

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

**Кафедра информационной безопасности
Факультета информационных технологий и анализа больших данных**

УТВЕРЖДАЮ

Проректор по учебной и
методической работе

_____ Е.А. Каменева

«20» июня 2024 г.

Резниченко С.А.

Основы информационной безопасности

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
10.03.01 «Информационная безопасность»,
Образовательная программа
«Безопасность автоматизированных систем в кредитно-финансовой сфере»

*Рекомендовано Ученым советом
Факультета информационных технологий и анализа больших данных
(протокол от «18» июня 2024г. № 45)*

*Одобрено советом кафедры информационной безопасности
(протокол от «07» июня 2024 г. № 2)*

Москва 2024

СОДЕРЖАНИЕ

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами 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 тем дисциплины	4
5.2. Учебно-тематический план	6
5.3. Содержание семинаров, практических занятий.....	7
6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	8
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	8
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю ..	9
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	13
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	17
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	21
10. Методические указания для обучающихся по освоению дисциплины	21
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	22
11.1. Комплект лицензионного программного обеспечения:	22
11.2. Современные профессиональные базы данных и информационные справочные системы	22
11.3. Сертифицированные программные и аппаратные средства защиты информации	22
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.....	22

1. Наименование дисциплины

«Основы информационной безопасности».

2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-1	Способность понимать значение и роль информации, информационных технологий и информационной безопасности в современном обществе	1. Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе.	Знать роль информации, информационных технологий и информационной безопасности в современном обществе. Уметь применять основные стандарты информационной безопасности реализации политики информационной безопасности
		2. Понимает значение единых для всех людей, общества, государства, человечества жизненно важных интересов: безопасности, доступа к информации.	Знать значение единых для всех людей, общества, государства, человечества жизненно важных интересов Уметь контролировать доступа к информации.
		3. Демонстрирует знание теории информационного общества, концепции цифрового государства, цифровой экономики.	Знать теории информационного общества, концепции цифрового государства, цифровой экономики Уметь разрабатывать руководящие документы информационной безопасности в кредитно-финансовых и банковских системах
		4. Демонстрирует знание основных доктринальных документов Российской Федерации в области безопасности, информационной безопасности, информационного общества и международных соглашений в этих областях.	Знать основные доктринальные документы Российской Федерации в области безопасности, информационной безопасности, информационного общества и международных соглашений в этих областях. Уметь разрабатывать руководящие документы информационной безопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» входит в общепрофессиональный цикл образовательной программы по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в кредитно-финансовой сфере».

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

Таблица 2

Вид учебной работы по дисциплине	Всего (в з.е и часах)	Семестр 1 (в часах)
Общая трудоёмкость дисциплины	3 з.е./108	108
Контактная работа-Аудиторные занятия	48	48
<i>Лекции</i>	16	16
<i>Семинары, практические занятия в т.ч.</i>	32	32
Самостоятельная работа	60	60
Вид текущего контроля	эссе	эссе
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 тем 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 и их краткая характеристика. Системные связи информационной безопасности с другими видами 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.

Тема 2. Информационные уязвимости объектов и угрозы информационной безопасности и их источники

Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные

информационные уязвимости. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз.

Тема 3. Средства обеспечения информационной безопасности

Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Тема 4. Риски информационной безопасности и проблема построения комплексной системы защиты информации

Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.

Тема 5. Общие вопросы организации системы защиты информации на предприятии

Технические, правовые и организационные методы и средства защиты информации. Защита от стихийных бедствий. Требования законодательства по обеспечению бесперебойности функционирования систем и непрерывности бизнеса. Стандарты и лучшие практики обеспечения непрерывности бизнеса. Показатели бесперебойности функционирования систем.

