

**Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)**

Владикавказский филиал Финуниверситета

Кафедра «Математика и информатика»

УТВЕРЖДАЮ
Директор филиала
Т.А. Хубаев
«28» апреля 2026 г.



А.М. Кумаритов

Основы информационной безопасности

для студентов, обучающихся по направлению подготовки
09.03.04 Программная инженерия,
ОП «Технологии разработки программного обеспечения»

*Рекомендовано Ученым советом Владикавказского филиала
Финансового университета
(протокол от «15» апреля 2026 г. № 30)*

*Одобрено на заседании кафедры «Математика и информатика»
(протокол от «10» апреля 2026 г. № 8)*

Владикавказ 2026

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.....	4
4.	Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся.....	4
5.	Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий.....	4
5.1.	Содержание дисциплины.....	4
5.2.	Учебно-тематический план.....	7
5.3.	Содержание семинаров.....	8
6.	Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	9
6.1.	Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	9
6.2.	Перечень вопросов, заданий, тем для подготовки к текущему контролю.....	10
7.	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	15
8.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	21
9.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	23
10.	Методические указания для обучающихся по освоению дисциплины.....	24
11.	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем.....	30
11.1.	Комплект лицензионного программного обеспечения.....	30
11.2.	Современные профессиональные базы данных и информационные справочные системы	30
11.3.	Сертифицированные программные и аппаратные средства защиты информации.....	30
12.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	30

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
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 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

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» является дисциплиной общефакультетского (предпрофильного) цикла» обязательной части учебного плана образовательной программы «Технологии разработки программного обеспечения» по направлению подготовки 09.03.04 Программная инженерия, профиль «Технологии разработки программного обеспечения».

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

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 3 (в часах)
Общая трудоёмкость дисциплины	4/144	144
Контактная работа- Аудиторные занятия	50	50
Лекции	16	16
Семинары, практические занятия	34	34
Самостоятельная работа	94	94
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, источники

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 этнос и 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

№ п/п	Наименование тем (разделов) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа - Аудиторная работа			Самост оя тельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практическ ие занятия		
1	Государственна я политика в области информационно й безопасности в системе национальной безопасности	27	8	2	6	19	Опрос, собеседование по домашним заданиям самостоятельной работы, решение практико- ориентированных задач.
2	Информационн ые уязвимости объектов и угрозы информационно й безопасности, источники	29	10	4	6	19	Опрос, собеседование по домашним заданиям самостоятельной работы, решение практико- ориентированных задач.
3	Современные инновационные технологии: преимущества и социальные последствия	31	12	4	8	19	Опрос, собеседование по домашним заданиям самостоятельной работы, решение практико- ориентированных задач.
4	Социальный аспект исследования проблем защиты информации с учётом угроз информационно й безопасности	31	12	4	8	19	Опрос, собеседование по домашним заданиям самостоятельной работы, решение практико- ориентированных задач.
5	Общие вопросы организации системы защиты	26	8	2	6	18	Опрос, собеседование по домашним

	информации в бизнесе						заданиям самостоятельной работы, решение практико-ориентированных задач.
В целом по дисциплине		144	50	16	34	94	Согласно учебному плану: контрольная работа
Итого в %			35	32	68	65	

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.	Интерактивная форма: опрос, собеседование по домашним заданиям самостоятельной работы, решение практико-ориентированных задач с последующим коллективным обсуждением их результатов
Информационные уязвимости объектов и угрозы информационной безопасности, источники	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз.	Интерактивная форма: опрос, собеседование по домашним заданиям самостоятельной работы, решение практико-ориентированных задач с последующим коллективным обсуждением их результатов
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 типы интернет-зависимости. Программно-аппаратные средства обеспечения информационной безопасности.	Интерактивная форма: опрос, собеседование по домашним заданиям самостоятельной работы, решение практико-ориентированных задач с последующим коллективным обсуждением их результатов

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.	Интерактивная форма: опрос, собеседование по домашним заданиям самостоятельной работы, решение практико-ориентированных задач с последующим коллективным обсуждением их результатов
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. Способы срыва информационно-психологического воздействия противника на социальные системы бизнеса. Индикаторы манипулятивного информационного воздействия на служащих.	Интерактивная форма: опрос, собеседование по домашним заданиям самостоятельной работы, решение практико-ориентированных задач с последующим коллективным обсуждением их результатов, защита контрольной работы

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	Изучение материалов лекций и литературы, предложенной преподавателем, поиск и анализ информации, содержащейся в Интернет-ресурсах.
Информационные уязвимости объектов и угрозы информационной безопасности, источники	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, классификация	Изучение материалов лекций и литературы, предложенной преподавателем, поиск и анализ информации, содержащейся в Интернет-ресурсах.

