV. Реализация механизмов защиты для обработки конфиденциальной информации в системах защищенного документооборота					
Тема 13: Система защищенного электронного документооборота.	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Тема 14.Построение СЭД без существенных настроек типовой IT – архитектуры.	1/1	1/0.5	1/0.3	1/1	ДОПК-1,3
Тема 15. Применение аппаратных средств аутентификации и хранения ключевой информации	2/1	2/0.5	2/0.3	1/1	ДОПК-1,3
Итого:	16/12	16/8	16/4	12/18	

4.2. Содержание тем дисциплины

Раздел I. Организация обработки конфиденциальных документов

Тема 1. Сущность, задачи и особенности конфиденциальной информации

Уровни доступности, сфера деятельности КД, отличие видов работ открытого и конфиденциального делопроизводства, уязвимость документированной информации, утечка информации, задачи КД, сущность КД.

Тема 2. Организация конфиденциального делопроизводства

Условия работы, подразделения по организации КД. Методика расчета численности сотрудников подразделения КД. Создание постоянно действующей экспертной комиссии (ПДЭК).

Тема 3. Документирование конфиденциальной информации

Документационное обеспечение деятельности предприятия. Определение состава КД. Подготовка и издание КД. Оформление и учет носителей конфиденциальной информации. Издание и учет проектов конфиденциальных документов. Оформление издаваемых КД.

Тема 4. Учет конфиденциальных документов

Документационное обеспечение деятельности предприятия. Общие требования к учету КД. Учет изданных КД. Учет поступивших КД. Учет конфиденциальных документов выделенного хранения.

Тема 5. Организация конфиденциального документооборота

Документационное обеспечение деятельности предприятия. Понятия и принципы организации КД. Система доступа к КД. Организация исполнения и отправления КД. Размножение КД.

Раздел II. Технологии защиты конфиденциальных документов

Тема 6. Размножение конфиденциальных документов

Проверки правильности проставления отметок о движении КД, дел и носителей. Основные требования к тексту служебных документов. Режим размножения КД. Порядок размножения КД. Организация исполнения, учета и размножения КД.

Тема 7. Составление номенклатур конфиденциального документооборота

Проверки правильности проставления отметок о движении КД, дел и носителей. Основные требования к тексту служебных документов. Составление номенклатур, формирование и оформление КД.

Тема 8. Подготовка КД для архивного хранения и уничтожения

Проверки правильности проставления отметок о движении КД, дел и носителей. Общие требования к бланкам предприятий. Экспертиза КД, подготовка КД и дел с КД для архивного хранения и уничтожения

Тема 9. Режим хранения конфиденциальной информации и обращение с ней

Режим хранения КД. Порядок обращения с КД. Назначение, виды и принципы проведения проверок наличия КД. Проверки правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (карточек).

Тема 10. Проверка наличия конфиденциальных документов

Проверки правильности проставления отметок о движении КД, дел и носителей. Квартальные проверки фактического наличия КД и документов. Годовая проверка наличия КД, документов выделенного хранения и учетных журналов (карточек). Не регламентные проверки наличия конфиденциальных носителей, документов и дел.

Раздел 3. Обеспечение режима конфиденциальности безопасного допуска к информационным ресурсам

Тема 11. Понятие и особенности конфиденциальной информации.

Общие положения. Персональные данные. Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Секрет производства (ноу-хау) и служебный секрет производства. Особенности документирования конфиденциальной информации. Определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов. Разработка Перечня конфиденциальной документированной информации. Учёт бумажных носителей конфиденциальной информации. Учёт проектов конфиденциальной документированной информации. Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения. Учёт использования и

хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов.

Особенности учёта и регистрации конфиденциальной документированный информации. Обработка поступающих конфиденциальных документов, их учёт и регистрация. Учёт и регистрация внутренних (созданных/изданных) конфиденциальных документов. Технологии исполнения и контроля за исполнением конфиденциальных документов. Учёт и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка. Учёт конфиденциальной документированной информации инвентарного (выделенного) хранения. Учёт конфиденциальной информации при ее автоматизированной обработке. Основные требования к разрешительной системе документа. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства. Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти. Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные. Особенности доступа к архивным конфиденциальным документам. Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации. Учёт персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена.

Тема 12. Составление номенклатуры дел, формирование и оформление конфиденциальных дел

Документальный фонд организации. Формирование конфиденциальных дел. Оформление конфиденциальных дел.

Экспертиза ценности конфиденциальных документов. Подготовка конфиденциальных документов и дел для архивного хранения. Подготовка конфиденциальных документов и дел к уничтожению.

Режим обмена конфиденциальной документированной информацией. Режим сохранности конфиденциальных документов и дел. Режим конфиденциальности при проведении совещаний и переговоров. Проверка наличия носителей конфиденциальной информации.

Раздел 4. Реализация механизмов защиты для обработки конфиденциальной информации в системах защищенного документооборота

Тема 13: Система защищенного электронного документооборота.

