



Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Кафедра информационной безопасности
Факультет информационных технологий и анализа больших данных

Документ подписан усиленной неквалифицированной электронной подписью.

Организация: «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сертификат: 3QREm61yNtPWmV7l8ZSchOFI5RHLM8ns

Утверждено: Проректор по учебной и методической работе, Е.А. Каменева

Дата: 08.12.2025 г.

С.А. Резниченко , А.Ю. Васильева
Основы информационной безопасности

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
09.03.04 - Программная инженерия,
Образовательная программа «Разработка и внедрение информационно -
аналитических систем»
Профиль:
«Разработка и внедрение информационно - аналитических систем»

Рекомендовано
Факультет информационных технологий и анализа больших данных
(протокол № 09 от 16.06.2026 г.)

Одобрено
Кафедра информационной безопасности
(протокол № 2 от 20.10.2025 г.)



Содержание

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	6
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	6
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	7
5.1. Содержание дисциплины	7
5.2. Учебно – тематический план	9
5.3. Содержание семинаров, практических занятий	11
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	19
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	19
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	22
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	24
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	6
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	9
10. Методические указания для обучающихся по освоению дисциплины	38
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	39
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	39



1. Наименование дисциплины

Основы информационной безопасности

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКП-4	Способность разрабатывать и предлагать архитектурные решения для информационно-аналитических систем	Умеет выбирать архитектурные решения для разрабатываемых информационных систем.	Знать: основы архитектуры, устройства и функционирования вычислительных систем. Уметь: идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки.
		Способен выбирать современные технологии, методы и подходы к реализации архитектурных решений.	Знать: методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Уметь: формировать технические и организационные меры для защиты программной системы от несанкционированного доступа к элементам конфигурации.
		Способен проводить интеграцию архитектурных и проектных решений для информационных систем с существующими решениями.	Знать: основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации. Уметь: оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		Умеет оформлять проектную документацию в соответствии с действующими стандартами.	Знать: нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Уметь: консультировать персонал автоматизированной системы по комплексу мер (правилам, процедурам, практическим приемам, руководящим принципам, методам, средствам) обеспечения защиты информации.
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике.	Знать: нормативные правовые акты, организационно-распорядительные документы и методические документы, определяющие требования к безопасности программного обеспечения. Уметь: формировать технические и организационные меры для защиты программной системы от несанкционированного доступа к элементам конфигурации.
		Проводит систематический обзор источников информации, анализировать содержащиеся в них данные, делать и обосновывать выводы на основе проведенного обзора.	Знать: методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Уметь: описывать и оценивать перечень элементов архитектуры, которые должны быть защищены от угроз безопасности информации, связанных с нарушением конфиденциальности, целостности и доступности.
		Демонстрирует знания основных требований информационной без-	Знать: методы управления требованиями по созданию комплексных систем информационной безопасности.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		опасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	Уметь: проверять требования с точки зрения их соответствия архитектуре системы информационной безопасности.



3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к «Циклу профиля».

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	5/180	180
Контактная работа – Аудиторные занятия	50	50
<i>Лекции</i>	<i>16</i>	<i>16</i>
<i>Семинары, практические занятия</i>	<i>34</i>	<i>34</i>
<i>Самостоятельная работа</i>	<i>130</i>	<i>130</i>
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен



5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Государственная политика в области информационной безопасности в системе национальной безопасности

Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности, краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности. Национальные интересы личности, общества и государства в информационной сфере. Основные направления реализации информационного суверенитета России. Государственные органы обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства. Основные нормативные акты в области обеспечения информационной безопасности.

Тема 2. Информационные уязвимости объектов и угрозы информационной безопасности

Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности. Угрозы конфиденциальности, целостности и доступности информации. Классификация угроз информационной безопасности. База данных угроз информационной безопасности ФСТЭК России.

Тема 3. Современные инновационные технологии: преимущества и социальные последствия

Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Основные факторы, способствующие в настоящее время повышению уязвимости информации в ИС и ИТКС. Обзор компьютерных преступлений в России и в мире. Базовые инновационные технологии XXI века. Негативные аспекты, возникающие с развитием современных технологий и глобальных сетей и отрицательно влияющие на общество. Основные типы интернет-зависимости. Базовые интернет-риски для детей. Негативное влияние гаджетов на мышление



человека. Основные симптомы социальной зависимости от соцсетей. Влияние отмены письма на личностные качества человека.