Современные инновационные технологии: преимущества и социальные последствия	Негативное влияние гаджетов на мышление человека. Основные симптомы социальной зависимости от соцсетей. Базовые интернет-риски для детей.	Изучение материалов лекций и литературы, предложенной преподавателем, поиск и анализ информации, содержащейся в Интернет-ресурсах.
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	Изучение материалов лекций и литературы, предложенной преподавателем, поиск и анализ информации, содержащейся в Интернет-ресурсах.
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.	Изучение материалов лекций и литературы, предложенной преподавателем, поиск и анализ информации, содержащейся в Интернет-ресурсах. Разбор вопросов, отводимых на самостоятельное освоение, выполнение домашних заданий самостоятельной работы. Выполнение контрольной работы.

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

Примерный перечень тем для подготовки к опросу, подготовки докладов, презентаций

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, источники

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 этнос и 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.

Примеры практико-ориентированных задач

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.

Примерные темы контрольной работы

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. Импортозамещение 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 «Математика и информатика».

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

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

Примерные вопросы для подготовки к экзамену

1. Защита информации от утечки по техническим каналам.
2. Защита конфиденциальной информации от внутренних угроз
3. Угрозы конфиденциальности, целостности и доступности информации.
4. Информационная война как высшая форма угрозы информационной безопасности.
5. Информационное обеспечение деятельности органов государственной власти

6. Методики обеспечения непрерывности бизнеса
7. Методы и средства обеспечения бесперебойности функционирования систем.
8. Модели компьютерной безопасности.
9. Криптографическая защита информации.
10. Угрозы несанкционированного доступа в компьютерную систему.

Пример экзаменационного билета

**Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)**

Кафедра: **Математика и информатика**

Дисциплина: **Основы информационной безопасности**

Филиал: **Владикавказский**; Форма обучения: **Очная**

Семестр: **3** Направление: **09.03.04 Программная инженерия**

Профиль: **Технологии разработки программного обеспечения**

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)

Подготовил: _____

На основе перечня теоретических вопросов и практико-ориентированных заданий, утвержденного на заседании кафедры «Математика и информатика» протокол № ____ от _____.2026 г.

Утверждаю:

Заведующий кафедрой _____

Дата __.__.2026г.

**Примеры оценочных средств для проверки индикаторов достижения
компетенций, формируемых дисциплиной**

Код и наименование компетенции	Наименование индикатора достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
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	1. Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике. Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	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	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.

			<p>Требования к выполнению задания:</p> <ol style="list-style-type: none"> 1. Выберите интересующую Вас тему и сформулируйте цель исследования. 2. Найдите и изучите минимум три надежных открытых источника информации по вашей теме. 3. Представьте полученные результаты в структурированном отчете. 4. Включите список всех использованных вами ресурсов с активными ссылками. 5. Отчет должен содержать введение, основную часть, заключение и библиографию.
	<p>2. Проводит систематический обзор источников информации, анализировать содержащиеся в них данные, делать и обосновывать выводы на основе проведенного обзора. Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции</p>	<p>Знать: Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных</p> <p>Уметь: Описывать и оценивать перечень элементов архитектуры, которые должны быть защищены от угроз безопасности информации, связанных с нарушением конфиденциальности, целостности и доступности</p>	<p>Выполните систематический обзор актуальных научных статей, монографий, периодических изданий и иных источников, посвящённых вопросам информационной безопасности. Проанализируйте содержащуюся в них информацию, сделайте выводы и приведите обоснованное резюме на основе проведенных обзоров. Требования к проведению обзора: 1. Определите круг ключевых вопросов и проблем, рассматриваемых в литературе по информационной безопасности. 2. Оцените качество представленных в источниках эмпирических данных и выводов авторов. 3. Сравните различные точки зрения исследователей и выделите общие тенденции и</p>

