

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

Тульский филиал Финуниверситета

Кафедра «Математика и информатика»

СОГЛАСОВАНО

ЗАО «ЛИМ»

Генеральный директор

 **В.В. Куликов**
«19» декабря 2024 г.



УТВЕРЖДАЮ

Директор филиала

Г.В. Кузнецов

«24» декабря 2024 г.



Е.В. Манохин

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
09.03.02 Информационные системы и технологии,
образовательная программа «Информационные технологии в экономике»,
профиль «Информационные технологии в управлении цифровой экономикой»

*Рекомендовано Ученым советом Тульского филиала Финуниверситета
(протокол от 24 декабря 2024 г. № 22)*

*Одобрено заседанием кафедры «Математика и информатика»
(протокол от 02 декабря 2024 г. № 5)*

Тула 2024

СОДЕРЖАНИЕ

№ п/п	Наименования	Стр.
1.	Название 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.	3
4.	Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	3
5.	Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объёмов (в академических часах) и видов учебных занятий	4
5.1.	Содержание дисциплины	4
5.2.	Учебно-тематический план	6
5.3.	Содержание семинаров, практических занятий	7
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 (согласно таблице 2)	10
7.	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	13
8.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	18
9.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	19
10.	Методические указания для обучающихся по освоению дисциплины	20
11.	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационно справочных систем (при необходимости)	21
12.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	21

1. Наименование дисциплины

Управление информационной безопасностью.

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	1. Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике.	Знать способы поиска информации в открытых источниках по вопросам информационной безопасности. Уметь находить в открытых источниках необходимую информацию по вопросам информационной безопасности.
		2. Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	Знать методы обзора и анализа информации по вопросам информационной безопасности. Уметь осуществлять систематический обзор источников информации по вопросам информационной безопасности, анализировать содержащиеся в них данные, делать обоснованные выводы на основе проведенного обзора.
		3. Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	Знать основные требования информационной безопасности, основные алгоритмы защиты информации. Уметь использовать основные алгоритмы защиты информации, в том числе с использованием криптографических протоколов.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к общефилиальному (предпрофильному) циклу дисциплин части учебного плана, формируемой участниками образовательных отношений, направления подготовки 09.03.02 Информационные системы и технологии.

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

Таблица 1

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Семестр 4 (в часах)
Общая трудоемкость дисциплины	4 зач.ед./144 ч.	144
Контактная работа-Аудиторные занятия	68	68
<i>Лекции</i>	34	34
<i>Семинары, практические занятия</i>	34	34
Самостоятельная работа	76	76
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	зачет	зачет

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

5.1. Содержание тем дисциплины

Раздел 1. Управление информационной безопасностью 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.

Основные положения законодательных актов России по информационной безопасности. Руководящие документы ФСТЭК. Основные подходы к аудиту информационной безопасности предприятия. Государственные и международные стандарты в области информационной безопасности. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности. Принципы организации работ с информацией, составляющей коммерческую тайну.

Раздел 2. Информационные уязвимости объектов

Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно-вычислительная система. Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации.

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

Методы практического обеспечения защиты информации корпоративных систем. Направления политики информационной безопасности предприятия. Проблемы защиты информации в банках.

Раздел 3. 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. Информационная война как высшая форма угрозы информационной безопасности.

Особенности защиты информации в вычислительных сетях. Особенности лицензирования в области информационной безопасности РФ. Специфика организации обучения и инструктирования сотрудников правилам работы с конфиденциальной информацией.

Подходы к классификации угроз угрозы информации по степени защиты. Уязвимости электронного документооборота. Основные принципы системной классификации угроз безопасности информации. Риски при идентификации и аутентификации пользователей. Риски утечки акустической информации. Риски утечки информации по техническим каналам.

Раздел 4. 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.

Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях. Определение криптографии, ее методы и алгоритмы. Определение стеганография, ее достоинства и недостатки. Системы криптографической защиты информации в России. Специфика программно-аппаратных, криптографических средств защиты информации банковских карт.

Раздел 5. 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. Основные подходы к оценке рисков атак на информационные системы. Типы компьютерных вирусов и специфических для них рисков. Модели оценки рисков. Наиболее актуальные подходы к управлению процессом защиты информации. Наиболее значимые нормативные документы, регулирующие процессы управления защитой информации.