Тема 4. Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности

Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Базовые угрозы безопасности личности. Основные права государства для обеспечения безопасности граждан. Базовый методический подход к изучению проблем ИБ. Основные функции органов системы ИБ. Базовые структурные компоненты системы ИБ. Основные факторы, воздействующие на информационную безопасность как социальную систему. Социальный подход к защите информации как средство методологического анализа информационной безопасности

Тема 5. Общие вопросы организации системы защиты информации в бизнесе

Технические, правовые и организационные методы и средства защиты информации. Защита от негативного воздействия. Требования законодательства по обеспечению бесперебойности функционирования систем и непрерывности бизнеса. Стандарты и лучшие практики обеспечения непрерывности бизнеса. Показатели бесперебойности функционирования систем. Базовые функции системы информационного противодействия. Система мероприятий по защите личности и социума от информационно-психологических операций. Способы срыва информационно-психологического воздействия противника на социальные системы бизнеса. Базовые этапы ликвидации последствий информационно-психологических операций противника. Основные направления достижения эффективной информационной защиты социальных систем и предприятий. Индикаторы манипулятивного информационного воздействия на служащих.



5.2. Учебно – тематический план

Очная форма обучения

п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Государственная политика в области информационной безопасности в системе национальной безопасности	32	6	2	4	26
2	Информационные уязвимости объектов и угрозы информационной безопасности	34	8	2	6	26
3	Современные инновационные технологии: преимущества и социальные последствия	38	12	4	8	26
4	Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	38	12	4	8	26
5	Общие вопросы организации системы защиты информации в бизнесе	38	12	4	8	26



п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная 			



5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Государственная политика в области информационной безопасности в системе национальной безопасности	Национальные интересы личности, общества и государства в информационной сфере. Государственные органы обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства. Основные нормативные акты в области обеспечения информационной безопасности.	Семинар-моделирование «Заседание Совета Безопасности» Форма: Ролевая игра, имитирующая выработку государственного решения. Цель: Применить теоретические знания для выработки практических мер реагирования на угрозу. Сценарий: Вводная: «Выявлена атака на ГИС ЖКХ региона с подменой данных о поставках тепла. Возможна техногенная катастрофа. Проходит заседание Совбеза». Роли (5–7 человек): • Председатель Совбеза (преподаватель или сильный студент) • Министр цифрового развития • Директор ФСТЭК • Руководитель НКЦКИ (ГосСОПКА) • Представитель МЧС (последствия) • Юрист (правовые основания для отключения трафика) Задачи:



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
		• Оценить угрозу (внешняя / внутренняя? целевая / хаотичная?). • Принять решение (локализовать узел, включить резервные каналы, изменить шифрование). • Оформить проект протокола заседания. Результат: Один итоговый документ (протокол оперативного совещания) с конкретными мерами.
Информационные уязвимости объектов и угрозы информационной безопасности	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз.	Семинар. Аналитическое структурирование «Построение карты угроз» Форма: Индивидуально-групповая работа с таксономической таблицей (метод «классификационной матрицы»). Цель: научиться самостоятельно классифицировать любую угрозу информационной безопасности по нескольким основаниям (источник, объект воздействия, свойство информации). Этапы проведения: Этап 1. Рассмотрение квалификации угроз ИБ Этап 2. Индивидуальная работа — карточки Каждый студент получает 10–12 карточек с описанием реальных угроз. Задача: заполнить матрицу, отнеся каждую угрозу к трём категориям. Пример карточки №1:



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий																					
		«Сотрудник банка случайно отправил файл с данными клиентов на личную почту, настроив автоответчик» <table><tr><th>№</th><th>Признак</th><th>Ответ студента</th></tr><tr><td>1.</td><td>Источник</td><td>Эндогенная (внутренняя халатность)</td></tr><tr><td>2.</td><td>Природа</td><td>Антропогенная (неумышленная)</td></tr><tr><td>3.</td><td>Цель (CIA)</td><td>Конфиденциальность</td></tr></table> Пример карточки №2: «Хакерская группа запустила шифровальщик, который зашифровал файлы на сервере и требует выкуп» <table><tr><th>№</th><th>Признак</th><th>Ответ студента</th></tr><tr><td>1</td><td>Источник</td><td>Экзогенная</td></tr><tr><td>2</td><td>Природа</td><td>Антропогенная (умышленная)</td></tr></table>	№	Признак	Ответ студента	1.	Источник	Эндогенная (внутренняя халатность)	2.	Природа	Антропогенная (неумышленная)	3.	Цель (CIA)	Конфиденциальность	№	Признак	Ответ студента	1	Источник	Экзогенная	2	Природа	Антропогенная (умышленная)
№	Признак	Ответ студента																					
1.	Источник	Эндогенная (внутренняя халатность)																					
2.	Природа	Антропогенная (неумышленная)																					
3.	Цель (CIA)	Конфиденциальность																					
№	Признак	Ответ студента																					
1	Источник	Экзогенная																					
2	Природа	Антропогенная (умышленная)																					