		<p>разногласия. 4. Сделайте собственные выводы относительно перспектив развития информационной безопасности на основании проведенного анализа литературы.</p> <p>Порядок выполнения задания:</p> <p>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).</p> <p>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.</p> <p>Написание итогового обзора:</p> <p>- Начните с введения, в котором обозначьте актуальность проблемы информационной безопасности и значимость её изучения. - Во второй части обзора дайте характеристику каждому источнику отдельно, подчеркивая особенности каждой публикации. - Затем обобщите общее содержание источников, сравните взгляды учёных друг с другом. - Заключение должно включать</p>
--	--	---

			ваши личные выводы и перспективы дальнейших исследований в области информационной безопасности.
	3. Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов. Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	<p>Знать: Методы управления требованиями по созданию комплексных систем информационной безопасности</p> <p>Уметь: Проверять требования с точки зрения их соответствия архитектуре системы информационной безопасности</p>	<p>Представьте себя специалистом по информационной безопасности. Вам поручено провести аудит информационной безопасности небольшой компании. Разработайте краткий перечень мероприятий, необходимых для повышения уровня защищенности информационных активов компании.</p> <p>Пример плана действий:</p> <ol style="list-style-type: none"> 1. Определение уязвимых мест в существующей инфраструктуре (сетевые устройства, серверы, рабочие станции). 2. Реализация мониторинга сетевого трафика и поведения пользователей. 3. Регулярное обновление программного обеспечения и установка патчей безопасности. 4. Организация регулярного резервного копирования важных данных. 5. Повышение осведомленности сотрудников путём тренингов и инструктажей по основам информационной безопасности.

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

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. Международный стандарт. ISO/IEC 27000:2012 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы. – режим доступа: <https://docs.cntd.ru/document/1200102762>;
6. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_48699/;
7. 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/;
8. 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-fevralya2013-g-n-17> (дата обращения 01.09.2025 г.)
9. 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/vsedokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения 01.09.2025 г.)

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

Основная литература:

1. Козьминых, С. И. Управление информационной безопасностью: учебное пособие / С. И. Козьминых, С. А. Борисов. — Москва: КноРус, 2026. — 281 с. — ISBN 978-5-406-14915-7. — URL: <https://book.ru/book/959440> — Режим доступа: Электронно-библиотечная система Book.ru. — Текст: электронный.

2. Крылов, Г. О. Базовые понятия информационной безопасности: учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва: Русайнс, 2025. — 257 с. — ISBN 978-5-466-09255-4. — URL: <https://book.ru/book/958467> — Режим доступа: Электронно-библиотечная система Book.ru. — Текст: электронный.

Дополнительная литература:

3. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - 2-е изд. - Москва: Гор. линия-Телеком, 2016. - 170 с. - ISBN 978-5-9912-0363-0. - URL: <https://znanium.ru/catalog/product/560782> — Режим доступа: Электронно-библиотечная система Znanium.com — Текст: электронный.

4. Мельников, В. П., Информационная безопасность: учебник / В. П. Мельников, А. И. Куприянов; под ред. В. П. Мельникова. — Москва: КноРус, 2025. — 267 с. — ISBN 978-5-406-13756-7. — URL: <https://book.ru/book/955528> — Режим доступа: Электронно-библиотечная система Book.ru. — Текст: электронный.

5. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-

16388-9. — URL: <https://urait.ru/bcode/588741> — Режим доступа: Электронно-библиотечная система Юрайт. — Текст: электронный.

6. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва: ИНФРА-М, 2022. — 327 с. — ISBN 978-5-16-015471-8. - URL: <https://znanium.ru/catalog/product/1865598> — Режим доступа: Электронно-библиотечная система Znanium.com — Текст: электронный.

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

1. www.cbr.ru - Официальный сайт Банка России
2. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
(<http://library.fa.ru/files/elibfa.pdf>)
3. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
4. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
5. Официальный сайт Минобороны РФ <https://stat.mil.ru/>
6. "Деловая онлайн библиотека" издательства "Альпина Паблишер" <http://lib.alpinadigital.ru/en/library>
7. Электронно-библиотечная система издательства "Лань" <https://e.lanbook.com/>
8. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
9. Информационно-образовательный портал Финуниверситета: <https://org.fa.ru>
10. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>

10. Методические указания для обучающихся по освоению дисциплины

Методика освоения дисциплины предусматривает подготовку обучающихся к лекциям, семинарам и практическим занятиям, выполнение студентами самостоятельной внеаудиторной работы, в том числе – контрольной работы.

Рекомендации по подготовке к лекционным занятиям.

