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

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
_____ 2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА»

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования: специалитет
Квалификация (степень) выпускника: экономист
Форма обучения: очная, 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: «Безопасность электронного документооборота» – Королев МО: «Технологический университет», 2023.

Рецензент: **к.в.н., доцент Воронов А.Н.**

Программа составлена в соответствии с требованиями федерального Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Самигов В.К., к.в.н., доцент				
Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023 г.				

Рабочая программа согласована:
Руководитель ОПОП_____ к.э.н., доцент Коба Е.Е.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023 г.				

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

Целью изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации в СЭДО;
2. Усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации в СЭДО, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Универсальные компетенции:

- УК-1- Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

Профессиональные компетенции:

- ПК-4- Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

УК-1.1-Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними;

УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению;

УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников;

УК-1.И-4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов;

УК-1. И-5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области;

ПК-4. И-1Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности;

ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-

информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками;
ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности;
ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.

Необходимые умения:

УК-1И-1.У-1 Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними;
УК-1. И-2. У-1 Умеет определять пробелы в информации, необходимой для решения проблемной ситуации;
УК-1. И-2. У-2 Умеет проектировать процессы по устранению пробелов в информации;
УК-1. И-3. У-1 Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников;
УК-1.И-4.У-1 Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов
УК-1.И-5.У-1 Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области

ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками;
ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации,
ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному обеспечению системы стратегического управления рисками;
ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации,
ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками
ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией,
ПК-4.И-3. У-2 Умеет применять принципы и методы управления проектами,
ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками
ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя

ПК-4. И-5. У-1 Умеет использовать в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья
ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации

Необходимые знания:
УК-1. И-1. З-1 . Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними
УК-1. И-2. З-1 Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации;
УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации;
УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников.
УК-1. И-4. З-1 Знает методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов
УК-1. И-5. З-1 Знает современные концепции философского и социального характера в своей предметной области, методологический инструментарий для их критической оценки

ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками;
ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации,
ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками;
ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками
ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками
ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией
ПК-4.И-3. З-2 Знает принципы и методы управления проектами
ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных)
ПК-4. И-5. З-1 Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации,
ПК-4. И-5. З-2 Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими средствами для людей с ограниченными возможностями здоровья
ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации;
ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота;
ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации.

2. Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Безопасность электронного документооборота» относится к части, формируемой участниками образовательных отношений дисциплин по выбору Блока 1 основной профессиональной образовательной программы подготовки специалистов по направлению 38.05.01 «Экономическая безопасность». Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на знаниях, полученных в средней общеобразовательной школе.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Экономическая безопасность», «Информационные системы в экономике», «Информационная безопасность операционных систем и баз данных», «Безопасность банковских и платежных ИС» и выполнении выпускной квалификационной работы специалиста.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и заочной формы составляет 3 зачетных единицы, 108 часов.

Виды занятий	**Всего часов**	**Семестр** 3	**Семестр** 4	**Семестр**	**Семестр** …
Общая трудоемкость	**108**	**108**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**48**	**48**			
Лекции (Л)	**16**	**16**			
Практические занятия (ПЗ)	**32**	**32**			
Лабораторные работы (ЛР)	**-**	**-**			
Самостоятельная работа	**60**	**60**			
Практическая подготовка	нет	нет			
Курсовые работы (проекты)	**-**	**-**			
Расчетно-графические работы	**-**	**-**			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний	**Тесты**	**Тесты**			
Вид итогового контроля	**Зачет с оценкой**	**Зачет с оценкой**			
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**12**	**12**			
Лекции (Л)	**4**	**4**			
Практические занятия (ПЗ)	**8**	**8**			
Лабораторные работы (ЛР)	**-**	**-**			
Практическая подготовка	**нет**	**нет**			