5.2. Учебно-тематический план

Таблица 3

№ п/ п	Наименование разделов дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа * - Аудиторная работа			Самостоятельная работа	
			Общая	Лекции	Семинары, практические занятия		
1.	Государственная политика в области информационной безопасности в системе национальной безопасности	20	6	2	4	14	Доклады и дискуссии
2.	Информационные уязвимости объектов и угрозы информационной безопасности и их источники	20	6	2	4	14	Доклады и дискуссии
3.	Средства обеспечения информационной безопасности	22	12	4	8	10	Доклады и дискуссии
4.	Риски информационной безопасности и проблема построения комплексной системы защиты информации	22	12	4	8	10	Доклады и дискуссии
5.	Общие вопросы организации системы защиты информации на предприятии	24	12	4	8	12	Доклады и дискуссии
	В целом по дисциплине	108	48	16	32	60	Согласно учебному плану: эссе
	Итого в %		44	33	67	56	

*объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности

5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование тем дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	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. Источники: 8.1, 8.3, 8.4, 8.5, 8.6; 8.28, 8.33, 9.1-9.14	групповые дискуссии, презентация основных подходов. Учебное задание: Практика работы с УЦ
Информационные уязвимости объектов и угрозы информационной безопасности и их источники	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Источники: 8.1, 8.2, 8.28, 9.1 – 9.14	групповые дискуссии, групповые дискуссии презентация основных подходов. Учебное задание: Общие правила работы с хэш-функций
Средства обеспечения информационной безопасности	Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам. Источники: 8.1, 8.4, 8.5; 8.33, 9.1-9.14	групповые дискуссии презентация основных подходов. Учебное задание: Реализация системного подхода при создании АСЗИ
Риски информационной безопасности и проблема построения комплексной системы защиты информации	Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Оценка рисков и организация управления процессом защиты информации. Источники: 8.1, 8.2, 8.3, 8.15, 8.29, 9.1-9.14	групповые дискуссии презентация основных подходов. Учебное задание: Работа с электронной подписью в организациях кредитно-финансовой сферы
Общие вопросы организации системы защиты информации на предприятии	Требования законодательства по обеспечению бесперебойности функционирования систем и непрерывности бизнеса. Стандарты и лучшие практики обеспечения непрерывности бизнеса. Показатели бесперебойности функционирования систем. Источники: 8.1, 8.2, 8.28, 9.1-9.14	групповые дискуссии презентация основных подходов. Учебное задание: Изучение иерархии УЦ

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

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

Таблица 5

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; - подготовка презентаций по теме; - выполнение учебного задания
Информационные уязвимости объектов и угрозы информационной безопасности и их источники	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Средства обеспечения информационной безопасности	Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Риски информационной безопасности и проблема построения комплексной системы защиты информации	Оценка рисков и организация управления процессом защиты информации.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Общие вопросы организации системы защиты информации на предприятии	Требования законодательства по обеспечению бесперебойности функционирования систем и непрерывности бизнеса. Стандарты и лучшие практики обеспечения непрерывности бизнеса.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания

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

Форма текущего контроля – эссе.

Основные формы текущего контроля:

- участие в дискуссиях по проблемным темам дисциплины;
- выступление с докладом по проблемным темам дисциплины;
- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, письменных работ, обсуждение и анализ их результатов.

Примерный перечень вопросов к дискуссии

1. Сравните между собой подходы к классификации угроз безопасности информации с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
2. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям.
3. Национальные интересы личности, общества и государства в информационной сфере.
4. Международные стандарты обеспечения непрерывности бизнеса.
5. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства

Примерные темы докладов с презентациями

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.

Примеры учебных практических 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.

Примерный перечень вопросов к письменной работе

1. Какие вам 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 вам методы и средства контроля акустической информации.

11. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

Примерные темы эссе

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 (Г осСОПКА)
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 в 2019 году
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 её 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 информационной безопасности.

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

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их 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, знаний и умений

Таблица 6

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенций	Типовые контрольные задания
ПКН-1 Способность понимать значение и роль информации, информационных технологий и информационной безопасности в современном обществе	1. Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе.	Знать роль информации, информационных технологий и информационной безопасности в современном обществе. Уметь применять основные стандарты информационной безопасности реализации политики информационной безопасности	Задание 1. Назовите национальные стандарты Российской Федерации в области программно-аппаратной защиты информации. Поясните их особенности и области применения.