Для наиболее полного освоения дисциплины студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, ее основные вопросы и рекомендуемую литературу. Это позволит сэкономить время на записывание основных вопросов темы;
- перед очередной лекцией просматривать материалы предыдущих, чтобы освоение материала не оставляло пробелов.

Рекомендации по подготовке к семинарам, практическим занятиям.

Студентам следует:

- проработать теоретический материал к занятию по рекомендованным литературным источникам и лекциям;
- использовать при подготовке к занятию нормативно-правовые документы, научные публикации, информационный материал, рекомендуемый преподавателем;
- перед занятиями задать вопросы по невыясненным в ходе самостоятельной подготовки темам или отдельным положениям темы;
- в ходе занятия давать четкие и исчерпывающие ответы на вопросы;
- на занятии демонстрировать понимание обсуждаемых тем и вопросов.

Студентам, пропустившим занятия по различным причинам, необходимо перед очередным занятием отработать пропущенный материал, подготовив его самостоятельно.

Методические рекомендации по выполнению различных форм самостоятельной работы

Студентам при организации самостоятельной работы следует руководствоваться Приказом Финансового университета № 1040/о от 11.05.2021г. «Об утверждении методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете».

Самостоятельная работа содержит в себе различные виды и формы работ. Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

В ходе изучения дисциплины предусмотрены следующие формы самостоятельной работы:

- подготовка к опросу;
- выполнение заданий самостоятельной работы,
- решение практико-ориентированных задач;
- выполнение контрольной работы;
- подготовка к экзамену.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны выполняться самостоятельно и представляться в установленный срок, а также должны соответствовать установленным требованиям по оформлению.

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным РПД;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, разбирать на занятиях и консультациях неясные вопросы;
- прорабатывать соответствующие теоретические и практические разделы

дисциплины, фиксируя неясные фрагменты для их обсуждения на консультации.

Методические рекомендации для обучающихся по выполнению контрольной работы

Контрольная работа является обязательной формой внеаудиторной самостоятельной работы студентов по дисциплине и может реализовываться как в письменном виде, так и с использованием информационных технологий и специализированных программных продуктов.

Цель выполнения контрольной работы, содержащей комплект заданий – овладение студентами навыками решения типовых расчетных задач, формирование учебно-исследовательских навыков, закрепление умений самостоятельно работать с различными источниками информации; проверка сформированности компетенций.

Целью выполнения контрольной работы является углубление и закрепление теоретических знаний и практических навыков студентов по дисциплине.

Контрольная работа по дисциплине выполняется по вариантам.

Содержание заданий контрольных работ охватывают основной материал соответствующих разделов (тем) дисциплин. Контрольные задания разрабатываются по многовариантной системе. Варианты контрольных работ равноценны по объему и сложности.

Контрольная работа выполняется студентом под руководством преподавателя кафедры «Математика и информатика», ведущим семинарские (практические) занятия.

Контрольная работа состоит из нескольких частей. Состав контрольной работы и очередность размещения отдельных частей:

- титульный лист;
- основная часть;
- список использованных источников;
- приложения (при наличии).

Титульный лист является первой страницей и заполняется по определенным правилам.

Основная часть выполняется согласно заданиям (вопросам) контрольных работ.

В список использованных источников включаются названия законодательных актов, нормативных документов, книг, статей, учебных пособий и т. п., которые, так или иначе, использовались студентом при выполнении работы.

В Приложения выносятся вспомогательные материалы, которые не содержат основную информацию, либо материалы, которые сложно разместить по тексту работы (большие схемы, таблицы, графические материалы, расчетные справочные данные, образцы первичных документов и т.п.). Непременным условием включения данных материалов в приложение является ссылка на них в тексте работы.

Требования к выполнению контрольной работы:

- четкость и последовательность изложения материала (решения) в соответствии с составленным планом;
- наличие обобщений и выводов, сделанных на основе изучения информационных источников по данной теме;
- предоставление в полном объеме решений имеющихся в задании практических задач;
- использование современных способов поиска, обработки и анализа информации;
- самостоятельность выполнения.

Требования к оформлению контрольной работы.

Контрольная работа выполняется на компьютере (гарнитура Times New Roman, шрифт 13 или 14) через 1-1,5 интервала с полями: верхнее, нижнее - 2; правое - 3; левое - 1,5. Отступ первой строки абзаца - 1,25. Нумерация страниц – внизу в центре.