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий			
		№	Признак	Ответ студента	
		3	Цель (CIA)	Доступность Целостность	+
		Этап 3. Проверка в парах Студенты обмениваются матрицами, проверяют, аргументируют несогласия. Этап 4. Общее обсуждение спорных кейсов Преподаватель выносит на экран самые спорные угрозы (например: «сбой питания ИБП из-за скачка напряжения, вызванного ураганом» → экзогенная? техногенная? Какая CIA?). Этап 5. Рефлексия Каждый студент устно называет одну угрозу, которая раньше не казалась ему угрозой, и поясняет почему. Результат: Заполненная классификационная матрица (10–12 угроз) в тетради каждого студента.			
Современные инновационные технологии: преимущества и социальные последствия	Обзор компьютерных преступлений в России и в мире. Базовые инновационные технологии XXI века. Негативные аспекты, возникающие с развитием современных технологий и глобальных сетей и отрицательно влияющие на общество. Основные	Семинар. Дебаты «Технологический прогресс: благо или угроза?» Форма: Структурированные академические дебаты. Цель: Научиться взвешенно оценивать социальные последствия внедрения базовых инновационных			



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий												
	типы интернет-зависимости. Программно-аппаратные средства обеспечения информационной безопасности.	технологий XXI века (ИИ, биотех, нейроинтерфейсы, квантовые вычисления). Тезисы для обсуждения: «Искусственный интеллект принесет человечеству больше пользы, чем вреда». «Развитие глобальных сетей сделало общество более уязвимым, чем защищенным». «Государство должно законодательно ограничить развитие квантовых вычислений до появления квантово-безопасной криптографии». Регламент (90 мин): <table><tr><th>№ пп</th><th>Этап</th><th>Время</th><th>Действие</th></tr><tr><td>1</td><td>Жеребьевка и подготовка</td><td>10 мин</td><td>Деление на 2 команды (утверждающие / отрицающие), капитан</td></tr><tr><td>2</td><td>Раунд 1</td><td>5 мин</td><td>Кейс утверждающей стороны</td></tr></table>	№ пп	Этап	Время	Действие	1	Жеребьевка и подготовка	10 мин	Деление на 2 команды (утверждающие / отрицающие), капитан	2	Раунд 1	5 мин	Кейс утверждающей стороны
№ пп	Этап	Время	Действие											
1	Жеребьевка и подготовка	10 мин	Деление на 2 команды (утверждающие / отрицающие), капитан											
2	Раунд 1	5 мин	Кейс утверждающей стороны											



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий			
		№ пп	Этап	Время	Действие
		3	Раунд 2	5 мин	Кейс отрицающей стороны
		4	Раунд 3	5 мин	Перекрестные вопросы
		5	Раунд 4	4 мин	Заключительное слово (по 2 мин каждой стороне)
		6	Рефлексия	5 мин	Зрители (незадействованные студенты) голосуют за убедительность
		Результат: Протокол дебатов с фиксацией сильнейших аргументов «за» и «против» по каждой технологии.			



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	1. Человек как «слабое звено»: объективная реальность или управленческая ошибка? 2. Социальная инженерия как системная угроза: классификация атак и психологические уязвимости. 3. Проблема «внутреннего нарушителя»: мотивация, профили и методы противодействия. 4. Цифровая гигиена и осведомлённость: измеримые результаты или ритуальные действия? 5. Конфликт между продуктивностью и безопасностью: социальный компромисс. 6. Организационная культура как фактор информационной безопасности. 7. Этические дилеммы мониторинга сотрудников: границы допустимого. 8. Социальные аспекты безопасности при удалённой и гибридной работе. 9. Роль социальных сетей и цифрового следа в формировании целевого профиля для атаки. 10. Методология социально-психологического эксперимента в исследованиях ИБ: возможности и ограничения.	Кейс-метод: «Социальная инженерия в действии — разбор, анализ и защита» Ролевая игра «Взлом через людей: атакующий и защитник»