Особенности конфиденциального электронного документооборота. Основные виды угроз информационной безопасности организации. Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе. Организация работ при создании системы защиты электронного документооборота. Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке. Обеспечение контроля защиты электронного документооборота. Аттестация автоматизированных информационных систем по

требования безопасности информации. Защита от вредоносных программ. Защита системы электронных сообщений.

Тема 14: Построение СЭД без существенных настроек типовой IT – архитектуры.

Основные требования к системам электронного документооборота. Краткая характеристика систем электронного документооборота.

Обобщенные требования к функционированию ЭДО. Декомпозиция задачи построения СЭД. Создание УЦ. Функции центра сертификации (ЦС). Механизмы защиты СЭДО. СМЭВ (система межведомственного электронного взаимодействия) как ее применять в системах ЭДО. Характеристика системы ЭДО «Канцлер», «Бюрократ», «Алтиус». Сокращение издержек при переходе на ЭДО: практические шаги. Цели проекта. Границы проекта. Ограничения и риски проекта. Рабочая группа. Выбор программной платформы. План проекта.

Тема 15. Применение аппаратных средств аутентификации и хранения ключевой информации

Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.
Аппаратные средства защиты в современных PKI решениях. Необходимость применения аппаратных средств аутентификации и хранения ключевой информации. Типовые требования к средствам аутентификации и хранения ключевой информации. Особенности корпоративного использования персональных средств аутентификации и хранения ключевой информации. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей. Типовые требования к системе управления токенами. Token Management System (TMS) компании Aladdin. Практика: комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Конфиденциальное делопроизводство и защищенный электронный документооборот» приведена в Приложении 1.

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

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL:

https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/ –** академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

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

Перечень программного обеспечения: MSOffice.

Информационные справочные системы:
Электронные ресурсы образовательной среды Университета.
Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Конфиденциальное делопроизводство и защищенный электронный документооборот»

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

Лекционные занятия:

– аудитория, оснащенная презентационной техникой (проектор, экран);

– комплект электронных презентаций / слайдов на темы:

Практические занятия:

– компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
– рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
– рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции)	: В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ДОПК-1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Тема:1,3,5,7,8	- владеет навыками выявления и устранения угроз информационной безопасности - владеет навыками реализации политики информационной безопасности - владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ - владеет навыками оценки адекватности моделей и анализа результатов моделирования - владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data	- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности - умеет представлять процессы в формализованном виде на языках моделирования ДОПК-- умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ - умеет делать обоснованный выбор существующих средств защиты	- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации - знает технологии проектирования и построения информационных систем - знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации - знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками - знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем - знает методы анализа процессов для определения актуальных угроз - знает

				mining - владеет навыками анализа надежности защиты информационных систем - владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну	информации для нейтрализации определенного вида угроз - владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации	особенности работы решений по защите информации в информационных процессах и системах - знает принципы обеспечения информационной безопасности объекта информатизаци - знает основные категории требований к программным и программно-аппаратным средствам защиты информации - знает требования по защите автоматизированных систем от НСД - знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
2.	ДОПК-3	Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	Тема:2,4,5,10-15	- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ - владеет навыками проведения лицензирования в области защиты информации - владеет навыками работы с нормативно-правовыми	- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов - умеет разрабатывать инструкции по	- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации - знает отечественные и зарубежные стандарты в области информационной безопасности - знает как разрабатывать технические задания на создание

				актами	организации защищённого документооборота и контролировать их исполнение - умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности	подсистем информационной безопасности открытых информационных систем - знает правовые нормы, инструкции и стандарты в области организации документооборота - знает правовые основы организации защиты государственной тайны и конфиденциальной информации - знает как разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации - знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационной безопасности персональных данных - знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ДОПК-1,3	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** ***• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** ***• компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).*** ***Максимальная сумма баллов - 5 баллов.***
ДОПК-1,3	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** ***• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** ***• компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Исследование выбранного объекта защиты информации – локальной вычислительной сети.

а. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.

2. Разработка требований к системе защиты информации локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

3. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.

4. Разработка пояснительной записки по созданию системы защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

5. Обосновать создание ЛВС, имеющий выход в сеть Интернет. Осуществить выбор средств и организационно – технических мер по защите информации выбранного объекта защиты (с учетом защиты информации от несанкционированного доступа к СЭД).

6. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

7. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД.

8. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД.

9. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

10. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД.

11. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.

12. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

13. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

14. Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа (для СЭД).

