

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

(Финуниверситет)

Тульский филиал Финуниверситета

Кафедра «Экономика и менеджмент»

СОГЛАСОВАНО

Правительство Тульской области
Комитет Тульской области по тарифам



УТВЕРЖДАЮ



Т.В. Медведева

**ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И
МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ**

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
38.03.04 Государственное и муниципальное управление
ОП «Государственное и муниципальное управление»
Профиль «Государственное и муниципальное управление»

*Рекомендовано Ученым советом Тульского филиала Финуниверситета
(протокол от 13 июня 2023 г. № 02)*

*Одобрено заседанием кафедры «Экономика и менеджмент»
(протокол от 06 июня 2023 г. № 13)*

Тула 2023

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	5
4. Объём дисциплины в зачётных единицах и в академических часах с выделением объёма аудиторной (лекции, семинары) и самостоятельной работы обучающихся	5
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	5
5.1. Содержание дисциплины	5
5.2. Учебно-тематический план	6
5.3. Содержание семинаров, практических занятий	8
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	10
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	10
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	12
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	17
7.1. Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний	17
7.2. Иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний	22
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	22
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	23
10. Методические указания для обучающихся по освоению дисциплины	23
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	26
11.1. Комплект лицензионного программного обеспечения:	26
11.2. Современные профессиональные базы данных и информационные справочные системы	26
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	26

1. Наименование дисциплины

Защита информации в системе государственного и муниципального управления.

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

В результате изучения дисциплины у студентов должны быть сформированы следующие компетенции:

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-7	Способность применять информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления	1. Демонстрирует знания в сфере информационно-коммуникационных технологий, информационной безопасности и защиты информации, основных положений законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления.	Знать правовой базис применения информационных технологий в государственном управлении, важнейшие источники знаний и лучшие мировые практики в сфере информационных технологий и государственных и муниципальных информационных систем. Уметь соотносить правовой базис применения информационных технологий в государственном управлении с практикой, работать с важнейшими источниками знаний, применять лучшие мировые практики в сфере информационных технологий и государственных и муниципальных информационных систем
		2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности	Знать основные методы выявления основных проблем в практическом применении ИКТ в государственном и муниципальном управлении. Уметь выявлять основные

		соответствующих органов власти и организаций.	проблемы в практическом применении ИКТ в государственном и муниципальном управлении.
		3. Применяет информационно-коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления.	Знать: существующие модели информационной безопасности в информационных системах, используемых для управления регионом.. Уметь: обосновывать решения задач в области информационной безопасности региона.
ПКП-4	Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований	1. Демонстрирует знание методов инструментов для управления развитием субъектов Российской Федерации и муниципальных образований.	Знать основные принципы и средства обработки информации из различных источников, в том числе в глобальных компьютерных сетях. Уметь использовать современные технологии обеспечения информационной безопасности.
		2. Владеет навыками подготовки решений и мероприятий с использованием современных методов инструментов для управления	Знать основы управления и особенности коммуникации при решении задач в области информационной безопасности. Уметь разрабатывать и обосновывать принципы организационно-управленческих решений в области информационно

		развитием субъектов Российской Федерации и муниципальных образований.	безопасности в профессиональной деятельности в сфере государственного и муниципального управления.
--	--	---	--

3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системе государственного и муниципального управления» входит в состав цикла профиля (элективного), профиль «Государственное и муниципальное управление» части дисциплин учебного плана, формируемой участниками образовательных отношений, направления подготовки 38.03.04 «Государственное и муниципальное управление».

4. Объём дисциплины в зачётных единицах и в академических часах с выделением объёма аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 1

Вид учебной работы	В зач. ед./часах	Семестры
		7
<i>Общая трудоемкость дисциплины</i>	5/180	180
<i>Контактная работа</i>	68	68
<i>Аудиторные занятия</i>		
Лекции	34	34
Семинары, практические занятия	34	34
<i>Самостоятельная работа</i>	112	112
Вид текущей аттестации	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

Раздел 1. Информационная безопасность 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.

Раздел 2. Информационные уязвимости объектов

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

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.

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.

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.

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

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. Развитие идей и концепций защиты информации в банках.

5.2. Учебно-тематический план

Таблица 2

№ п.п.	Наименование темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего часов	Контактная работа - Аудиторная работа			Самостояте льная работа	
			Общая	Лекции	Семинары,		

					практические занятия		
1.	Информационная безопасность в системе национальной безопасности	30	12	6	6	18	Доклады, презентации, обсуждение в группе, опрос.
2.	Информационные уязвимости объектов	30	12	6	6	18	Доклады, презентации, обсуждение в группе, опрос.
3	Угрозы информационной безопасности и их источники	30	12	6	6	18	Доклады, презентации, обсуждение в группе, опрос.
4	Средства обеспечения информационной безопасности	30	8	4	4	18	Доклады, презентации, обсуждение в группе, опрос.
5	Риски информационной безопасности и проблема построения комплексной системы защиты информации	30	12	6	6	18	Доклады, презентации, обсуждение в группе, опрос. Выполнение контрольной работы
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	30	12	6	6	18	Доклады, презентации, обсуждение в группе, опрос. Выполнение контрольной работы
	В целом по дисциплине	180	68	34	34	112	Согласно учебному плану: контрольная работа
	Итого в %	100	38	19	19	62	-