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Общие вопросы организации системы защиты информации в бизнесе	1. Система защиты информации (СЗИ) как бизнес-процесс: затраты или инвестиции? 2. Выбор модели управления ИБ: централизованная, децентрализованная или гибридная? 3. Риск-ориентированный подход: как измерить и приоритезировать угрозы в условиях ограниченного бюджета? 4. Соглашение об уровне услуг (SLA) по ИБ: реальность или фикция? 5. Проблема «избыточной безопасности»: когда защита мешает бизнесу. 6. Взаимодействие службы ИБ с другими подразделениями: партнёрство или конфликт? 7. Аутсорсинг vs инсорсинг (собственная служба): что выгоднее и безопаснее? 8. Управление непрерывностью бизнеса (BCM) и восстановление после инцидентов (DRP) как часть СЗИ. 9. Обучение и осведомлённость персонала: как превратить "человеческий фактор" в актив. 10. Измерение эффективности системы защиты информации: что, как и для кого измерять?	Деловая игра «Бюджетная комиссия: защита информации или развитие бизнеса?» Мастерская «Аудит системы защиты информации бизнеса по чек-листу»



6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Государственная политика в области информационной безопасности в системе национальной безопасности	Государственные органы обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - выполнение учебного задания
Информационные уязвимости объектов и угрозы информационной безопасности	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, классификация	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - выполнение учебного задания
Современные инновационные технологии: преимущества и социальные последствия	Негативное влияние гаджетов на мышление человека. Основные симптомы социальной зависимости от соцсетей. Базовые интернет-риски для детей.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - выполнение учебного задания
Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	Основные факторы, воздействующие на информационную безопасность как социальную систему. Социальный подход к защите информации как средство методологического анализа информационной безопасности.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - выполнение учебного задания



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы организации системы защиты информации в бизнесе	Требования законодательства по обеспечению бесперебойности функционирования систем и непрерывности бизнеса. Стандарты и лучшие практики обеспечения непрерывности бизнеса. Базовые этапы ликвидации последствий информационно- психологических операций противника. Основные направления достижения эффективной информационной защиты социальных систем и предприятий.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - выполнение учебного задания



6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

ПРИМЕРНЫЕ ТЕМЫ КОНТРОЛЬНЫХ РАБОТ

1. VPN – Виртуальные частные сети
2. Административно-правовая ответственность в информационной сфере
3. Безопасность в интернете
4. Безопасность веб-приложений
5. Государственная система защиты информации в России
6. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
7. Гражданско-правовая ответственность в информационной сфере
8. Единая биометрическая система (ЕБС) данных клиентов банков
9. Защита информационной среды бизнеса от киберпреступлений
10. Защита коммерческой тайны компании
11. Защита конфиденциальной информации от внутренних угроз
12. Защита персональных данных в России
13. Импортзамещение в сфере информационной безопасности
14. Информационная безопасность в банках
15. Информационная безопасность в социальных сетях
16. Информационная безопасность государства
17. Информационная безопасность цифровой экономики России
18. Информационное обеспечение деятельности органов государственной

власти

19. Источники угроз безопасности персональных данных
20. Как защититься от вредоносных файлов различных типов
21. Как злоумышленники воруют данные с помощью социальной инженерии
22. Как работает современный веб-фишинг
23. Как работают вредоносные веб-сайты
24. Киберпреступность в мире
25. Киберпреступность и киберконфликты
26. Классические файловые вирусы
27. Криптография
28. Меры государственного контроля в области обеспечения безопасности кибернетической информации
29. Место информационной безопасности в стратегии национальной

безопасности

Российской Федерации

30. Национальная биометрическая платформа



31. Основные каналы утечки информации в компании
 32. Основные угрозы информационной безопасности
 33. Повышение осведомлённости сотрудников компании: вклад в безопасность компании
 34. Понятие правового режима информации
 35. Понятия информации и информационных ресурсов в законодательстве
 36. Потери банков от киберпреступности
 37. Право граждан на доступ к информации
 38. Шпионские программы – новое оружие для международного кибершпионажа
 39. Правовая защита информации
 40. Правовой режим информации, составляющей государственную тайну
 41. Правовой режим коммерческой тайны
 42. Правовой режим персональных данных
 43. Предотвращения утечек информации (DLP)
 44. Преступления в информационной сфере
 45. Профессиональная и служебная тайна в РФ
 46. Сбор информации из открытых источников – как видят вас потенциальные злоумышленники?
 47. Система резервного копирования
 48. Системы аутентификации
 49. Современная защита информационной безопасности в России: проблемы и направления развития
 50. Содержание правового режима информации
 51. Стратегия национальной безопасности Российской Федерации
 52. Уголовно-правовая ответственность в информационной сфере
 53. Цензура (контроль) в интернете. Опыт Китая
 54. Что собой представляет DDoS-атака
- Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

Дополнительная информация

Примерный перечень вопросов к письменной работе

1. Какие известны подходы к классификации угроз безопасности информации?
2. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
3. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?



4. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
5. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
6. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
7. Раскройте основное содержание алгоритма электронной подписи.
8. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
9. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.
10. Назовите известные методы и средства контроля акустической информации.
11. Приведите известные методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить, используя критерий «эффективность / стоимость».



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

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-4. Способность разрабатывать и предлагать архитектурные решения для информационно-аналитических систем	Умеет выбирать архитектурные решения для разрабатываемых информационных систем.	Знать: основы архитектуры, устройства и функционирования вычислительных систем. Уметь: идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки.	В компании разворачивается новое корпоративное приложение. В процессе установки на рабочие станции пользователей возникают различные сбои. Вы являетесь ответственным за внедрение. Ваша задача: 1. Идентифицировать инциденты: проанализировать предоставленный журнал установки (лог) и классифицировать все возникшие проблемы. 2. Определить корневые причины: для каждого инцидента определить первопричину (например, конфликт версий, отсутствие прав, несовместимость оборудования). 3. Принять решение об изменении процедуры: разработать и обосновать изменения в текущей процедуре установки ПО, чтобы предотвратить повторение данных инцидентов в будущем.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	Способен выбирать современные технологии, методы и подходы к реализации архитектурных решений.	Знать: методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Уметь: формировать технические и организационные меры для защиты программной системы от несанкционированного доступа к элементам конфигурации.	Задание 1. Вам поручено спроектировать архитектуру подсистемы «Дистанционное банковское обслуживание» для крупного коммерческого банка. Система должна предоставлять клиентам доступ к счетам через веб-портал и мобильное приложение. Функциональные требования: • Аутентификация и авторизация клиентов. • Просмотр баланса и выписок по счетам. • Переводы между своими счетами и на счета других клиентов. • Оплата услуг (ЖКХ, мобильная связь, прочее). Нефункциональные требования в области ИБ (*Security Requirements*): • Конфиденциальность данных: данные о транзакциях и балансе клиента должны быть зашифрованы как при передаче, так и при хранении. Доступ к данным должен иметь только сам клиент и уполномоченные сотрудники банка. • Целостность данных: любые изменения финансовой информации должны быть защищены от несанкционированного или случайного искажения. • Доступность сервиса: платформа должна быть устойчива к DDoS-атакам и оставаться доступной для легитимных пользователей даже под нагрузкой. • Неотказуемость (non-repudiation): клиент не должен иметь возможности заявить, что он не совершал подтвержденную им операцию. • Безопасность аутентификации: необходимо реализовать многофакторную аутентификацию для подтверждения критически важных операций.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			Задание: 2. Предложить архитектурное решение для обеспечения безопасности, спроектировать высокоуровневую схему взаимодействия компонентов системы с учетом внедрения средств защиты.
	Способен проводить интеграцию архитектурных и проектных решений для информационных систем с существующими решениями.	Знать: основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации. Уметь: оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации.	Задание: Вам необходимо подготовить план мероприятий по защите ИСПДн. Для этого выполните следующие шаги: 1. Классификация системы. На основе Постановления Правительства РФ № 1119 определите уровень защищенности данной ИСПДн. Обоснуйте свой выбор, указав все факторы (категория ПДн, количество субъектов, тип актуальных угроз). 2. Определение требований. Ссылаясь на Приказ ФСТЭК России № 21 перечислите группы мер по обеспечению безопасности ПДн, которые должны быть реализованы для установленного уровня защищенности. Назовите не менее трех конкретных мер из разных групп. 3. Выбор нормативной базы. Перечислите основные федеральные законы и подзаконные акты (указы Президента, постановления Правительства, приказы регуляторов), которыми вы будете руководствоваться при выполнении этого проекта. Укажите полные названия как минимум четырех ключевых документов. 4. Практический шаг. Опишите одно конкретное техническое или организационное мероприятие, которое вы бы внедрили первым, и укажите, какой документ служит его прямым основанием. Требования к выполнению задания:



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			1. Выберите интересующую Вас тему и сформулируйте цель исследования. 2. Найдите и изучите минимум три надежных открытых источника информации по теме. 3. Представьте полученные результаты в структурированном отчете. 4. Включите список всех использованных ресурсов с активными ссылками. 5. Отчет должен содержать введение, основную часть, заключение и библиографию.
	Умеет оформлять проектную документацию в соответствии с действующими стандартами.	Знать: нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Уметь: консультировать персонал автоматизированной системы по комплексу	Задача: организация внедряет новую автоматизированную систему, обрабатывающую конфиденциальную информацию. Требуется подготовить документацию для этапа технического проектирования системы защиты информации. Необходимо: • Написать документ на создание СЗИ в строгом соответствии с ГОСТ 34.602-89. • Составить описание актуальных угроз и потенциальных нарушителей согласно методикам ФСТЭК России. • Разработать сценарии тестирования средств защиты и проверки выполнения требований ТЗ Перечислите все нормативно-правовые акты, которые следует учесть для каждого этапа работ.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		мер (правилам, процедурам, практическим приемам, руководящим принципам, методам, средствам) обеспечения защиты информации.	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике.	Знать: нормативные правовые акты, организационно-распорядительные документы и методические документы, определяющие требования к безопасности программного обеспечения. Уметь: формировать технические и организационные меры для защиты про-	Задание: выберите одну из предложенных ниже тем и проведите самостоятельный поиск необходимой информации в открытых источниках сети Интернет. Подготовьте отчет о результатах Вашего исследования, включая ссылки на использованные ресурсы. Выбор темы: выберите одну тему из списка ниже: 1. Проблемы фишинга и способы предотвращения мошенничества в электронной почте. 2. Обзор популярных антивирусных решений и их эффективность. 3. Современные методы защиты персональных данных пользователей в социальных сетях. 4. Анализ основных угроз кибератак для организаций малого бизнеса. 5. Роль шифрования данных в обеспечении конфиденциальности информации. Требования к выполнению задания: 1. Выберите интересующую Вас тему и сформулируйте цель исследования.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
коммуникационных технологий и с учетом основных требований информационной безопасности		граммной системы от несанкционированного доступа к элементам конфигурации.	2. Найдите и изучите минимум три надежных открытых источника информации по выбранной теме. 3. Представьте полученные результаты в структурированном отчете. 4. Включите список всех использованных ресурсов с активными ссылками. 5. Отчет должен содержать введение, основную часть, заключение и библиографию.
	Проводит систематический обзор источников информации, анализировать содержащиеся в них данные, делать и обосновывать выводы на основе проведенного обзора.	Знать: методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Уметь: описывать и оценивать перечень элементов архитектуры, которые должны быть защищены от угроз без-	Задание: составьте доклад по теме "Методики определения актуальных угроз безопасности персональных данных". Порядок выполнения задания: 1. Подбор источников: используя электронные библиотеки и базы данных (например, eLibrary, SpringerLink, Google Scholar), найдите публикации по ключевым словам («информационная безопасность», «защита данных», «киберугрозы», «шифрование»), отберите минимум пять значимых источников информации (монографии, научные статьи, обзоры). 2. Чтение и анализ: ознакомьтесь с каждым источником подробно, выявляя ключевые идеи, методологию исследования, результаты и рекомендации авторов, запишите наиболее важные моменты каждого источника, составьте таблицу сравнения подходов и выводов ученых. 3. Описание наиболее популярных методик определения актуальных угроз безопасности персональных данных (не более 2-х).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		опасности информации, связанных с нарушением конфиденциальности, целостности и доступности.	
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	Знать: методы управления требованиями по созданию комплексных систем информационной безопасности. Уметь: проверять требования с точки зрения их соответствия архитектуре системы информационной безопасности.	Тема: верификация и валидация. Задание: когда система будет готова, как Вы проверите, что требование "Данные должны быть зашифрованы при хранении" выполнено корректно? Чем отличается проверка выполнения технического задания (верификация) от подтверждения того, что это защищает данные так, как хотел заказчик (валидация)? Какие существуют методы управления требованиями по созданию комплексных систем информационной безопасности? Требования к выполнению задания: 1. Найдите и изучите минимум три надежных открытых источника информации по выбранной теме. 2. Представьте полученные результаты в структурированном отчете. 3. Включите список всех использованных ресурсов с активными ссылками. 4. Отчет должен содержать введение, основную часть, заключение и библиографию.