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

Формой контроля знаний по дисциплине «Конфиденциальное делопроизводство и защищенный электронный документооборот» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-1,3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***

Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-1,3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	Экзамен	ДОПК-1,3	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять

						полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумени

						е использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

Пример тестирования 1

1) **Какой вид тайны включает полученную федеральными органами власти информацию составляющую КТ других субъектов и собственную информацию предприятия ограниченную служебной необходимости?**

(!) Коммерческая тайна
(!) Профессиональная тайна
(!) Банковская тайна
(?) Служебная тайна

2) **К формам уязвимости документированной информации?**

(!) Хищение и потеря носителя
(!) Потеря носителя и искажение информации
(?) Хищение, потеря, уничтожение носителя и искажение информации
(!) несанкционированное уничтожение и искажение информации

3) **Неразрешённый выход информации за пределы защищаемой зоны это?**

(?) Утечка КИ
(!) Потеря КИ
(!) Кража КИ
(!) Хищение КИ

4) **Разглашение какой информации является формой проявления уязвимости?**

(!) Государственной информации
(?) Конфиденциальной информации
(!) Открытой информации

(!) Коммерческой информации

5) Документы КД должны обеспечивать:

(?) Полноту, достоверность и своевременность

(!) Полноту и достоверность

(!) Достоверность и своевременность

(!) Своевременность и полноту

6) Какие особенности обуславливает сущность КД

(!) Научные и технологические

(?) Организационные и технологические

(!) Правовые и организационные

(!) Научные и экономические

7) Что понимается под документированием информации?

(!) Процесс обработки и защиты документов

(!) Создание и регламентация документов

(!) Анализ и изготовление документов

(?) Процесс подготовки и изготовления документов

8) Какие документы относятся к секретному делопроизводству?

(?) Государственная тайна

(!) Коммерческая тайна

(!) Служебная тайна

(!) Профессиональная тайна

9) **К секретной информации относится :**

(?) государственная тайна;

(!) коммерческая тайна;

(!) профессиональная тайна;

(!) конфиденциальная информация.

10) **Сферу коммерческой тайны регулирует :**

(!) Федеральный закон «О коммерческой тайне в коммерческих организациях»;

(!) Федеральный закон «О коммерческих организациях»;

(!) Федеральный конституционный закон «О коммерческой тайне»

(?) Федеральный закон «О коммерческой тайне».

11) **Ценность конфиденциальной информации означает :**

(!) размер прибыли при использовании такой информации фирмой;

(!) размер убытков при утрате такой информации;

(!) моральный ущерб при утрате такой информации или ее использовании в неправомерных целях;

(?) размер прибыли при использовании такой информации фирмой и размер убытков при ее утрате.

12) Выберите неверный вариант. «В задачи постоянно действующей экспертной комиссии входит:

(!) проведение аналитических работ по предотвращению утечки и утраты конфиденциальной информации

(!) снятие или снижение грифа конфиденциальности на документах и делах;
(!) разработка перечня издаваемых в фирме конфиденциальных документов;
(?) организация работы с конфиденциальными документами.

13) **Процедура уничтожения конфиденциальных документов и носителей информации документируется в :**
(!) свидетельстве об уничтожении;
(!) справке об уничтожении;
(!) протоколе о ходе уничтожения;
(?) акте об уничтожении.

14) Какой номер ФЗ регулирует деятельность в области персональных данных?

(!)ФЗ №150
(!)ФЗ №98
(?)ФЗ №152
(!)ФЗ №138

15) **При выдаче документа из конфиденциального дела сотруднику организации делается отметка в:**
(?) карточке учета разрешений и выдачи;
(!) карточке учета разрешений;
(!) карточке учета выдачи документов;
(!) внутренней описи дела.

16) **Гриф конфиденциальности располагается:**
(!) на документе по нижнему полю;
(!) на бланке документа после его номера и даты;
(?) на бланке документа в левом верхнем углу;
(!) на первом листе документа в правом верхнем углу.

17) Утечка конфиденциальной информации это?
(?) непрерывный выход информации за пределы контролируемой зоны
(!) уничтожение конфиденциальной информации
(!) обработка конфиденциальной информации вне контролируемой зоны
(!) считывание конфиденциальной информации с источника

18) Конфиденциальное делопроизводство решает следующую задачу:
(?) Документционного обеспечения всех видов конфиденциальной информации
(!) Распространение конфиденциальной информации
(!) Организация работы с сотрудника допущенных к государственной тайне
(!) Внедрение и создание политики безопасности в учреждении

19) Формой уязвимость документационной информации является:
(!) Утечка информации
(!) Блокирование информации

(?) Потеря носителя информации
(!) Выход информации за пределы контролируемой зоны

20) Какой документ определяет деятельность сотрудника подразделения конфиденциального делопроизводства:

(!) Приказ руководителя предприятия
(?) Должностная инструкция
(!) ФЗ «О конфиденциальной информации!»
(!) ФЗ «Об информации, информационных технологиях и защиты информации»

Пример тестирования 2

1) Какой документ определяет деятельность сотрудника подразделения конфиденциального делопроизводства:

(!) изготовление и учет проектов конфиденциальной документов
(!) определение состава конфиденциальных документов
(?) уничтожение проектов конфиденциальных документов
(!) оформление издаваемых документов

2) На что влияет объем и характер издаваемых документов?