Информационные риски организации. Стратегии снижения рисковозависимости предприятия в процессе управления. Характер оценивания информационных рисков в процессе управления предприятием.

Раздел 6. Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей

Развитие идей и концепций защиты информации в банках. Специфика рисков банковских угроз информационной безопасности. Типы угроз банковской безопасности. Наиболее уязвимые для банков каналы передачи информации.

Основные методы защиты от перехвата информации в банковских системах. Перспективы использования блокчейна для защиты банковской информации. Элементы комплексной системы информационной безопасности предприятия. Методы защиты информации техническими средствами в каналах связи банков. Организационные источники и каналы утечки информации в банках. Условия проверки на полиграфе в финансовых организациях. Особенности организации защиты информации в кадровой службе.

5.2. Учебно-тематический план

Таблица 2

№ № п/ п	Наименование темы (раздела) дисциплины	Трудоемкость в часах				Самостоятель ная работа	Формы текущего контроля успеваемости
		Всего	Контактная работа - Аудиторная работа				
			Общая	Лекции	Семинары, практические занятия		
1.	Управление информационной безопасностью в системе национальной безопасности	16	8	4	4	8	Дискуссия, обсуждение
2.	Информационные уязвимости объектов	16	8	4	4	8	Выполнение индивидуальных заданий
3.	Угрозы информационной безопасности и их источники	16	8	4	4	8	Выполнение индивидуальных заданий
4.	Средства обеспечения информационной безопасности	26	12	6	6	14	Выполнение индивидуальных заданий
5.	Риски информационной безопасности и проблема построения комплексной системы защиты информации	34	16	8	8	18	Выполнение индивидуальных заданий
6.	Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей	36	16	8	8	20	Выполнение индивидуальных заданий
В целом по дисциплине		144	68	34	34	76	Согласно учебному плану: контрольная работа
Итого в %		100	47	50	50	53	-

5.3. Содержание семинаров, практических занятий

Таблица 3

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Тема 1. Управление информационной безопасностью в системе национальной безопасности	1. Основные положения законодательных актов России по информационной безопасности. 2. Руководящие документы ФСТЭК. 3. Основные подходы к аудиту информационной безопасности предприятия. 4. Государственные и международные стандарты в области информационной безопасности. 5. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности. 6. Принципы организации работ с информацией, составляющей коммерческую тайну. Рекомендуемые источники: 8. 1-4; 9.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Изучение профессиональной терминологии в области информационной безопасности и информационного противоборства. Моделирование наиболее эффективного решения проблемы обеспечения информационной безопасности.
Тема 2. Информационные уязвимости объектов	1. Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации. 2. Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости. 3. Методы практического обеспечения защиты информации корпоративных систем. Направления политики информационной безопасности предприятия. Проблемы защиты информации в банках. Рекомендуемые источники: 8. 1-4; 9.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Анализ конкретных правовых актов в области информационной безопасности.
Тема 3. Угрозы информационной безопасности и их источники	1. Подходы к классификации угроз угрозы информации по степени защиты. 2. Уязвимости электронного документооборота. 3. Основные принципы системной классификации угроз безопасности информации. 4. Риски при идентификации и аутентификации пользователей. 5. Риски утечки акустической информации.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры

	6. Риски утечки информации по техническим каналам. Рекомендуемые источники: 8. 1-4; 9.	и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
Тема 4. Средства обеспечения информационной безопасности	1. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях. 2. Определение криптографии, ее методы и алгоритмы. 3. Определение стеганография, ее достоинства и недостатки. 4. Системы криптографической защиты информации в России. 5. Специфика программно-аппаратных, криптографических средств защиты информации банковских карт. Рекомендуемые источники: 8. 1-4; 9.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование способов противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.
Тема 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации	1. Основные подходы к оценке рисков атак на информационные системы. 2. Типы компьютерных вирусов и специфических для них рисков. 3. Модели оценки рисков. 4. Наиболее актуальные подходы к управлению процессом защиты информации. 5. Наиболее значимые нормативные документы, регулирующие процессы управления защитой информации. Рекомендуемые источники: 8. 1-4; 9.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Разработка методики оценки информационных рисков, ее обсуждение и экспертная оценка.
Тема 6. Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей	1. Специфика рисков банковских угроз информационной безопасности. 2. Типы угроз банковской безопасности. 3. Наиболее уязвимые для банков каналы передачи информации. 4. Основные методы защиты от перехвата информации в банковских системах. 5. Перспективы использования блокчейна для защиты банковской информации. Рекомендуемые источники: 8. 1-4; 9.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование возможных каналов перехвата при передаче информации системами связи (электромагнитные, электрические, индукционные) и разработка способов их защиты.