Самостоятельная работа	**96**	**96**			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Вид итогового контроля	**Экзамен**	**Экзамен**			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Заочное	Практические занятия, час. Заочное	Занятия в интерактивной форме, час	Код компетенций
Раздел 1. Обеспечение режима конфиденциальности безопасного допуска к информационным ресурсам				
Тема 1. Понятие и особенности СЭДО	3/0.5	6/1	6/0.5	УК-1; ПК-4.
Тема 2. Составление номенклатуры дел, формирование и оформление конфиденциальных дел	3/0.5	6/1	6/0.5	УК-1; ПК-4.
Раздел 2. Реализация механизмов защиты для обработки конфиденциальной информации в системах защищенного документооборота				
Тема 3: Система защищенного электронного документооборота.	3/1	6/2	6/1	УК-1; ПК-4.
Тема 4.Построение СЭД без существенных настроек типовой IT – архитектуры.	3/1	6/2	6/1	УК-1; ПК-4.
Тема 5. Применение аппаратных средств аутентификации и хранения ключевой информации	4/1	8/2	8/1	УК-1; ПК-4.
Итого:	16/4	32/8	32/4	

4.2. Содержание тем дисциплины

Раздел 1. Обеспечение режима конфиденциальности безопасного допуска к информационным ресурсам

Тема 1. 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 2. 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 2. Реализация механизмов защиты для обработки конфиденциальной информации в системах защищенного документооборота

Тема 3: 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 4: 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 5. 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 «Безопасность электронного документооборота» приведена в Приложении 1.

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

Основная литература:

1. Мошак Н.Н. Защищенные информационные системы [Электронный ресурс]: учебное пособие / Мошак Н.Н., Птицына Л.К. - Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. - 216 с. URL: https://e.lanbook.com/book/180099

2. 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: 03.10.2022). – Режим доступа: по подписке.

Дополнительная литература:

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. http://znanium.com/bookread2.php?book=851088

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8.
URL: http://znanium.com/go.php?id=544554

4. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник/Н.Н. Куняев, А.С. Демушкин и др. 2-е изд, перераб и доп - М.: Логос, 2015.-500 с. (Новая университетская библиотека) ISBN 978-5- 98704-711-8

5. Додонова И.В. Автоматизированная обработка банковской информации. уч. пос.- М. КНОРУС.2014-170 с. SBN 978-5- 406-035333-7

6. Управление рисками организации : Учебное пособие / Антонов Геннадий Дмитриевич, Валерий Максимович, Ольга Петровна. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 153 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-16-010203-0.
URL: http://znanium.com/go.php?id=475625

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 (модуля) приведены в Приложении 2 к настоящей рабочей программе.

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

- **Перечень программного обеспечения:** MS Office, Power Point.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность электронного документооборота»

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 Windows; офисные программы MS Office 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

«БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА»

Специальность подготовки: 38.05.01 Экономическая безопасность

Специализация: экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2022

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;	Тема:1,2,3,4,5	УК-1.1-Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; УК-1.И-4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов; УК-1. И-5 Использует логико-методологический инструментарий для критической оценки современных концепций	УК-1И-1.У-1 Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними; УК-1. И-2. У-1 Умеет определять пробелы в информации, необходимой для решения проблемной ситуации; УК-1. И-2. У-2 Умеет проектировать процессы по устранению пробелов в информации; УК-1. И-3. У-1 Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников; УК-1.И-4.У-1 Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе	УК-1. И-1. З-1 . Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними УК-1. И-2. З-1 Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой

				философского и социального характера в своей предметной области;	системного и междисциплинарных подходов УК-1.И-5.У-1 Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	информацией из различных источников. УК-1. И-4. З-1 Знает методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов УК-1. И-5. З-1 Знает современные концепции философского и социального характера в
2.	ПК-4	Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегическо	Тема:1,2,3,4,5	ПК-4. И-1 Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-	ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности ПК-4. И-2. У-1 Умеет координировать	ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации, ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности

		го управления рисками		информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые,	работы по технико-информационному обеспечению системы стратегического управления рисками; ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией, ПК-4.И-3. У-2 Умеет применять принципы и методы управления	ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками; ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией ПК-4.И-3. З-2 Знает принципы и методы управления проектами ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств

				графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя ПК-4. И-5 Использует в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья ПК-4. И-6 Решает поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной	проектами, ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками; ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя. ПК-4. И-5. У-1 Умеет использовать в профессиональной деятельности основные	в области управления информационными технологиями и информационной безопасности ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) ПК-4. И-5. З-1 Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, ПК-4. И-5. З-2 Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими

				информации	методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	средствами для людей с ограниченными возможностями здоровья ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации; ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота; ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации

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

Код компетенции	**Инструменты, оценивающие сформированность компетенции**	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1, ПК-4	*Тест*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 90% правильных ответов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 70% правильных ответов;* • *компетенция освоена на базовом уровне – от 51% правильных ответов;* *В) не сформирована (компетенция не сформирована) – менее 50% правильных ответов*	*Проводится письменно. Время, отведенное на процедуру - 30 минут.* *Неявка – 0 баллов.* *Критерии оценки определяются процентным соотношением.* *Неудовлетворительно – менее 50% правильных ответов.* *Удовлетворительно - от 51% правильных ответов.* *Хорошо - от 70%.* *Отлично – от 90%.* *Максимальная оценка – 5 баллов.*
УК-1, ПК-4	Доклад в форме презентации	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	***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.***
УК-1, ПК-4	***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. 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).

Примерная тематика заданий на контрольную работу:

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.
18. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
19. Информационная безопасность при составление и направление ЭД участником – отправителем.

20. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
21. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

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

Формой контроля знаний по дисциплине «Безопасность электронного документооборота» являются две текущие аттестации в виде тестов и одна промежуточная 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	УК-1; ПК-4	30 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Проводится в сроки, установленные графиком образовательного	тестирование	УК-1; ПК-4	30 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно -

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
процесса						от 51% правильных ответов.
Проводится в сроки, установленные графиком образовательного процесса	Зачет	УК-1; ПК-4	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	***критерии оценки: «Зачтено»:*** • ***знание основных понятий предмета;*** • ***умение использовать и применять полученные знания на практике;*** • ***работа на семинарских занятиях;*** • ***знание основных научных теорий изучаемых***

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
						предметов; • *ответ на вопросы билета.* *«Не зачтено»:* • *демонстрирует частичные знания по темам дисциплин;* • *незнание основных понятий предмета;* • *неумение использовать и применять полученные знания на практике;* • *не работал на семинарских занятиях;* *не*

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
						отвечает на вопросы.

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, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

Тестовые задания

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.

7. По каким основным направлениям целесообразно проводить оценку возможных угроз

(!) обеспечение стабильности общества, государства

(!) обеспечение безопасности национальных интересов

(!) обеспечение безопасности информации

(?) обеспечение защиты информационных ресурсов предприятий

8. Что может рассматриваться в качестве угроз развитию отечественной индустрии информации

(!) Противодействие доступу РФ к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий

(!) Закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам

(!) Вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи

(?) Низкая эффективность информационного обеспечения государственной политики Российской Федерации

9. Какие из перечисленных направлений являются основными направлениями ведения информационных войн?

(!)воздействие на информационные ресурсы и аппаратно-программные средства противника

(!) психологическое воздействие на живых людей

(?) клевета на страну-противника

(?) психологическое воздействие на животных

10. К числу исключительных правовых режимов, которые могут вводиться на территории страны или отдельных ее регионов не относится:

(!) специальный

(?) военное положение

(?) чрезвычайное положение

(?) режим контртеррористической операции

11. Чрезвычайное положение вводится лишь при наличии обстоятельств, которые представляют собой непосредственную угрозу жизни и безопасности граждан или конституционному строю Российской Федерации и устранение которых невозможно без применения чрезвычайных мер. К таким обстоятельствам относятся:

(!) попытки насильственного изменения конституционного строя Российской Федерации, захвата или присвоения власти, вооруженный мятеж, массовые беспорядки, террористические акты, блокирование или захват особо важных объектов или отдельных местностей, подготовка и деятельность незаконных вооруженных формирований, межнациональные, межконфессиональные и региональные конфликты, сопровождающиеся

насильственными действиями, создающие непосредственную угрозу жизни и безопасности граждан, нормальной деятельности органов государственной власти и органов местного самоуправления;

(!) чрезвычайные ситуации природного и техногенного характера,

чрезвычайные экологические ситуации, в том числе эпидемии и эпизоотии, возникшие в результате аварий, опасных природных явлений, катастроф, стихийных и иных бедствий, повлекшие (могущие повлечь) человеческие жертвы, нанесение ущерба здоровью людей и окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности населения и требующие проведения масштабных аварийно-спасательных и других неотложных работ.