			<p>Задание 2. Разработайте документ «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».</p>
	<p>2. Понимает значение единых для всех людей, общества, государства, человечества жизненно важных интересов: безопасности, доступа к информации.</p>	<p>Знать значение единых для всех людей, общества, государства, человечества жизненно важных интересов Уметь контролировать доступа к информации.</p>	<p>Задание 1. Предложите план внедрения ЭП в кредитной организации на основе знания стандартов.</p> <p>Задание 2. Опишите мероприятия по контролю внедрения ЭП</p>
	<p>3. Демонстрирует знание теории информационного общества, концепции цифрового государства, цифровой экономики.</p>	<p>Знать теории информационного общества, концепции цифрового государства, цифровой экономики Уметь разрабатывать руководящие документы информационной безопасности в кредитно-финансовых и банковских системах</p>	<p>Задание 1. Какие справочные правовые системы необходимы для получения доступа к нормативным актам по вопросам информационной безопасности</p> <p>Задание 2. Разработайте мероприятия по контролю внедрения ЭП в кредитно-финансовых и банковских системах</p>
	<p>4. Демонстрирует знание основных</p>	<p>Знать основные доктринальные документы</p>	<p>Задание 1. Опишите требования,</p>

	доктринальных документов Российской Федерации в области безопасности, информационной безопасности, информационного общества и международных соглашений в этих областях.	Российской Федерации в области безопасности, информационной безопасности, информационного общества и международных соглашений в этих областях. Уметь разрабатывать руководящие документы информационной безопасности	предъявляемые регуляторами при установлении требований по защите персональных данных Задание 2. Разработать проект мероприятий по модернизации системы информационной безопасности для локальной вычислительной сети кредитно-финансовой организации.
--	---	--	---

Примерный перечень вопросов к экзамену

1. Государственная система защиты информации в России
2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
3. Гражданско-правовая ответственность в информационной сфере
4. Единая биометрическая система (ЕБС) данных клиентов банков
5. Защита информационной среды бизнеса от киберпреступлений
6. Защита коммерческой тайны компании
7. Защита конфиденциальной информации от внутренних угроз
8. Защита персональных данных в России
9. Импортзамещение в сфере информационной безопасности
10. Информационная безопасность в социальных сетях
11. Киберпреступность и киберконфликты
12. Классические файловые вирусы
13. Меры государственного контроля в области обеспечения безопасности кибернетической информации
14. Место информационной безопасности в стратегии национальной безопасности Российской Федерации

15. Национальная биометрическая платформа
16. Основные каналы утечки информации в компании
17. Основные угрозы информационной безопасности
18. Система обеспечения информационной безопасности объекта информатизации.
19. Понятие правового режима информации
20. Понятия информации и информационных ресурсов в законодательстве
21. Потери банков от киберпреступности
22. Право граждан на доступ к информации
23. Шпионские программы - новое оружие для международного кибершпионажа
24. Правовая защита информации
25. Правовой режим информации, составляющей государственную тайну
26. Правовой режим коммерческой тайны
27. Правовой режим персональных данных
28. Предотвращения утечек информации (DLP)
29. Преступления в информационной сфере
30. Профессиональная и служебная тайна в РФ
31. Сбор информации из открытых источников - как видят вас потенциальные злоумышленники?
32. Система резервного копирования
33. Системы аутентификации
34. Современная защита информационной безопасности в России: проблемы и направления её развития
35. Информационная безопасность государства
36. Информационная безопасность цифровой экономики России
37. Информационное обеспечение деятельности органов государственной власти
38. Киберпреступность в мире
39. Новые факторы использования криптографических средств в цифровой среде.
40. Задачи и средства обнаружения и противодействия компьютерным атакам в

киберпространстве.

Пример экзаменационного билета

<p align="center">Федеральное государственное образовательное бюджетное учреждение высшего образования «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ» (Финансовый университет)</p> <p>Кафедра <u>информационной безопасности</u> Дисциплина <u>«Основы информационной безопасности»</u> <u>Факультет информационных технологий и анализа больших данных</u> Форма обучения <u>очная</u> Семестр 1 Направление 10.03.01 <u>«Информационная безопасность»</u> Профиль <u>«Безопасность автоматизированных систем в кредитно-финансовой сфере»</u></p> <p align="center">ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</p> <table border="1"><tr><td>1.</td><td>Информационное обеспечение деятельности органов государственной власти</td><td>(15 баллов)</td></tr><tr><td>2.</td><td>Защита конфиденциальной информации от внутренних угроз</td><td>(15 баллов)</td></tr><tr><td>3.</td><td>Определите основные задачи аттестации защищённых информационных систем по требованиям безопасности и предложите план мероприятий её проведения.</td><td>(30 баллов)</td></tr></table> <p>Подготовил _____ С.А. Резниченко На основе перечня теоретических вопросов и практико-ориентированных заданий, утвержденного на заседании кафедры информационной безопасности (протокол № __ от _____) Утверждаю: заведующий кафедрой _____ В.М. Селезнёв Дата _____</p>			1.	Информационное обеспечение деятельности органов государственной власти	(15 баллов)	2.	Защита конфиденциальной информации от внутренних угроз	(15 баллов)	3.	Определите основные задачи аттестации защищённых информационных систем по требованиям безопасности и предложите план мероприятий её проведения.	(30 баллов)
1.	Информационное обеспечение деятельности органов государственной власти	(15 баллов)									
2.	Защита конфиденциальной информации от внутренних угроз	(15 баллов)									
3.	Определите основные задачи аттестации защищённых информационных систем по требованиям безопасности и предложите план мероприятий её проведения.	(30 баллов)									