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

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

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Управление информационной безопасностью в системе национальной безопасности	1. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности. 2. Принципы организации работ с информацией, составляющей коммерческую тайну	- работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
Тема 2. Информационные уязвимости объектов	3. Антропогенные информационные уязвимости. 4. Техногенные информационные уязвимости. 5. Организационно-правовые и комбинированные информационные уязвимости.	- работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; - подготовка презентаций по теме.
Тема 3. Угрозы информационной безопасности и их источники	1. Техногенные угрозы информационной безопасности. 2. Угрозы информационной безопасности, связанные с человеческим фактором. 3. Особенности защиты информации в вычислительных сетях. 4. Особенности лицензирования в области информационной безопасности РФ. 5. Специфика организации обучения и инструктирования сотрудников правилам работы с конфиденциальной информацией.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
Тема 4. Средства обеспечения информационной безопасности	1. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. 2. Программно-аппаратные, криптографические и стенографические средства обеспечения информационной безопасности. 3. Пассивные и активные средства противодействия техническим разведкам. 4. Защита информации от утечки по техническим каналам	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.

Тема 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации	1. Информационные риски организации. 2. Стратегии снижения рискозависимости предприятия в процессе управления. 3. Характер оценивания информационных рисков в процессе управления предприятием.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
Тема 6. Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей	1. Элементы комплексной системы информационной безопасности предприятия. 2. Методы защиты информации техническими средствами в каналах связи банков. 3. Организационные источники и каналы утечки информации в банках. 4. Условия проверки на полиграфе в финансовых организациях. 5. Особенности организации защиты информации в кадровой службе.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю (согласно таблице 2)

Текущий контроль осуществляется в ходе учебного процесса и контроля самостоятельной работы обучающихся, по результатам выполнения контрольных работ. Основными формами текущего контроля знаний являются:

- обсуждение вопросов и задач, вынесенных в планах семинарских занятий в качестве самостоятельных заданий;
- решение задач в аудитории по теме занятия, выполнение заданий на компьютере, их обсуждение;
- подготовка, обсуждение вопросов и задач внеаудиторных самостоятельных и аудиторных контрольных работ.

Примерный перечень вопросов к контрольной работе, примеры заданий контрольных работ

1. Социальная значимость специалиста в области информационной безопасности.
2. Современные угрозы интересам личности и обеспечение информационной безопасности.
3. Информационные войны: особенности их ведения в современном мире.
4. Проблема разработки «Этического кодекса» специалиста в области информационной безопасности.
5. Особенности профессиональной коммуникации в информационном обществе.
6. Основные пути формирования толерантности у специалиста в области информационной безопасности.
7. Национально-культурная специфика «хакерства» как субкультуры.
8. Социально-психологический портрет инсайдера в области информационной безопасности.
9. Математика и криптография: основные тенденции развития.
10. Современная конкурентная разведка и ее возможности.

11. Правовые проблемы информационной безопасности.
12. Big Data и Управление информационной безопасностью.
13. Современные дискуссии о копирайте.
14. Трудности внедрения электронной цифровой подписи в России
15. Проблемы обеспечения информационной безопасности систем электронного правительства.
16. «Темный Интернет»: перспективы и опасности его развития.
17. Квантовые компьютеры и перспективы развития информационной безопасности.
18. Возможности современных интеллектуальных систем (ИИ) в обеспечении информационной безопасности.
19. Криптовалюты и управление информационной безопасностью.
20. Значение развития технологий блокчейна для информационной безопасности.
21. Социально-психологические и личностные характеристики специалиста по защите информации.
22. Профилактические меры по предотвращению компьютерной преступности.
23. Биометрия в банковских системах и проблемы обеспечения информационной безопасности.
24. Нейросети и возможности их использования для выявления угроз информационной безопасности.
25. Самообучающиеся информационные системы и возможности их использования в информационной безопасности.