(!) изготовление документов
(!) сертификация документов
(?) защита документов
(!) модификация документов

3) От чего зависит эффективность управляемой и производственной деятельности?

(!) количества информации
(!) правильности документов
(?) характера документов
(!) состава документов

4) Что не требует порядок изготовления конфиденциальных документов?

(!) Определенных знаний, которые постоянно пополняются
(!) специально-оборудованного помещения
(!) допуск сотрудников
(?) оборудование, изготовленное под руководством ПДЭК

5) Что не предусматривает допуск сотрудников?

(!) ознакомление сотрудников с перечнем сведений, составляющих коммерческую тайну
(?) внесение изменений в документы по своему усмотрению
(!) ознакомление сотрудников с положениями законодательства
(!) принятие сотрудниками обязательств по соблюдению какого-либо вида тайн на предприятии

6) Чьим приказом создается ПДЭК?

(!) президентом РФ
(!) ФСТЭК
(?) руководителем предприятия
(!) системным администратором

7) Кто из должностных лиц не входит в состав ПДЭК?

(!) руководитель отдела службы безопасности
(!) руководитель архива предприятия
(?) квалифицированные сотрудники
(!) квалифицированные сотрудники, имеющие допуск к коммерческой тайне

8) Что не входит в задачи ПДЭК?

(!) проведение аналитической работы по предотвращению утечки и утраты конфиденциальной информации
(?) оформление на работу высококвалифицированных сотрудников, имеющих допуск к коммерческой тайне
(!) разработка перечня сведений составляющих коммерческую и служебную тайну
(!) снижение и снятие степени конфиденциальных сведений и графа конфиденциальной информации

9) Какие параметры отражает коммерческая тайна предприятия?

(?) На кого возложена защита КТ
(!) Чьи интересы обеспечивает режим СТ
(!) Какие документы относят к общедоступным
(!) Информацию ограниченного доступа

10) На какие виды деятельности распространяется КД?

(?) Управленческую и различные производственные виды деятельности
(!) Техническую и организационную
(!) Правовую и техническую
(!) Все ответы верны

11) Что такое утечка КИ?

(?) Непрерывный, неразрешенный выход информации за пределы зоны или какого-то круга лиц
(!) Несанкционированное уничтожение носителя КИ
(!) Искажение информации
(!) Утрата информации в случае халатности персонала

12) В каком документе закреплены задачи и функции подразделения КД?

(!) Инструкция
(?) Положение о подразделениях
(!) Перечень задач и функций
(!) Требования и стандарты

13) На сколько категорий подразделяют уровни доступности документа?

(!) 4
(?) 2
(!) 3
(!) 5

14) Какие документы относятся к сфере секретного делопроизводства?

(!) Коммерческая тайна
(?) Государственная тайна
(!) Служебная тайна
(!) Семейная тайна

15) Формы уязвимости документированной информации?

(!) Кража
(!) Разрушение
(!) Утеря
(!) Изменение, модификация
(?) Все перечисленные

16) На кого возлагается процесс издания, обработки, хранения КД при его незначительном объеме?

(!) На специальное подразделение КД
(!) На специально нанятых лиц, обеспечивающих лиц
(?) На лица специально назначенных приказом руководителя предприятия из других подразделений
(!) Все неверны

17) Как принято называть документы содержащие КТ и СТ?

(?) Конфиденциальными
(!) Секретные
(!) Особой важности
(!) Все верно

18) Блокирование информации означает?

(?) Блокирование правомочных пользователей к ней
(!) Блокирование информации от злоумышленников
(!) Блокирование правомочных пользователей и злоумышленников
(!) Нет правильных ответов

19) Какую ответственность несут сотрудники КД, ответственные за утрату КД или разглашение, содержащие в ней информацию?

(!) Дисциплинарную
(!) Административную
(!) Гражданско-правовую
(?) Все верно

20) На какие группы делятся совокупность компонентов, обеспечивающих работоспособность и здоровье сотрудников в служебном помещении?

(!) Состояние служебных помещений, организация трудового процесса
(!) Поддержание здорового микроклимата в коллективе
(?) Все верны
(!) Верен только первый

Пример тестирования 3

1. Что понимается под идентификацией:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процедура предоставления субъекту прав доступа;
процесс управления доступом субъектов к ресурсам системы.

2. Сколько компонентов включает в себя система аутентификации:
3;
4;
5;
6.

3. Что понимается под администрированием:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процедура предоставления субъекту прав доступа;
процесс управления доступом субъектов к ресурсам системы.

4. Что понимается под аудитом:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процесс контроля доступа субъектов к ресурсам системы;
процесс управления доступом субъектов к ресурсам системы.

5. Что понимается под авторизацией:
процедура распознавания субъекта;
процедура предоставления субъекту прав доступа;
процесс контроля доступа субъектов к ресурсам системы;
процедура проверки подлинности субъекта.