Иллюстративный материал (схемы, диаграммы, рисунки, таблицы и др.) встраивается в текст работы или выносится в Приложения.

При написании допускаются только общепринятые сокращения (например, тыс. руб.).

В тексте обязательны ссылки на литературные источники, лучше всего постраничные.

Объем контрольной работы составляет не более 6 страниц, не включая таблиц, графиков и т.п. (при наличии).

Законченная контрольная работа, содержащая все требуемые элементы оформления, вставленная в папку (или файл) и скрепленная по левому краю, сдается на кафедру или непосредственно руководителю контрольной работы – преподавателю; ведущему семинарские (практические) занятия по дисциплине. Он осуществляет проверку контрольной работы, а также оказывает помощь при подготовке к ее защите.

Контрольная работа защищается в назначенные сроки. Защита работы проводится до начала сессии (в крайнем случае, до начала экзамена по соответствующему предмету). При защите студент кратко излагает основные положения работы, последовательность ее выполнения, свои предложения.

При защите работы студент должен свободно ориентироваться в изложенном материале работы; ответить на все замечания преподавателя; уметь отвечать на вопросы преподавателя по выполненной работе.

Оценка контрольных работ студентов проводится в процессе текущего контроля успеваемости студентов.

Критерии оценки контрольной работы

Оценка «отлично» (5-6 баллов) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания вопросов контрольной работы /и/или умение уверенно применять их на практике при решении конкретных задач.

Оценка «хорошо» (3-4 балла) выставляется студенту, если он твердо знает материал контрольной работы, грамотно и по существу излагает его /и/или умеет применять полученные знания на практике при решении конкретных задач, но допускает некоторые неточности.

Оценка «удовлетворительно» (например, 2 балла) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, обнаружившему нарушения логической последовательности в изложении материала, но при этом владеющему основными вопросами, выносимыми на контрольную работу и необходимыми для дальнейшего обучения /и/или умеющему применять полученные знания по образцу в стандартной ситуации.

Оценки «неудовлетворительно» (0 баллов) заслуживает студент, который не знает большей части основного содержания выносимых на контрольную работу вопросов, тем дисциплины, допускает грубые ошибки в формулировках основных понятий /и/или не умеет использовать полученные знания при решении типовых практических задач.

При оценивании контрольной работы на «неудовлетворительно» она должна быть переделана (исправлена) в соответствии с полученными замечаниями, сдана на проверку заново и защищена не позднее срока окончания ее приёма и защиты.

Оценка результатов текущего контроля успеваемости и промежуточной аттестации обучающихся осуществляется в соответствии с Балльно-рейтинговой системой Финансового университета (Приказ Финансового университета № 2187/о от 01.10.2024 г. «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по образовательным программам высшего образования в Финансовом университете»).

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

11.1. Комплект лицензионного программного обеспечения:

- 1) Антивирусная защита Kaspersky Security для виртуальных и облачных сред;
- 2) Windows, Microsoft Office или Astra Linux, Libre Office.

11.2. Современные профессиональные базы данных и информационные справочные системы:

1. Информационно-правовая система «Консультант Плюс»
2. Информационно-правовая система «Гарант»: <https://www.garant.ru>
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не используются

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

Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения

Аудитория № 36

Специализированная мебель:

Стол (учительский) – 1 шт.

Стол компьютерный – 1 шт.

Стол (студенческий) двухместный – 13 шт.

Стулья – 27 шт.

Доска меловая – 1 шт.

Технические средства обучения:

Компьютер в сборе – 1 шт.

Экран настенный – 1 шт.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду Финансового университета

Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения

Аудитория № 32

Специализированная мебель:

Стол компьютерный – 20 шт.

Стол (двухместный) – 7 шт.

Стул – 34 шт.

Шкаф – 1 шт.

Технические средства обучения:

Компьютер в сборе – 20 шт.

Мультимедиа-проектор – 1 шт.

Экран настенный – 1 шт.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду Финансового университета

Помещение для самостоятельной работы обучающихся:

Кабинет № 55. Читальный зал:

Специализированная мебель:

Стол – 20 шт.

Стул – 40 шт.

Шкаф для книг – 4 шт.

Стеллаж книжный – 13 шт.

Стеллаж выставочный – 4 шт.

Технические средства обучения:

Компьютер в сборе – 6 шт.

Телевизор – 1 шт.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Финансового университета