(?) другие ситуации

(?) чрезвычайное положение вводится по желанию народа

12. Основными объектами национальной безопасности страны являются:

(!) Личность, общество, государство;

(?) Гос.бюджет, общество, личность;

(?) Общество, государство, президент;

(?) Президент, государство, личность;

13. По природе возникновения угрозы безопасности делятся на:

(?) Глобальные и локальные;

(?) Личные и территориальные;

(!) Объективные и субъективные;

(?) Внутренние и внешние;

14. Основными приоритетами информационной безопасности в РФ являются:

(?) Государственная безопасность, безопасность правительства РФ, безопасность личности;

(!) Национальная оборона, государственная безопасность, общественная безопасность;

(?) Безопасность правительства РФ, общественная безопасность, безопасность личности;

(?) Общественная безопасность, национальная оборона, безопасность правительства РФ.

15. Основной целью совершенствования нормативно-правового обеспечения информационной безопасности является:

(?) устранение пробелов в законодательстве, препятствующих организации эффективного противодействия угрозам

(?) создание системы сбора и анализа данных об источниках угроз информационной безопасности

(!) создание условий для ликвидации, предупреждения и пресечения проявлений угроз безопасности основных объектов национальных интересов

(?) создание системы сбора и анализа данных об источниках угроз информационной безопасности

16. Одним из основных направлений совершенствования нормативно-правового обеспечения безопасности объектов национальных интересов в информационной сфере является:

(?) создание организационно-правовых механизмов обеспечения информационной безопасности;

(!) повышение структурной упорядоченности нормативных правовых актов

(?) определение правового статуса всех субъектов отношений

(?) совершенствование системы подготовки кадров

17. К Специфическим направлениям обеспечения информационной безопасности для чрезвычайных условий Доктрина не относит:

(?) Разработку эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций

(?) совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуации, об условиях их возникновения и развития

(?) повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;

(!) разработку системы информирования населения в чрезвычайных ситуациях

18. Выберите неверный вариант. Террористическая деятельность включает в себя:

(?) организацию, планирование, подготовку, финансирование и реализацию террористического акта

(?) организацию, планирование, подготовку, финансирование и реализацию террористического акта

(?) вербовку, вооружение, обучение и использование террористов;

(!) информационный шпионаж

19. Выберите неверный вариант. Противодействие терроризму - это деятельность, включающая в себя:

(?) предупреждение терроризма, в том числе по выявлению и последующему устранению причин и условий, способствующих совершению террористических актов (профилактика терроризма);

(?) выявление, предупреждение, пресечение, раскрытие и расследование террористического акта (борьба с терроризмом);

(?) минимизация и (или) ликвидация последствий проявлений терроризма;

(!) проведение контртеррористической операции

20. На территории (объектах), в пределах которой (на которых) введен правовой режим контртеррористической операции, в порядке, предусмотренном законодательством Российской Федерации, на период ее проведения допускается применение ряда мер и временных ограничений. К ним не относится:

(?) ведение контроля телефонных переговоров

(?) ведение контроля иной информации, передаваемой по каналам телекоммуникационных систем

(?) осуществление поиска на каналах электрической связи и в почтовых отправлениях

(!) контроль всего персонала

21. Какова главная задача при президенте РФ, по противодействию попыткам фальсификации Истории в ущерб интересам России, которая была образована в соответствии с указом Президента РФ от 15 мая 2009г?

(!) обеспечение согласованной деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и организаций, направленной на противодействие попыткам фальсификации истории в ущерб интересам России.

