

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 РФ
Утверждено: Проректор по учебной и методической работе Е.А. Каменева
Сертификат: vab3hWX8lZTEJWpnCVq1RpUrf8nMhkNq
Дата: 03.12.2025 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 «Инженер-разработчик программного обеспечения»

Профиль:

«Инженер-разработчик программного обеспечения»

Рекомендовано

*Факультет информационных технологий и анализа больших данных
(протокол № 1 от 21.10.2025 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	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	5
5.1.	Содержание дисциплины	5
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	11
7.	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	15
8.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	20
9.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	24
10.	Методические указания для обучающихся по освоению дисциплины	25
11.	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	25
12.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	26

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» относится к «Общефакультетскому (предпрофильному) циклу».

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

Очно-заочная форма обучения

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	20	20
Лекции	4	4
Семинары, практические занятия	16	16
Самостоятельная работа	124	124
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				
		Всего	Контактная работа - Аудиторная работа			Самостоя тельная работа
			Общая, в т.ч.:	Лекции	Семинары, практическ ие занятия	
1	Государственная политика в области информационной безопасности в системе национальной безопасности	24	2	0	2	22
2	Информационные уязвимости объектов и угрозы информационной безопасности, источники	28	2	0	2	26
3	Современные инновационные технологии: преимущества и социальные последствия	30	6	2	4	24
4	Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	30	6	2	4	24
5	Общие вопросы организации системы защиты информации в бизнесе	32	4	0	4	28
	Итого	144	20	4	16	124

5.3. Содержание семинаров

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.	групповые дискуссии
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.	групповые дискуссии
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.	групповые дискуссии
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.	групповые дискуссии
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.	групповые дискуссии

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, источники	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
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	- работа с учебной, научной и справочной литературой;- конспект;- подготовка сообщений по теме;- выполнение учебного задания

	социальных систем и предприятий.	
--	----------------------------------	--

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

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

Типовые контрольные задания

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.
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.

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

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

Типовые контрольные задания

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 разногласия. 4. Сделайте собственные выводы относительно перспектив развития информационной безопасности на основании проведенного анализа литературы.

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. Написание итогового обзора: - 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 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

Знать: Методы управления требованиями по созданию комплексных систем информационной безопасности

Уметь: Проверять требования с точки зрения их соответствия архитектуре системы информационной безопасности

Типовые контрольные задания

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.

Пример плана действий:

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.

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.

Примерные вопросы для подготовки к экзамену

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.

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

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 (дата обращения 01.09.2025 г.)
2. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_112701 (дата обращения 01.09.2025 г.)
3. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808> (дата обращения 01.09.2025 г.)
4. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_48699 (дата обращения 01.09.2025 г.)
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 (дата обращения 01.09.2025 г.)
6. Международный стандарт. ISO/IEC 27000:2012 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы. – режим доступа: <https://docs.cntd.ru/document/1200102762> (дата обращения 01.09.2025 г.)
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/> (дата обращения 01.09.2025 г.)
8. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808> (дата обращения 01.09.2025 г.)

9. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – режим доступа: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения 01.09.2025 г.)

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/ (дата обращения 01.09.2025 г.)

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> (дата обращения 01.09.2025 г.)

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> (дата обращения 01.09.2025 г.)

13. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – режим доступа: <https://npopris.ru/wp-content/uploads/2015/09/%D0%93%D0%9E%D0%A1%D0%A2-34.003-90.pdf> (дата обращения 01.09.2025 г.)

14. ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. – режим доступа: <https://meganorm.ru/Data/106/10698.pdf> (дата обращения 01.09.2025 г.)

15. ГОСТ Р 50922 Защита информации. Основные термины и определения. – режим доступа: <https://docs.cntd.ru/document/1200058320> (дата обращения 01.09.2025 г.)

16. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – режим доступа: <https://docs.cntd.ru/document/1200075565> (дата обращения 01.09.2025 г.)

17. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения. – режим доступа: <https://docs.cntd.ru/document/1200108858> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)
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/> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)
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> (дата обращения 01.09.2025 г.)

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> (дата обращения 01.09.2025 г.)

Основная литература:

1. Козьминых, С.И. Управление информационной безопасностью : Учебное пособие / С.И. Козьминых, С.А. Борисов Электрон. дан. Москва : КноРус, 2026 281 с. Режим доступа: book.ru Internet access <https://book.ru/book/959440> ISBN 978-5-406-14915-7. [БИК ID: RU\bookru\bibl\959440]
2. Кибербезопасность в условиях электронного банкинга : практическое пособие / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская, В. А. Конявский, И. Г. Назаров ; под ред. П. В. Ревенков Москва : Прометей, 2020 522 с. : ил. Библиогр. в кн Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация <https://biblioclub.ru/index.php?page=book&id=610688> ISBN 978-5-907244-61-0. [БИК ID: 28]
3. Крылов, Г.О. Базовые понятия информационной безопасности : Учебное пособие / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина Электрон. дан. Москва : Русайнс, 2025 257 с. Режим доступа: book.ru Internet access <https://book.ru/book/958467> ISBN 978-5-466-09255-4. [БИК ID: RU\bookru\bibl\958467]

Дополнительная литература:

1. Баранова, Елена Константиновна Актуальные вопросы защиты информации : Монография / Национальный исследовательский университет "Высшая школа экономики" 2 Москва : Издательский Центр РИОР, 2025 216 с. (Научная мысль)
Дополнительное профессиональное образование
<https://znanium.ru/catalog/document?id=459567> ISBN 978-5-369-01972-6 ISBN 978-5-16-113215-9 (электр. издание) ISBN 978-5-16-020563-2 (ISBN соиздателя) . [БИК ID: RU\infra-m\znanium\bibl\2169152]
2. Чистов, Дмитрий Владимирович Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. 2-е изд., пер. и доп Электрон. дан. Москва : Юрайт, 2025 273 с (Высшее образование) URL: <https://urait.ru/bcode/560485> (дата обращения: 01.09.2025). Режим доступа: Электронно-библиотечная система Юрайт, для

авториз. пользователей <https://urait.ru/bcode/560485> ISBN 978-5-534-20361-5 : 1399.00. [БИК ID: RU2fURAIT2f560485]

3. Хорев, Павел Борисович Программно-аппаратная защита информации : Учебное пособие / Московский энергетический институт 3, испр. и доп. Москва : ООО "Научно-издательский центр ИНФРА-М", 2022 327 с. (Высшее образование: Магистратура) ВО - Бакалавриат <https://znanium.com/catalog/document?id=397282> ISBN 978-5-16-015471-8 ISBN 978-5-16-107928-7 (электр. издание) . [БИК ID: RU\infra-m\znanium\bibl\1865598]

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

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. Microsoft Office (Windows)
3. Windows
4. Kaspersky

Современные профессиональные базы данных и информационные справочные системы:

1. 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.