



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: z4oR9+q8tM7HRKxyroZt9IJ1rYnX2JiG

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

Дата: 03.07.2026 г.

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

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки

09.03.03 - Прикладная информатика,

Образовательная программа «Прикладные информационные системы в экономике и
финансах»

Профиль:

«Прикладные информационные системы в экономике и финансах»

Рекомендовано

*Факультет информационных технологий и анализа больших данных
(протокол № 03 от 16.12.2025 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	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	13
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	13
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	16
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	18
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	34
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	35
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	35



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
ПKN-2	Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования	Владеет объектно-ориентированным языком программирования на уровне знания синтаксиса и семантики, основ стандартной библиотеки.	Знать: Принципы организации и структуру систем защиты программного обеспечения автоматизированных систем. Уметь: Формировать политику безопасности программных компонентов автоматизированных систем.
		Использует инструментальные средства программирования (IDE, SDK, API, популярные фреймворки и библиотеки).	Знать: принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам. Уметь: осуществлять контроль обеспечения уровня защищенности в автоматизированных системах.
		Организовывает кодовую базу, ориентируется в существующем коде, демонстрирует знание общепринятых соглашений и политик в области оформления кода.	Знать: Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем
		Проектирует текстовый, программный или графический интерфейс	Знать: программные средства обеспечения безопасности данных.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		программной системы исходя из ее назначения.	Уметь: классифицировать и оценивать угрозы информационной безопасности.
ПКН-7	Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения, в том числе с учетом требований информационной безопасности	Демонстрирует знание основ функционирования компьютерной техники, решает часто возникающие проблемы в их эксплуатации, выполняет первичную установку и настройку популярных программ и операционных систем.	Знать: типовые причины инцидентов, возникающих при установке программного обеспечения. Уметь: идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки.
		Демонстрирует знание основ функционирования операционных систем и компьютерных сетей, настраивает сетевые подключения и службы, диагностирует их работу и решает типичные задачи администрирования сетей.	Знать: типы программно-аппаратных средств обеспечения защиты информации автоматизированных систем. Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах.
		Использует серверные операционные системы для разработки и развертывания сетевых приложений, настраивает веб-службы, частично автоматизирует эти процессы.	Знать: основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Уметь: классифицировать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.
		Демонстрирует знание основ компьютерной безопасности, алгорит-	Знать: основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в ав-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		мов шифрования, хеширования, понятий аутентификации, авторизации, цифровых сертификатов, протоколов безопасной передачи данных.	томатизированных системах. Уметь: контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.



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

Заочная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 3 (в часах)
Общая трудоемкость дисциплины	4/144	144
Контактная работа – Аудиторные занятия	12	12
<i>Лекции</i>	<i>4</i>	<i>4</i>
<i>Семинары, практические занятия</i>	<i>8</i>	<i>8</i>
<i>Самостоятельная работа</i>	<i>132</i>	<i>132</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 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

Заочная 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	28	2	2	0	26
2	Информационные уязвимости объектов и угрозы информационной безопасности	28	2	0	2	26
3	Современные инновационные технологии: преимущества и социальные последствия	28	2	0	2	26
4	Социальный аспект исследования проблем защиты информации с учётом угроз информационной безопасности	28	2	0	2	26
5	Общие вопросы организации системы защиты информации в бизнесе	32	4	2	2	28



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	-	-
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.	опрос обучающихся, 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.	опрос обучающихся, 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	опрос обучающихся, групповые дискуссии



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	системы ИБ. Базовые структурные компоненты системы ИБ.	
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.	опрос обучающихся, 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	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. 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