(?) обеспечение своевременной деятельности федеральных органов государственной власти, направленной на противодействие попыткам фальсификации истории в ущерб интересам России.

(?) обеспечение согласованной деятельности федеральных органов государственной власти, направленной на противодействие техническим средствам разведки.

(?) обеспечение финансирования деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и организаций, направленной на противодействие попыткам фальсификации истории в ущерб интересам России.

Вопросы к зачету с оценкой

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.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА»

(Приложение 2 к рабочей программе)

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Квалификация (степень) выпускника: экономист
Форма обучения: очная, заочная

Королев

2023

1. Общие положения

Цель дисциплины:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации в СЭДО;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации в СЭДО, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

Задачи дисциплины:

Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации и формированием у обучающихся системы знаний, умений и навыков по защите информации, обеспечению информационной безопасности граждан, общества и государства. В том числе:

- построение разрешительной системы доступа к конфиденциальной информации;
- определение номенклатуры дел, формирование и оформление конфиденциальных дел;
- разносторонний обзор систем электронного документооборота;
- раскрытие общих положений по защите информации в СЭД;
- научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации с СЭД;
- ознакомить студентов при решении поставленных задач с помощью перспективных технологий и методов защиты информации;
- ознакомить студентов с методикой применения и использования встроенных механизмов защиты информации;
- ознакомить студентов с порядком применения средств добавочной защиты информации.

2. Указания по проведению практических занятий

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

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

Образовательные технологии: *групповая дискуссия*

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.

Продолжительность занятия: 7/1 час.

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.

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

Образовательные технологии: *групповая дискуссия*

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.

Продолжительность занятия: 7/2 часа.

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

Практическое занятие 3

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

Образовательные технологии: *групповая дискуссия*

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.

Продолжительность занятия: 6/1 часа.

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

Практическое занятие 4

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

Образовательные технологии: *групповая дискуссия*

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:

Часть 1:

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.

Продолжительность занятия: 6/2 часа.

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 5

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

Образовательные технологии: *групповая дискуссия*

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.

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).

Продолжительность занятия: 6/2 часа.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных защищенных систем ЭДО;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения/заочная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**60/96**
Вопросы, выносимые на самостоятельное изучение	15/24
Подготовка к практическим занятиям	15/24
Подготовка к лабораторным занятиям	-
Подготовка докладов	15/24
Выполнение практических заданий	15/24

Вопросы, выносимые на самостоятельное изучение:
для заочной формы обучения:

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

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.

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.

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

4. 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).

5. 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.

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).

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	15/24	Изучение открытых источников
2.	Подготовка к практическим занятиям	15/24	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	Изучение открытых источников
4.	Тематика докладов	15/24	
5.	Выполнение практических заданий	15/24	

Примерные темы докладов

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. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

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).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Мошак Н.Н. Защищенные информационные системы [Электронный ресурс]: учебное пособие / Мошак Н.Н., Птицына Л.К. - Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. - 216 с. URL: https://e.lanbook.com/book/180099

2. 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: 03.10.2022). – Режим доступа: по подписке.

Дополнительная литература:

- Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 (дата обращения: 03.10.2022). – Режим доступа: по подписке.
- Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. http://znanium.com/bookread2.php?book=851088
- Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8.
URL: http://znanium.com/go.php?id=544554
- Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник/Н.Н. Куняев, А.С. Демушкин и др. 2-е изд, перераб и доп - М.: Логос, 2015.-500 с. (Новая университетская библиотека) ISBN 978-5- 98704-711-8
- Додонова И.В. Автоматизированная обработка банковской информации. уч. пос.- М. КНОРУС.2014-170 с. SBN 978-5- 406-035333-7
- Управление рисками организации : Учебное пособие / Антонов Геннадий Дмитриевич, Валерий Максимович, Ольга Петровна. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 153 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-16-010203-0.
URL: http://znanium.com/go.php?id=475625

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

Перечень программного обеспечения: *MS Office, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине «Безопасность электронного документооборота».