6. Назовите основное свойство однонаправленной хэш-функции:
невозможность восстановления исходного значения;
возможность восстановления исходного значения;
возможность редактирования исходного значения;
все значения ключей хэш-функций равны друг другу.

4.2 Типовые вопросы, выносимые на экзамен

1. Сущность, задачи и особенности конфиденциального делопроизводства.
2. (виды тайны, утечка или утрата информации, особенности).

3. Организация конфиденциального делопроизводства.
4. (должностные инструкции, оборудование помещения, задачи ПДЭК).
5. Состав конфиденциальных документов.
6. Оформление и учет носителей конфиденциальной информации.
7. (формы журналов учета)
8. Изготовление и учет проектов конфиденциальных документов.
9. (формы журналов учета).
10. Оформление издаваемых конфиденциальных документов.
11. (реквизиты документа).
12. Общие требования к учету конфиденциальных документов.
13. Учет изданных документов.
14. (формы журналов учета)
15. Учет поступивших документов.
16. (формы журналов учета)
17. Учет конфиденциальных документов выделенного хранения.
18. (формы журналов учета)
19. Размножение конфиденциальных документов
20. (формы журналов учета)
21. Понятия и принципы организации конфиденциального документооборота.
22. Система доступа к конфиденциальным документам.
23. Организация исполнения конфиденциальных документов.
24. (формы журналов учета, оформление документа)
25. Отправление конфиденциальных документов.
26. Составление номенклатур конфиденциальных дел.
27. (формы журналов учета)
28. Формирование конфиденциальных дел
29. Оформление конфиденциальных дел.
30. (формы карточек учета, опись документов, заверительная надпись).
31. Экспертиза ценности конфиденциальных документов.
32. Подготовка конфиденциальных дел и документов для архивного хранения.
33. (формы описи дел)
34. Подготовка конфиденциальных дел и документов для уничтожения.
35. (форма акта)
36. Режим хранения конфиденциальных документов.
37. (формы журналов учета)
38. Порядок обращения с конфиденциальными документами
39. (форма описи)
40. Назначение, виды и принципы проведения проверок наличия конфиденциальных документов.
41. Проверки правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (картотек).
42. Проверки правильности проставления отметок о движении конфиденциальных документов, дел и носителей.

43. Квартальные проверки фактического наличия конфиденциальных носителей и документов (форма акта).

44. Годовая проверка наличия конфиденциальных дел, документов выделенного хранения и учетных журналов (картотек).

45. Не регламентные проверки наличия конфиденциальных носителей, документов и дел.

Часть 2

1.Назовите процедуры, выполняемые при регистрации пользователя в системе.

2. Что такое аутентификация.

3. Что такое идентификация.

4. Что такое авторизация.

5. Структура модели OSI.

6. Что такое администрирование.

7. Перечислите элементы аутентификации.

8. Для чего служит механизм управления доступом.

9. Перечислите факторы аутентификации.

10. Приведите примеры факторов аутентификации.

11. Назовите методы парольной аутентификации.

12. Приведите пример аутентификации пользователя на основе открытого пароля.

13. Что такое однонаправленные хэш – функции.

14. Что такое PIN- код.

15. назовите области и условие использования PIN- кода.

16. Для чего необходимы парольные политики.

17. Приведите примеры атак на системы, в которых используется аутентификация на основе пароля.

18. Перечислите физиологические биометрические характеристики.

19. Назовите поведенческие биометрические характеристики.

20. Опишите принцип работы биометрических систем.

21. Приведите примеры атак на системы, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от подобных атак.

22. Что такое одноразовые пароли.

23. Опишите принцип работы OTP – токеном метода «запрос – ответ».

24. Приведите пример аутентификации пользователя при использовании OTP – токеном метода «только ответ».

25. Приведите пример аутентификации пользователя при использовании OTP – токеном метода « синхронизация по времени».

26. Приведите пример аутентификации пользователя при использовании OTP – токеном метода « синхронизация по событию».

27. Из каких элементов состоит ключевая пара и для чего предназначен каждый элемент.

28. Что такое ЭЦП? Приведите примеры использования.

29. В каких случаях можно использовать криптографию с открытым ключом.

30. Приведите пример использования криптографии с открытым ключом для шифрования сообщения.

31. Приведите пример аутентификации пользователя с помощью открытых ключей (PKI)..

32. Назовите способы хранения закрытого ключа.

33. Назовите недостатки аутентификации с помощью открытых ключей.

34. Приведите примеры атак на системы, использующие аутентификацию с помощью открытых ключей, и способы защиты от подобных атак.

35. Назовите основные особенности протоколов LAN Manager и NT LAN Manager.

36. Назовите типы аутентификации в NTLM.

37. Приведите примеры атак на системы, использующие аутентификацию с помощью протоколов LANMAN и NTLM, и защиты от них.

38. Перечислите преимущества протокола Kerberos.