Примеры практико-ориентированных заданий

1. Создание политики безопасности для коммерческой организации.
2. Разработка показателей оценки эффективности функционирования комплексной системы защиты информации.
3. Расчет показателей надежности, доступности, сопровождаемости автоматизированной системы.
4. Оценка информационных рисков автоматизированной системы.
5. Применение методики проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.
6. Что такое триада CIA в информационной безопасности? Раскройте каждую аббревиатуру.
7. В чем разница между уязвимостью, угрозой и риском?
8. Объясните принцип наименьших привилегий (Principle of Least Privilege).
9. Что такое "поверхность атаки" (Attack Surface)?
10. Дайте определение социальной инженерии и приведите пример (не фишинг).
11. Назовите три основных фактора аутентификации с примерами для каждого.
12. Почему использование одного только пароля считается слабой защитой?
13. Как работает многофакторная аутентификация (MFA) и почему она эффективнее двухфакторной (2FA)?
14. Что такое атака методом перебора (Brute-force) и как от нее защититься?
15. В чем разница между идентификацией, аутентификацией и авторизацией?
16. Чем компьютерный вирус отличается от компьютерного червя?
17. Что делает программа-вымогатель (Ransomware) и какой главный способ защиты от нее?
18. Опишите атаку типа «Человек посередине» (Man-in-the-Middle).
19. Что такое DDoS-атака и какова ее основная цель?
20. Что такое SQL-инъекция и на что она направлена?
21. Для чего нужен межсетевой экран (Firewall) и на каких уровнях модели OSI он может работать?
22. В чем разница между шифрованием данных «в покое» (at rest) и «при передаче» (in transit)?
23. Зачем нужно устанавливать обновления безопасности (патчи) для операционной системы и приложений?
24. Что такое VPN и какую основную задачу безопасности он решает при использовании публичного Wi-Fi?

Примеры вопросов для подготовки к промежуточной аттестации



1. Защита информации от утечки по техническим каналам.
2. Угрозы конфиденциальности, целостности и доступности информации.
3. Информационная война как высшая форма угрозы информационной безопасности.
4. Методики обеспечения непрерывности бизнеса
5. Методы и средства обеспечения бесперебойности функционирования систем.
6. Модели компьютерной безопасности.
7. Криптографическая защита информации.
8. Угрозы несанкционированного доступа в компьютерную систему.
9. Вредоносное ПО: Охарактеризуйте основные типы (вирусы, черви, трояны, руткиты, программы-вымогатели).
10. Сетевые атаки: Принципы реализации DoS и DDoS атак, спуфинга, фишинга, атак типа «человек посередине» (MITM).
11. Социальная инженерия: Что это такое, основные методы (фишинг, вишинг, претекстинг) и способы защиты от них.
12. Управление доступом: Модели разграничения доступа (дискреционная, мандатная, ролевая — RBAC).
13. Криптография: Симметричные и асимметричные алгоритмы шифрования. Что такое хэш-функции и электронная цифровая подпись (ЭЦП)?
14. Инфраструктура безопасности: Принципы работы межсетевых экранов (Firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS), VPN-сетей и антивирусных комплексов.
15. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».
16. Персональные данные: Базовые требования к обеспечению безопасности ПДн в соответствии с № 152-ФЗ.
17. Международный стандарт ISO/IEC 27001, его структура и назначение.
18. Триада ЦРУ (CIA triad): Дайте определение конфиденциальности, целостности и доступности. Какие еще свойства выделяют в расширенных моделях (например, подлинность и неотказуемость)?
19. Активы и угрозы: Что такое информационный актив? Классификация основных угроз (естественные, антропогенные, случайные и преднамеренные).
20. Кто является субъектом, а кто — объектом доступа в системах защиты информации?



21. Менеджмент и аудит ИБ на уровне предприятия.
22. Аудит ИБ автоматизированных банковских систем.
23. Аудит ИБ электронной коммерции.
24. Информационная безопасность предпринимательской деятельности.
25. Организационно-экономическое обеспечение ИБ.
26. Инженерно-техническое обеспечение компьютерной безопасности.
27. Почему использование одного только пароля считается слабой защитой?
28. Как работает многофакторная аутентификация (MFA) и почему она эффективнее двухфакторной (2FA)?
29. Что такое атака методом перебора (Brute-force) и как от нее защититься?
30. В чем разница между идентификацией, аутентификацией и авторизацией?
31. Чем компьютерный вирус отличается от компьютерного червя?
32. Что делает программа-вымогатель (Ransomware) и какой главный способ защиты от нее?
33. Опишите атаку типа «Человек посередине» (Man-in-the-Middle).
34. Что такое DDoS-атака и какова ее основная цель?