Примерный перечень вопросов к аудиторной письменной работе

1. «Глубокая паутина»: перспективы и опасности его развития.
2. Новые социальные сетевые технологии и Управление информационной безопасностью.
3. Проблемы обеспечения информационной безопасности в банковских системах.
4. Искусственный интеллект и Управление информационной безопасностью.
5. Блокчейна и Управление информационной безопасностью
6. Основные подходы к эффективному ведению информационных войн.
7. Перспективы развития информационной безопасности в XXI веке.
8. Электронные деньги и проблемы информационной безопасности.
9. Математические методы в криптографии.
10. Типология и национально-психологические особенности хакеров.
11. Нейросети в информационной безопасности
12. Этический кодекс специалиста в области информационной безопасности
13. Профессиональные сообщества и Управление информационной безопасностью
14. Управление информационной безопасностью
15. Этика специалиста в области информационной безопасности

16. Электронное правительство и Управление информационной безопасностью
17. Виды компьютерной преступности компьютерной преступности
18. Эволюция информационных систем и информационной безопасности
19. Контент - анализ и Управление информационной безопасностью
20. Копирайт и Управление информационной безопасностью
21. Личность и ее Управление информационной безопасностью.
22. Значение информационной безопасности в развитии общества.
23. Требования к специалисту по защите информации
24. Инсайдинг и Управление информационной безопасностью.
25. Электронная подпись и Управление информационной безопасностью.

Примерный перечень докладов и презентаций по проблемным темам дисциплины

1. Проблема определения понятия «информационный риск».
2. Специфика информационного риска в рискологии.
3. Проблема количественного измерения информационного риска.
4. Основные подходы к определению качественной специфики информационного риска.
5. Специфика рисков информационной безопасности в России.
6. Специфика рисков информационной безопасности в Китае.
7. Специфика рисков информационной безопасности в США.
8. Специфика рисков информационной безопасности в Индии.
9. Специфика рисков информационной безопасности в Англии.
10. Специфика рисков информационной безопасности во Франции.
11. Специфика рисков информационной безопасности в Германии.
12. Особенности рисков информационной безопасности в Японии.
13. Специфика рисков информационной безопасности в Канаде.
14. Специфика рисков информационной безопасности в Австралии.
15. Особенности хакерской активности в Канаде.
16. Особенности хакерской активности в Австралии.
17. Особенности хакерской активности в России.
18. Особенности хакерской активности в Японии.
19. Особенности хакерской активности в Германии.
20. Особенности хакерской активности в Китае.
21. Особенности хакерской активности в Англии.
22. Особенности хакерской активности во Франции.
23. Особенности хакерской активности в США.
24. Особенности хакерской активности в Индии.
25. Проблема использования новых социальных сетевых технологий при оценке информационных рисков.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

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».

Таблица 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые задания
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	Индикатор 1. Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике.	Знать способы поиска информации в открытых источниках по вопросам информационной безопасности. Уметь находить в открытых источниках необходимую информацию по вопросам информационной безопасности.	Задание 1. Выявить основные принципы управления при решении задач в области информационной безопасности. Задание 2. Провести анализ возможных стратегий при решении задач в области информационной безопасности.
	Индикатор 2. Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	Знать методы обзора и анализа информации по вопросам информационной безопасности. Уметь осуществлять систематический обзор источников информации по вопросам информационной безопасности, анализировать содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	Задание 1. Разработать стратегию эффективного управления для решения задач обеспечения информационной безопасности. Задание 2. Разработать этапы реализации стратегии и определить сопутствующие риски при решении задач обеспечения информационной безопасности. Задание 3. Определить риски и степень ответственности при решении задач информационной безопасности. Задание 4. Разработать базовые положения этического кодекса

			специалиста в области информационной безопасности.
	Индикатор 3. Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	Знать основные требования информационной безопасности, основные алгоритмы защиты информации. Уметь использовать основные алгоритмы защиты информации, в том числе с использованием криптографических протоколов.	Задание 1. Выбрать наиболее эффективные средства сбора необходимой информации для решения задач информационной безопасности. Задание 2. Провести анализ возможных стратегий сбора информации для решения профессиональных задач. Задание 3. Разработать алгоритм выбора наиболее эффективных информационных ресурсов и программ для решения задач обеспечения информационной безопасности. Задание 4. Проанализировать и выбрать наиболее эффективные для решения проблем информационной безопасности информационные ресурсы. Задание 5. Разработать алгоритм выбора и использования имеющихся новых социальных сетевых технологий для обеспечения информационной безопасности. Задание 6. Разработать алгоритм и критерии отбора информации для решения профессиональных задач в глобальных компьютерных сетях.