39. Опишите функции сервера аутентификации, входящего в состав центра распределения ключей протокола Kerberos.

40. Приведите примеры атак на Kerberos и способы защиты от них.

41. Перечислите преимущества реализации протокола Kerberos в ОС Windows 2000 и последующих ОС в сравнении с более ранними продуктами семейства Windows.

42. Приведите пример способа интеграции шифрования в протокол Kerberos.

43. Возможные атаки на Kerberos + PKINIT и методы защиты от них.

44. Какие протоколы включены в механизм аутентификации Point-to-Point Protocol (PPP).

45. Перечислите основные элементы стандарта 802.1x.

46. Какие методы EAP стандарта 802.1x включены в стандартную комплектацию Windows XP.

47. Опишите взаимодействие между пользователем, клиентом и сервером RADIUS.

48. Опишите метод получения ключей шифрования, используемых для PPP.

49. Какие возможности обеспечивает протокол SSL для безопасности связи.

50. Что включает в себя ассоциация безопасности.

51. Перечислите способы аутентификации при использовании протокола IPSec.

52. Какие протоколы IPSec защитить не может.

53. Преимущества протокола IPSec.

54. На каких этапах должна быть обеспечена безопасность закрытого ключа пользователя.

55. Перечислите подходы к обеспечению безопасности закрытых ключей.

56. Перечислите функции централизованной системы управления.

57. Перечислите основные критерии выбора персонального средства аутентификации и хранения ключевой информации.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– Сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.

– Освоение студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

Задачами дисциплины являются:

1. Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
2. Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

2.Указания по проведению практических занятий

3.

Тема 1. Сущность, задачи и особенности конфиденциальной информации

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Сущность, задачи и особенности КД.
2. Документирование КД.
3. Учет КД.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 2. Организация конфиденциального делопроизводства, общие положения

Практическое занятие 2.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные понятия.
2. Характеристика систем доступа к конфиденциальной информации.
3. Организация исполнения конфиденциальных документов.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 3. Документирование конфиденциальной информации

Практическое занятие 3.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Порядок составления номенклатур КД.
2. Формирование дел для КД.
3. Оформление дел для КД.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите

информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 4. Учет конфиденциальных документов

Практическое занятие 4..
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. ПДЭК.
2. Проведение экспертизы ценности КД.
3. Подготовка КД на уничтожение.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 5. Организация конфиденциального документооборота

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятия и принципы организации КД.
2. Система доступа к КД.
3. Организация исполнения и отправления КД.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите

информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 6. Размножение конфиденциальных документов

Практическое занятие 6.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Организация размножения КД.
2. Журнал учета размножения КД.

3. Продолжительность занятия:1.0/1.0 часов

Учебная литература: основная [1,2,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Тема 7. Составление номенклатур конфиденциального документооборота

Практическое занятие 7.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Составление номенклатур КД.
2. Формирование КД.
3. Оформление КД.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт

дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 8. Подготовка КД для архивного хранения и уничтожения

Практическое занятие 8.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Экспертиза КД.
2. Подготовка КД для архивного хранения и уничтожения.
3. Подготовка дел для архивного хранения и уничтожения.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках. ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 9. Режим хранения конфиденциальной информации и обращение с ней

Практическое занятие 9.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Режим хранения КД.
2. Порядок обращения с КД.
3. Назначение, виды и принципы проведения проверок наличия КД.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:1.0/1.0 часов

Тема 10. Проверка наличия конфиденциальных документов

Практическое занятие 10.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Проверки правильности проставления отметок о движении КД, дел и носителей.
2. Квартальные проверки фактического наличия КД и документов.
3. Годовая проверка наличия КД, документов выделенного хранения и учетных журналов (карточек).
4. Не регламентные проверки наличия конфиденциальных носителей, документов и дел.

Учебная литература: основная [1,3]; дополнительная [1,3,4]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия:7.0/3.0 часов

Часть 2 (по выбору преподавателя)

Тема 1. Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации. Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации

Практическое занятие 1.

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. разрешительная система доступа к документам.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные сервисы для обеспечения надежной аутентификации и управления доступом
2. Авторизация при доступе к объекту.
3. Система аудита Active Directoru.
4. Назначение и решаемые задачи инфраструктуры открытых ключей.
5. Управление идентификацией (ILM).
6. Microsoft Identity Integration Server (MIIS).
7. Системы обеспечения.

Тема 2. Составление номенклатуры дел, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации

Практическое занятие 2.

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. составление номенклатуры дел и подготовка их для архивного хранения.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Управление доступом в СУБД Oracle с помощью встроенных механизмов безопасности.
2. Управление доступом в СУБД Oracle с помощью криптографических средств защиты.

Тема 3: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации

Практическое занятие 3.

Практическое занятие 1.
Вид практического занятия**: *подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Описание продуктов компании *CITRIX SYSTEMS.*
2. Компоненты систем, построенных с использованием XenApp.