ПРИМЕР ЭКЗАМЕНАЦИОННОГО БИЛЕТА

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Информационное обеспечение деятельности органов государственной власти (15 баллов)
2. Защита конфиденциальной информации от внутренних угроз (20 баллов)
3. Определите основные задачи аттестации защищённых информационных систем по требованиям безопасности и предложите план мероприятий проведения. (25 баллов)



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

Основная литература:

1. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. 2-е изд., стер. Санкт-Петербург : Лань, 2022 324 с. Книга из коллекции Лань - Информатика <https://e.lanbook.com/book/195510> ISBN 978-5-8114-9489-7. [БИК ID: RU-LAN-BOOK-195510]
2. Игнатьева, Е. П. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Игнатьева Е. П. Иркутск : ИРНИТУ, 2023 96 с. Книга из коллекции ИРНИТУ - Информатика <https://e.lanbook.com/book/497837> ISBN 978-5-8038-1976-2. [БИК ID: RU-LAN-BOOK-497837]

Дополнительная литература:

1. Основы информационной безопасности: Практикум / Паршенкова Ю. А. Ч. 1 : Основы информационной безопасности: Практикум. Часть 1 . Ч. 1 / Паршенкова Ю. А. Москва : РТУ МИРЭА, 2025 74 с. Книга из коллекции РТУ МИРЭА - Информатика <https://e.lanbook.com/book/493478> ISBN 978-5-7339-2448-9. [БИК ID: RU-LAN-BOOK-493478]
2. Основы информационной безопасности: Практикум / Паршенкова Ю. А. Ч. 2 : Основы информационной безопасности: Практикум. Часть 2 . Ч. 2 / Паршенкова Ю. А. Москва : РТУ МИРЭА, 2025 68 с. Книга из коллекции РТУ МИРЭА - Информатика <https://e.lanbook.com/book/493481> ISBN 978-5-7339-2449-6. [БИК ID: RU-LAN-BOOK-493481]

Нормативные правовые акты:

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798
2. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_112701
3. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808>
4. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_48699
5. Распоряжение Правительства России от 28.07.2017 г. № 1632-р «Об



утверждении Программы «Цифровая экономика Российской Федерации». – режим

доступа: https://www.consultant.ru/document/cons_doc_LAW_221756

6. Международный стандарт. ISO/IEC 27000:2012 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы. – режим доступа: <https://docs.cntd.ru/document/1200102762>

7. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). – режим доступа:

<https://opk.spb.ru/iso-ies-27001-2005>

8. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808>

9. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_48699

10. Распоряжение Правительства России от 28.07.2017 г. № 1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_221756/

11. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – режим доступа:

<https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>

12. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных

данных». – режим доступа: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>

13. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – режим доступа: <https://npropris.ru/wp-content/uploads/2015/09/%D0%93%D0%9E%D0%A1%D0%A2-34.003-90.pdf>

14. ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. – режим доступа: <https://meganorm.ru/Data/106/10698.pdf>

15. ГОСТ Р 50922 Защита информации. Основные термины и определения. – режим доступа: <https://docs.cntd.ru/document/1200058320>



16. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – режим доступа: <https://docs.cntd.ru/document/1200075565>
17. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения. – режим доступа: <https://docs.cntd.ru/document/1200108858>
18. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. – режим доступа: <https://docs.cntd.ru/document/1200146707>
19. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – режим доступа: <https://docs.cntd.ru/document/1200101777>
20. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – режим доступа: <https://docs.cntd.ru/document/1200105710>
21. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – режим доступа: <https://docs.cntd.ru/document/1200105711>
22. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – режим доступа: <https://opk.spb.ru/iso-ies-27001-2005>
23. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – режим доступа: <https://docs.cntd.ru/document/1200103619>
24. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – режим доступа: <https://docs.cntd.ru/document/1200084141>
25. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – режим доступа: <https://docs.cntd.ru/document/1200076806>



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

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
(<http://library.fa.ru/files/elibfa.pdf>)
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
4. Электронно-библиотечная система Znanium <http://www.znanium.com>
5. Электронно-библиотечная система издательства "Лань" <https://e.lanbook.com/>
6. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>
7. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
8. Информационно-образовательный портал Финуниверситета: <https://org.fa.ru>



10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 01.10.2024 № 2187/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по образовательным программам высшего образования в Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.



11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

Комплект лицензионного программного обеспечения:

1. Astra Linux
2. Пакет офисных программ
3. Windows

Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»

Сертифицированные программные и аппаратные средства защиты информации

1. не предусмотрены

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

1. Учебная аудитория для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)
2. Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.
3. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)