Примерный перечень вопросов к зачету

1. Какие вам известны подходы к классификации угроз безопасности информации?
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

4. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?
5. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
6. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.
7. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.
8. Охарактеризуйте проблему определения предметной области информационной безопасности.
9. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.
10. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.
11. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?
12. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.
13. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
14. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
15. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
16. Объясните, что представляет собой стеганография?
17. Расскажите об особенностях симметричных и несимметричных шифров.
18. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?
19. Охарактеризуйте наиболее известный алгоритм шифрования DES.
20. Каковы основные особенности криптосистем с общедоступным ключом?
21. Раскройте основное содержание алгоритма электронной цифровой подписи.
22. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.
23. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
24. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

25. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
26. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?
27. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
28. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.
29. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
30. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.
31. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.
32. Дайте классификацию источников утечки информации по техническим каналам.
33. Назовите известные вам методы и средства контроля акустической информации.
34. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.
35. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.
36. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.
37. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.
38. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.
39. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?
40. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.
41. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.
42. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.
43. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.
44. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд,

преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

45. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.
46. Интеллектуальная банковская карта, ее защита.
47. Меры наказания за противозаконные деяния в сфере платежных карт.
48. Меры предосторожности при использовании банкоматов.
49. Меры предосторожности при оплате картой покупок в Интернете.
50. Базовый набор требований к системе ИБ организаций БС РФ.

Примеры тестовых заданий

Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство:

- a. доступность
- b. детерминированность
- c. восстанавливаемость
- d. целостность.

Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели:

- a. искажение
- b. наблюдение
- c. компрометация
- d. перехват.

Длина исходного ключа у алгоритма шифрования DES (бит)

- a. 56
- b. 128
- c. 64
- d. 256.

Защита информации это:

- a. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- b. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- c. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- d. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё. Обоснуйте ваш выбор.

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- a. активный перехват;
- b. пассивный перехват;
- c. аудиоперехват;
- d. исследования.

Примеры практико-ориентированных (ситуационных) заданий

1. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации?
2. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
3. Рассмотрите возможности несанкционированного получения информации в следующем случае:
 - в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;
 - объектами несанкционированных действий, являются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;
 - каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача ее на печать.Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?
4. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.
5. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

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

Нормативные акты

1. ISO/IEC 27001:2013 Информационные технологии - методы информационной безопасности - Системы управления информационной безопасностью – требования.
2. ISO/IEC 27005:2011 Информационные технологии - методы информационной безопасности - Системы управления информационной безопасностью.
3. ISO/IEC 27031:2011 Информационные технологии - методы информационной безопасности - Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса.

4. ISO/IEC 27032:2012 Информационные технологии - методы информационной безопасности - Руководящие указания по кибербезопасности.

Основная литература

1. Суворова Г.М. Информационная безопасность [Электронный ресурс]: учебное пособие для вузов/Г.М. Суворова. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 277 с.//Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/544029>. (дата обращения: 30.09.2024)
2. Гришина Н.В. Основы управления информационной безопасностью [Электронный ресурс]: учебно-методическое пособие/Н.В. Гришина. Москва: ИНФРА-М, 2021. 99 с. URL: <https://znanium.ru/catalog/product/1859951>. (дата обращения: 30.09.2024).

Дополнительная литература

3. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]: монография/И.С. Клименко. Москва: ИНФРА-М, 2024. 180 с. URL: <https://znanium.com/catalog/product/2052391>. (дата обращения: 30.09.2024).
4. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник для вузов/Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; под редакцией Т.А. Поляковой, А.А. Стрельцова. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 357 с.//Образовательная платформа Юрайт [сайт]. URL: <https://urait.ru/bcode/555950>. (дата обращения: 30.09.2024).