Тема 4: Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота

Практическое занятие 3.

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

Часть 1: Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003
Часть 2: Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП
Часть 3: Технология программно-аппаратной защиты

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии при построении СЭД.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Часть1:

1.Общие сведения об аутентификации пользователей в домене Windows Server 2003 с помощью цифровых сертификатов и ключей eToken.

2. Установка и настройка Центра сертификации (CA), подготовка консоли Центра сертификации, издание сертификатов

3. Использование ключей eToken для регистрации в домене, для запуска приложений от имени другого пользователя и для подключения сетевых дисков с использованием прав доступа другого пользователя.

Часть2:

1. Общие сведения о безопасном доступе к информационным ресурсам организации.
2. Удаленный доступ к рабочему столу (RDP).
3. Виртуальные частные сети (VPN).
4. Общие сведения о протоколе EAP.
5. Защищенное подключение к Web – серверу (HTTPS).
6. Шифрование и использование ЭЦП.

Часть3:

1. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.

2. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.

3. Механизм удаленного (сетевого) мониторинга активности системы защиты, как альтернатива применению аппаратной компоненте защиты.

Тема 5. Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.

Применение аппаратных средств аутентификации и хранения ключевой информации

Практическое занятие 3.

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

Часть 1: Метод контроля вскрытия аппаратуры
Часть 2: Электронная цифровая подпись

Цель занятия: ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Общий подход к контролю вскрытия аппаратуры техническими средствами защиты.

2. Реализация системы контроля вскрытия аппаратуры.

3. Принципы комплексирования средств защиты информации.

4.Комплексирование механизмов защиты информации от НСД.

5.Комплексирование в одной системе механизмов технической и объектовой защиты информации с единым сервером безопасности.

3. Указания по проведению лабораторных работ

Лабораторная работа 1. Стадии, обработки и защиты конфиденциальных документов входного потока. Стадии обработки и защиты конфиденциальных документов выходного и внутреннего потоков

Цель работы: Закрепление и углубление теоретических знаний полученных на лекционных и практических занятиях и в процессе изучения специальной литературы;
Приобретение навыков использования системы конфиденциального документооборота;
Последовательное практическое изучение системы конфиденциального делопроизводства.

Задание

1. Прием, первичная обработка, предварительное рассмотрение и распределение поступивших конфиденциальных документов.
2. Традиционный учет поступивших документов и формирование справочно – информационного банка данных по документам.
3. Автоматизированный учет поступивших документов и формирование справочно - информационного банка данных по документам.
4. Оформление и учет носителей конфиденциальной информации.
5. Изготовление конфиденциальных документов.
6. Контроль исполнения конфиденциальных документов.
7. Копирование и размножение документов.
8. Учет подготовленных (изданных КД).
9. Инвентарный учет документов и изданий.
10. Экспедиционная обработка документов.
11. Оформить отчет по лабораторной работе.
12. Ответить на контрольные вопросы.

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия: 4.0/3.0 часов

Лабораторная работа 2. Систематизация и оперативное хранение конфиденциальных документов и дел

Цель работы: Закрепление и углубление теоретических знаний полученных на лекционных и практических занятиях и в процессе изучения специальной литературы;
Приобретение навыков использования системы конфиденциального документооборота;
Последовательное практическое изучение системы конфиденциального делопроизводства.

Задание

1. Номенклатура дел.
2. Формирование и оформление дел.
3. Уничтожение документов, дел и носителей информации.
4. Подготовка дел к передаче в ведомственный архив.
5. Оформить отчет по лабораторной работе.
6. Ответить на контрольные вопросы.

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия: 4.0/3.0 часов

Лабораторная работа 3. Архивное хранение конфиденциальных документов и дел

Цель работы: Закрепление и углубление теоретических знаний полученных на лекционных и практических занятиях и в процессе изучения специальной литературы;
Приобретение навыков использования системы конфиденциального документооборота;
Последовательное практическое изучение системы конфиденциального делопроизводства.

Задание

1. Номенклатура дел.
2. Формирование и оформление дел.
3. Уничтожение документов, дел и носителей информации.
4. Подготовка дел к передаче в ведомственный архив.
5. Оформить отчет по лабораторной работе.
6. Ответить на контрольные вопросы.

Учебная литература: основная [1,2,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия: 4.0/3.0 часов

Лабораторная работа 4. Проверка наличия конфиденциальных документов, дел и носителей информации

Цель работы: Закрепление и углубление теоретических знаний полученных на лекционных и практических занятиях и в процессе изучения специальной литературы;
Приобретение навыков использования системы конфиденциального документооборота;
Последовательное практическое изучение системы конфиденциального делопроизводства.

Задание

1. Комплектование ведомственного архива, классификация и учет дел.
2. Организация использования архивных документов и обеспечения их сохранности.
3. Оформить отчет по лабораторной работе.
4. Ответить на контрольные вопросы.