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

Нормативные акты

Нормативные акты

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (В редакции от 02.07.2021 г.).

2. Федеральный закон от 06.04.2011 № 63 -ФЗ «Об электронной подписи». [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

3. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне» (В редакции от 11.06.2021 г.)
4. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (В редакции от 09.03.2021 г.).
5. Распоряжение Правительства России от 28 июля 2017 г. №1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации»
6. Международный стандарт. ISO/IEC 27000:2005 Информационные
7. технологии. Методы обеспечения безопасности. Определения и основные принципы. [Электронный документ]. Режим доступа: URL:
8. <http://www.consultant.ru/>.
9. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.
10. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне» (В редакции от 11.06.2021 г.)
11. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (В редакции от 09.03.2021 г.).
12. Распоряжение Правительства России от 28 июля 2017 г. №1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации»
13. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
14. 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».
15. ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

16. ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
17. ГОСТ Р 50922 Защита информации. Основные термины и определения.
18. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
19. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
20. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.
21. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
22. ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
23. ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
24. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
25. ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
26. ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
27. ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

Рекомендуемая литература:

а) основная:

28. Крылов, Г. О. Базовые понятия информационной безопасности: учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. – Москва : Русайнс, 2020. - 258 с. – Текст : непосредственный. – То же. – 2024. – ЭБС BOOK.ru. - URL:<https://book.ru/book/953646> (дата обращения: 11.07.2024). – Текст : электронный.

29. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. – ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1284190>; ЭБС Университетская библиотека online. - URL: <https://biblioclub.ru/index.php?page=book&id=610688> (дата обращения: 11.07.2024). – Текст : электронный.

30. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола : Поволжский государственный технологический университет, 2020. - 154 с. – ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1894130> (дата обращения: 11.07.2024). – Текст : электронный.

б) дополнительная:

31. 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 : Горячая линия-Телеком, 2016. – 170 с. – ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/560782> (дата обращения: 11.07.2024). - Текст : электронный.

32. Мельников, В. П. Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева; под ред. В. П. Мельникова. — 2-е изд., перераб. и доп. - Москва : КноРус, 2022. — 371 с. — (Бакалавриат). - ЭБС BOOK.ru. — URL: <https://book.ru/book/941809> (дата обращения: 11.07.2024). — Текст : электронный.

33. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие /

П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1865598> (дата обращения: 11.07.2024). — Текст : электронный.

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

1. Сайт Центрального банка Российской Федерации: www.cbr.ru.
2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru.
3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>.
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>.
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>.
7. Электронно-библиотечная система Znaniy <http://www.znaniy.com>.
8. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>.
9. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>.
10. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>.
11. Электронная библиотека Издательского дома «Гребенников» <https://grebennikon.ru/>.
12. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>.
13. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>.
14. Национальная электронная библиотека <http://нэб.рф/>.
- 15.

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 23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры 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

11.1. Комплект лицензионного программного обеспечения:

ОС Astra Linux, Windows, Microsoft Office
антивирус Kaspersky

11.2 Современные профессиональные базы данных и информационные справочные системы:

1. Информационно-правовая система «Гарант».
2. Информационно-правовая система «Консультант Плюс».
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>.
4. Система комплексного раскрытия информации «СКРИН» -<http://www.skrin.ru/>.

11.3 Сертифицированные программные и аппаратные средства защиты информации:

Не предусмотрены.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Занятия по дисциплине проводятся в аудиториях, оборудованных

мультимедийными комплексами, компьютерами с выходом в Интернет.