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

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
4. Электронно-библиотечная система Znanium <http://www.znanium.com>
5. Электронно-библиотечная система издательства «ЮРАЙТ» <https://www.biblio-online.ru/>
6. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>
7. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
8. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
9. Национальная электронная библиотека <http://нэб.рф/>
10. Сайт Федеральной службы по техническому и экспортному контролю www.fstec.ru
11. Проект «Управление информационной безопасностью бизнеса» <http://www.infosecurity.ru/>
12. «Государственные стандарты» <http://meganorm.ru/list/14-0.htm>
13. «Инфофорум» <http://www.infoforum.ru/>
14. «Академия информационной самозащиты» <http://www.iwars.su/>
15. «Управление информационной безопасностью» <http://www.itsec.ru/main.php/>

10. Методические указания для обучающихся по освоению дисциплины

Обучение по дисциплине предполагает изучение курса на аудиторных занятиях (лекции и семинарские занятия) и самостоятельной работы. Семинарские занятия по дисциплине предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций. Курс предполагает широкое использование интерактивных методов обучения. Для проведения семинарских занятий активно используются методы работы в малых группах, вовлечение в индивидуальную работу. При проведении семинарских занятий используются презентации.

Студентам необходимо ознакомиться с содержанием рабочей программы дисциплины (далее - РПД), с целями и задачами дисциплины, методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры.

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, студентам необходимо перед каждой лекцией просматривать рабочую программу дисциплины, просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось – обратиться к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Студентам при подготовке к семинарским занятиям следует:

- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и там, где это необходимо, нормативно-правовые акты, интернет-источники;
- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении практико-ориентированных заданий, заданных для самостоятельного решения;
- в ходе семинара давать конкретные, четкие ответы по существу вопросов;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных анализов, ситуаций, в случае затруднений обращаться к преподавателю.

После теоретического лекционного курса и обсуждения вопросов на практических занятиях каждый студент самостоятельно выполняет индивидуальное задание, к которому следует тщательно подготовиться. Положительный результат будет получен, если студент систематически посещает лекции, активно участвует в работе на семинарских занятиях, самостоятельно работает по программе курса. Успешное выполнение письменной работы во многом зависит от правильной организации ее подготовки и написания, а также соблюдения основных требований, которые к ней предъявляются.

Методические рекомендации к выполнению контрольной работы

Требования к структуре и содержанию работы

Работа должна содержать следующие структурные элементы:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения.

Общий объем работы без приложений должен составлять 10-15 страниц.

Требования к оформлению

Контрольная работа должна быть оформлена в соответствии с ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления».

Список литературы оформляется в соответствии с требованиями ГОСТ Р 7.0.5—2008 «Библиографическая ссылка».

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

лицензионное отечественное:

1. Антивирусная защита Kaspersky Endpoint Security.
2. Astra Linux.
3. LibreOffice.

лицензионное импортное:

ПО для ТСО лиц с ограниченными возможностями здоровья.

свободно распространяемое:

Архиватор KDE (Ark).

11.2. Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Информационно-образовательные ресурсы личных кабинетов обучающихся платформы Финансового университета - <https://org.fa.ru/>.

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не используются.

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

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

Специализированная мебель:

Парты студенческие двухместные – 32 шт.

Парты студенческие трехместные – 16 шт.

Стол преподавателя – 1 шт.

Стул для преподавателя – 3 шт.

Учебная доска меловая - 1 шт.

Кафедра переносная – 1 шт.

Технические средства обучения:

Компьютер – 1 шт.

Проектор – 1 шт.

Интерактивный экран с акустикой – 1 шт.

Помещение для самостоятельной работы.

Учебно-методический кабинет.

Специализированная мебель:

Стол (учительский) – 1 шт.

Стол студенческий двухместный – 15 шт.

Столы для автоматизированных рабочих мест (одноместные) - 5 шт.

Стол для автоматизированного рабочего места преподавателя – 1 шт.

Стулья – 28 шт.

Стул для преподавателя – 1 шт.

Кресло офисное – 2 шт.

Тумба – 1 шт.

Тумба библиотечная – 1 шт.

Шкаф книжный открытый – 3 шт.

Книжный стеллаж – 22 шт.

Шкаф – пенал – 2 шт.

Стеллаж выставочный – 1 шт.

Шкаф – витрина – 3 шт.

Шкаф для документов закрытый – 2 шт.

Шкаф книжный застекленный – 2 шт.

Шкаф картотечный – 1 шт.

Технические средства обучения:

Компьютер – 2 шт.

Моноблок - 6 шт.

Проектор – 1 шт.

Экран моторизированный – 1 шт.

Колонки - 1 шт.

Принтер для печати рельефно-точечным шрифтом Брайля VP EmBraille - 1 шт.

Дисплей Брайля - 1 шт.

Видеоувеличитель - 1 шт.

Принтер - 1 шт.

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