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
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 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. Основы обеспечения информационной безопасности в банках
2. Особенности обеспечения информационной безопасности в социальных сетях
3. Информационная безопасность государства
4. Информационная безопасность цифровой экономики России
5. Информационное обеспечение деятельности органов государственной власти
6. Источники угроз безопасности персональных данных
7. VPN – Виртуальные частные сети
8. Административно-правовая ответственность в информационной сфере
9. Безопасность в интернете
10. Безопасность веб-приложений
11. Государственная система защиты информации в России
12. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
13. Гражданско-правовая ответственность в информационной сфере
14. Единая биометрическая система (ЕБС) данных клиентов банков
15. Защита информационной среды бизнеса от киберпреступлений
16. Защита коммерческой тайны компании
17. Защита конфиденциальной информации от внутренних угроз
18. Защита персональных данных в России
19. Импортозамещение в сфере информационной безопасности
20. Как злоумышленники воруют данные с помощью социальной инженерии
21. Как работает современный веб-фишинг
22. Как работают вредоносные веб-сайты
23. Киберпреступность в мире
24. Киберпреступность и киберконфликты
25. Классические файловые вирусы
26. Криптография
27. Меры государственного контроля в области обеспечения безопасности кибернетической информации
28. Место информационной безопасности в стратегии национальной безопасности Российской Федерации
29. Национальная биометрическая платформа
30. Основные каналы утечки информации в компании
31. Основные угрозы информационной безопасности



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

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»
12. Защита файлов: как защитить документ Excel от изменений (защита листа vs книги, пароли), создать резервную копию?
13. Уничтожение информации: Методы надежного уничтожения данных с носителей
14. Протоколы безопасности: Как работает TLS-рукопожатие для защиты интернет-соединений (HTTPS)?



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
ПKN-2. Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования	Владеет объектно-ориентированным языком программирования на уровне знания синтаксиса и семантики, основ стандартной библиотеки.	Знать: Принципы организации и структуру систем защиты программного обеспечения автоматизированных систем. Уметь: Формировать политику безопасности программных компонентов автоматизированных систем.	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. Выберите одну тему из списка ниже: 1. Обоснование необходимости модернизации (изменение законодательства, новые угрозы, развитие автоматизированной системы). 2. Оценка соответствия требованиям регуляторов (Приказы ФСТЭК, ФСБ). 3. Разработка плана мероприятий по реализации (этапы, сроки, ответственные). 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.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			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.
	Использует инструментальные средства программирования (IDE, SDK, API, популярные фреймворки и библиотеки).	Знать: принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам. Уметь: осуществлять контроль обеспечения уровня защищенности в автоматизированных системах.	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. Выберите одну тему из списка ниже: 1. Нормативный и организационный контроль 2. Мониторинг угроз и оценка рисков. 3. Технический и инструментальный аудит Требования к выполнению 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.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	Организовывает кодовую базу, ориентируется в существующем коде, демонстрирует знание общепринятых соглашений и политик в области оформления кода.	Знать: Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем	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. Выберите одну тему из списка ниже: 1. Нарушение конфиденциальности, целостности и доступности данных 2. Естественные (природные, техногенные) и искусственные (умышленные и неумышленные действия человека). 3. Несанкционированный доступ (НСД), перехват, внедрение вредоносного ПО. Требования к выполнению 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.
	Проектирует текстовый, программный или графический интерфейс программ-	Знать: программные средства обеспечения безопасности данных.	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:



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	ной системы исходя из ее назначения.	Уметь: классифицировать и оценивать угрозы информационной безопасности.	1. Методологии оценки рисков и моделирование угроз 2. Оценка угроз в специализированных и критических системах 3. Классификация и нейтрализация конкретных классов угроз Требования к выполнению 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.
ПKN-7. Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения,	Демонстрирует знание основ функционирования компьютерной техники, решает часто возникающие проблемы в их эксплуатации, выполняет первичную установку и настройку	Знать: типовые причины инцидентов, возникающих при установке программного обеспечения. Уметь: идентифицировать инциденты, возникающие при установке программ-	Задание: при установке корпоративного ПО на рабочие станции пользователей возникает ошибка «Не удалось зарегистрировать модуль». Идентификация инцидента: проблема вызвана отсутствием прав администратора у учетной записи пользователя, из-за чего установщик не может внести записи в реестр Windows. Опишите пошагово алгоритм Ваших действий. Обоснуйте ответ.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
в том числе с учетом требований информационной безопасности	популярных программ и операционных систем.	ного обеспечения, и принимать решение по изменению процедуры установки.	
	Демонстрирует знание основ функционирования операционных систем и компьютерных сетей, настраивает сетевые подключения и службы, диагностирует их работу и решает типичные задачи администрирования сетей.	Знать: типы программно-аппаратных средств обеспечения защиты информации автоматизированных систем. Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в авто-	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. Выберите одну тему из списка ниже: 1. Архитектура и классификация систем безопасности 2. Идентификация, аутентификация и контроль доступа 3. Защита от несанкционированного доступа: основные подходы, методики Требования к выполнению 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 вами ресурсов с активными ссылками. 5. Отчет должен содержать введение, основную часть, заключение и библиографию.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		матизированных системах.	
	Использует серверные операционные системы для разработки и развертывания сетевых приложений, настраивает веб-службы, частично автоматизирует эти процессы.	Знать: основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Уметь: классифицировать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.	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. Выберите одну тему из списка ниже: 1. Серверные операционные системы • Отличия серверных ОС (Windows Server, Linux: Ubuntu Server, AlmaLinux, Debian) от десктопных. • Управление пользователями, правами доступа (ACL), процессами, дисковыми квотами и системными службами (systemd, cron). • Настройка брандмауэров (iptables, firewalld, UFW), создание политик безопасности и управление сертификатами. 2. Развертывание сетевых приложений • Понятие гипервизоров (KVM, VMware), создание виртуальных машин и управление ими. • Основы Docker и Docker Compose. Создание Docker-образов для упаковки веб-приложений. • Настройка прокси-серверов и балансировщиков нагрузки (NGINX, HAProxy, Apache).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			3. Настройка веб-служб • Конфигурация DNS (Bind9, CoreDNS), DHCP и служб каталогов (Active Directory, LDAP). • Установка и оптимизация связок LAMP/LEMP, СУБД (PostgreSQL, MySQL/MariaDB), NoSQL (Redis, MongoDB). • Настройка почтовых серверов (Postfix, Dovecot), FTP/SFTP и сетевых хранилищ (NFS, Samba). Требования к выполнению 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.
	Демонстрирует знание основ компьютерной безопасности, алгоритмов шифрования, хеширования,	Знать: основные криптографические методы, алгоритмы, протоколы, используемые для защиты ин-	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. Выберите одну тему из списка ниже: 1. Криптографические методы и алгоритмы



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	понятий аутентификации, авторизации, цифровых сертификатов, протоколов безопасной передачи данных.	формации в автоматизированных системах. Уметь: контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.	• Симметричное шифрование: алгоритмы для быстрого шифрования данных (AES-128/256, ГОСТ 34.12-2015, ChaCha20). • Асимметричное шифрование: алгоритмы обмена ключами и шифрования (RSA, ECC, Диффи-Хеллман, ГОСТ 34.10-2018). • Хеширование: контроль целостности данных и защита паролей (SHA-256, SHA-512, ГОСТ Р 34.11-2012). • Электронные цифровые подписи (ЭЦП / ЭП): обеспечение авторства и подлинности (RSA, ECDSA). • Ваш вариант. 2. Криптографические и сетевые протоколы • Применение TLS 1.2 / TLS 1.3 для безопасных соединений (HTTPS). • Применение протоколов VPN-сетей и шлюзов (IPsec, OpenVPN, WireGuard). • Применение SSH (Secure Shell) и настройка ключей доступа. • Использование протоколов OAuth 2.0, OpenID Connect, RADIUS, TACACS+. • Ваш вариант. 3. Защита веб-служб и приложений (Web API) • Инфраструктура открытых ключей (PKI): управление цифровыми сертификатами, центры сертификации (CA). • Безопасность API: использование JWT (JSON Web Token), API-ключей, CORS и rate-limiting. • Защита веб-серверов: настройка безопасности на уровне Nginx, Apache, IIS.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
			• Межсетевые экраны и WAF: фильтрация вредоносного трафика с помощью Web Application Firewall. • Ваш вариант. 4. Автоматизация развертывания и безопасность • Инструменты для написания скриптов конфигурации серверов и веб-служб. • Безопасная передача паролей, ключей и сертификатов в автоматизированных пайплайнах. • Безопасный запуск веб-служб в изолированной среде и настройка Network Policies • Централизованный сбор системных журналов и обнаружение аномалий • Ваш вариант. Требования к выполнению 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.



Примеры практико-ориентированных заданий

Для обеспечения закрепления навыков планируется выполнение практико-ориентированных заданий. Примеры тем:

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. Можно ли автосохранение считать полноценной заменой обычному сохранению?
7. Проектное задание: разработка основ ИБ для учебного проекта (анализ угроз и выбор решений).