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1,2].

Продолжительность занятия: 4.0/3.0 часов

Часть 2:

Учебные вопросы

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой,

изложенными выше. Запустить программу labWork6.exe, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.

2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.

5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.

6. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта

Примечание: по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Раздел I. Организация обработки конфиденциальных документов**	***Подготовка докладов по темам:*** 1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения. 2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения. 3. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS. 4. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД. 5. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия.

		6. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД. 7. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД. 8. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия. 9. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия. 10. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств. 11. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет. 12. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации. 13. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям. 14. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД. 15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

		16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД). 17. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.
2.	**Раздел II. Технологии защиты конфиденциальных документов**	***Подготовка докладов по темам:*** 1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения. 2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения. 3. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS. 4. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД. 5. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия. 6. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД. 7. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД. 8. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия. 9. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения

		целостности информации; потенциально возможные злоумышленные действия. 10. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств. 11. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет. 12. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации. 13. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям. 14. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД. 15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации. 16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД). 17. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.
3	**Раздел III. Обеспечение режима конфиденциальности безопасного допуска к**	***Подготовка докладов по темам:*** 1. Оформление конфиденциальных дел. 2. (формы карточек учета, опись документов, заверительная надпись). 3. Экспертиза ценности конфиденциальных документов.

	информационным ресурсам	4. Подготовка конфиденциальных дел и документов для архивного хранения. 5. (формы описи дел) 6. Подготовка конфиденциальных дел и документов для уничтожения. 7. (форма акта) 8. Режим хранения конфиденциальных документов. 9. (формы журналов учета) 10. Порядок обращения с конфиденциальными документами 11. (форма описи) 12. Назначение, виды и принципы проведения проверок наличия конфиденциальных документов. 13. Проверки правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (картотек). 14. Проверки правильности проставления отметок о движении конфиденциальных документов, дел и носителей. 15. Квартальные проверки фактического наличия конфиденциальных носителей и документов (форма акта). 16. Годовая проверка наличия конфиденциальных дел, документов выделенного хранения и учетных журналов (картотек). 17. (форма акта) 18. Не регламентные проверки наличия конфиденциальных носителей, документов и дел. 19. Информационная безопасность электронных платежуй с помощью цифровых денег. 20. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами. 21. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах. 22. Информационная безопасность и правила обмена электронными документами. Общие

		требования, предъявляемые к ЭД (пакетам ЭД). 23. Информационная безопасность при составление и направление ЭД участником – отправителем. 24. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. 25. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.
4	**Раздел IV. Реализация механизмов защиты для обработки конфиденциальной информации в системах защищенного документооборота**	***Подготовка докладов по темам:*** 1. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД. 2. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД. 3. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД. 4. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД. 5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД. 6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию. 7. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД. 8. Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа

		(для СЭД).

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4.Примерная тематика контрольных работ:

1. Сущность, задачи и особенности конфиденциального делопроизводства.
2. (виды тайны, утечка или утрата информации, особенности).
3. Организация конфиденциального делопроизводства.
4. (должностные инструкции, оборудование помещения, задачи ПДЭК).
5. Состав конфиденциальных документов.
6. Оформление и учет носителей конфиденциальной информации.
7. (формы журналов учета)
8. Изготовление и учет проектов конфиденциальных документов.
9. (формы журналов учета).
10. Оформление издаваемых конфиденциальных документов.

11. (реквизиты документа).
12. Общие требования к учету конфиденциальных документов.
13. Учет изданных документов.
14. (формы журналов учета)
15. Учет поступивших документов.
16. (формы журналов учета)
17. Учет конфиденциальных документов выделенного хранения.
18. (формы журналов учета)
19. Размножение конфиденциальных документов
20. (формы журналов учета)
21. Понятия и принципы организации конфиденциального документооборота.
22. Система доступа к конфиденциальным документам.
23. Организация исполнения конфиденциальных документов.
24. (формы журналов учета, оформление документа)
25. Отправление конфиденциальных документов.
26. Составление номенклатур конфиденциальных дел.
27. (формы журналов учета)
28. Формирование конфиденциальных дел
29. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения.
30. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения.
31. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS.
32. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД.
33. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия.
34. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД.
35. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД.
36. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
37. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия.

38. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.
39. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет.
40. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.
41. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.
42. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.
43. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.
44. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД).
45. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.
46. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
47. Информационная безопасность при составление и направление ЭД участником – отправителем.
48. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
49. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

11. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
12. http://informika.ru/ – образовательный портал.

13. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
14. www.biblioclub.ru - Универсальная библиотека онлайн.
15. www.rucont.ru - ЭБС «Руконт».
16. http://www.academy.it.ru/ – академия АЙТИ.
17. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
18. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
19. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Конфиденциальное делопроизводство и защищенный электронный документооборот»»