Примеры вопросов для подготовки к промежуточной аттестации

Примерный перечень вопросов для подготовки к экзамену:

1. Что такое информационная безопасность (ИБ) и каковы её три главные составляющие (конфиденциальность, целостность, доступность)?
2. Дайте определение понятию «информационный актив» и приведите примеры.
3. Что такое угроза информационной безопасности и чем она отличается от уязвимости и риска?
4. Объясните разницу между аутентификацией, авторизацией и идентификацией пользователя.
5. Что такое политика информационной безопасности организации и для чего она нужна?
6. Объясните разницу терминов "Событие информационной безопасности" и "Инцидент информационной безопасности"
7. Защита информации от утечки по техническим каналам.
8. Угрозы конфиденциальности, целостности и доступности информации.
9. Информационная война как высшая форма угрозы информационной безопасности.
10. Методики обеспечения непрерывности бизнеса
11. Методы и средства обеспечения бесперебойности функционирования систем.
12. Модели компьютерной безопасности.



13. Криптографическая защита информации.
14. Угрозы несанкционированного доступа в компьютерную систему.
15. Назовите основные виды вредоносного программного обеспечения (вирусы, черви, трояны, программы-вымогатели) и их отличия.
16. Что такое социальная инженерия? Приведите примеры атак с её использованием (фишинг, претекстинг).
17. Опишите механизм проведения DDoS-атаки и её цели.
18. В чём разница между инсайдером (внутренним нарушителем) и внешним злоумышленником?
19. Что такое уязвимость «нулевого дня» (zero-day)?
20. Для чего используются межсетевые экраны (брандмауэры) и системы обнаружения/предотвращения вторжений (IDS/IPS)?
21. Как работает шифрование данных? В чём разница между симметричным и асимметричным шифрованием?
22. Что такое VPN и какие задачи он решает в контексте ИБ?
23. Какова основная функция антивирусного программного обеспечения и почему важно его регулярно обновлять?
24. Объясните принцип работы двухфакторной (2FA) или многофакторной (MFA) аутентификации.
25. Какие основные законы Российской Федерации регулируют сферу информационной безопасности (например, ФЗ-152 «О персональных данных»)?
26. Назовите несколько международных стандартов в области ИБ (например, ISO/IEC 27001, NIST Cybersecurity Framework) и кратко опишите их назначение.

ПРИМЕРЫ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ

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)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Раскройте понятия: «конфиденциальность», «целостность», «доступность» информации. Приведите примеры нарушения каждого из них. Какими нормативными



документами закреплены данные понятия. (15 баллов)

2. Опишите принципы построения системы ИБ: опишите основные подходы (например, защита сетей, приложений, данных). (20 баллов)

3. Какая мера защиты эффективна против фишинга?(25 баллов)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3

1. Аутентификация и авторизация: в чем разница? Примеры применения методов. (15 баллов)

2. Особенности реализации и назначение элементов распределенной архитектуры применения СЗИ для защиты ЛВС (20 баллов)

3. Облачные сервисы для обеспечения защиты информации. Опишите ситуацию, когда применение программно-аппаратных средств, размещенных в облаке, запрещено. (25 баллов)



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

Основная литература:

1. 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]
2. 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]
3. 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]

Дополнительная литература:

1. 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]
2. 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]

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 01.12.2025 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 01.12.2025 г.)
3. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808> (дата обращения 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 г.)
8. Федеральный закон от 06.10.1997 г. № 131-ФЗ «О государственной тайне». – режим доступа: <https://duma.consultant.ru/documents/1152808> (дата обращения 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 г.)

15. ГОСТ Р 50922 Защита информации. Основные термины и определения. – режим доступа: <https://docs.cntd.ru/document/1200058320> (дата обращения 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 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 01.12.2025 г.)

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. www.cbr.ru - Официальный сайт Банка России
3. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
4. Электронно-библиотечная система Znanium <http://www.znaniium.com>
5. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
6. Информационно-образовательный портал Финуниверситета: <https://org.fa.ru>
7. • Электронно-библиотечная система издательства Лань <https://e.lanbook.com/>
8. «Деловая онлайн библиотека» издательства «Альпина Паблишер» – <http://lib.alpinadigital.ru/en/library>
9. • Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
10. • Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.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. Windows
3. Kaspersky
4. Microsoft Office (Windows)

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.