5.3. Содержание семинаров, практических занятий

Таблица 3

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
1.Понятийный аппарат и основы терминологии информационной и национальной безопасности. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности.	1. Основные подходы к определению понятия "информационная безопасность". 2. Подходы к классификации угроз безопасности информации. 3. Методы практического обеспечения защиты информации корпоративных систем. 4. Направления политики информационной безопасности предприятия. 5. Проблемы защиты информации в Интернет. Рекомендуемые источники: 8 [1-10], 9 [1-10].	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.
2.Организационно-правовые и комбинированные информационные уязвимости.	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. Рекомендуемые источники: 8 [1-10], 9 [1-10].	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Применение математического аппарата в профессиональной деятельности при выявлении сущности проблем, возникающих в задачах обеспечения информационной безопасности. Анализ конкретных правовых актов в области информационной безопасности.
3.Эндогенные и экзогенные, антропогенные и техногенные угрозы	Подходы к классификации угроз угрозы информации по степени защиты. Уязвимости электронного	Групповые дискуссии, мозговой штурм, презентация основных подходов.

информационной безопасности, их классификация.	документооборота. Основные принципы системной классификации угроз безопасности информации. Риски при идентификации и аутентификации пользователей. Риски утечки акустической информации. Риски утечки информации по техническим каналам. Рекомендуемые источники: 8 [1-10], 9 [1-10].	Учебное задание: Моделирование видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
4. Программно-аппаратные, криптографические и стеганографические средства защиты информации.	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 [1-10], 9 [1-10].	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование способов противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.
5. 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. Рекомендуемые источники: 8 [1-10], 9 [1-10].	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Разработка методики оценки информационных рисков, ее обсуждение и экспертная оценка.
6. Угрозы безопасности информации, обрабатываемой в компьютерных банковских системах.	1. Специфика рисков банковских угроз информационной безопасности. 2. Типы угроз банковской безопасности. 3. Наиболее уязвимые для банков каналы передачи информации.	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование возможных каналов

	4. Основные методы защиты от перехвата информации в банковских системах. 3.Перспективы использования блокчейна для защиты банковской информации. Рекомендуемые источники: 8 [1-10], 9 [1-10].	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
1.Понятийный аппарат и основы терминологии информационной и национальной безопасности. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности.	1. Основные проблемы информационной безопасности. 2. Смысл понятия «технический канал утечки информации». 3. Методы защиты от утечки информации по акустическому каналу. 4. Основные положения Доктрины информационной безопасности РФ. 5. Закон, определяющий техническое регулирование.	- работа с учебной, научной и справочной литературой; -подготовка презентаций по теме.
2.Организационно-правовые и комбинированные информационные уязвимости.	1. Защита информации в деловой переписке. 2. Особенности системы государственного управления Российской Федерации в области обеспечения информационной безопасности. 3. Основное содержание деятельности ФСТЭК и ФСБ России в области обеспечения информационной безопасности. 4. Особенности сертификации в области информационной безопасности РФ. 5. Функции и структура государственной системы обеспечения информационной безопасности.	- работа с учебной, научной и справочной литературой; -подготовка презентаций по теме.
3.Эндогенные и экзогенные, антропогенные и	1. Особенности защиты информации в вычислительных сетях. 2. Особенности лицензирования в	-работа с учебной, научной и справочной

техногенные угрозы информационной безопасности, их классификация.	области информационной безопасности РФ. 3. Специфика организации обучения и инструктирования сотрудников правилам работы с конфиденциальной информацией. 4. Техногенные угрозы информационной безопасности. 5. Угрозы информационной безопасности, связанные с человеческим фактором.	литературой; -подготовка презентаций по теме.
4. Программно-аппаратные, криптографические и стеганографические средства защиты информации.	1. Отличие криптографии от криптоанализа. 2. Законодательные акты, регулирующие электронную подпись. 3. Инфраструктура электронной подписи. 4. Основные способы аутентификации. 5. Методы криптографического закрытия информации. 6. Особенности отечественного стандарта шифрования.	-работа с учебной, научной и справочной литературой; -подготовка презентаций по теме.
5. Оценка рисков и организация управления процессом защиты информации.	1. Экономика предприятия и информационная безопасность. 2. Задачи службы безопасности организации. 3. Информационные риски организации. 4. Стратегии снижения рискозависимости предприятия в процессе управления. 5. Характер оценивая информационных рисков в процессе управления предприятием.	-работа с учебной, научной и справочной литературой; -подготовка презентаций по теме.
6. Угрозы безопасности информации, обрабатываемой в компьютерных банковских системах.	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 презентаций по теме.

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

Типовые задания контрольной работы

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 информационная безопасность
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 информационная безопасность
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 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.

Вопросы для подготовки к текущему контролю

1. Основные подходы к определению понятия "информационная безопасность".
2. Подходы к классификации угроз безопасности информации.
3. Методы практического обеспечения защиты информации корпоративных систем.
4. Направления политики информационной безопасности предприятия.
5. Проблемы защиты информации в Интернет.

6. Основные положения законодательных актов России по информационной безопасности.
7. Руководящие документы ФСТЭК России.
8. Основные подходы к аудиту информационной безопасности предприятия.
9. Государственные и международные стандарты в области информационной безопасности.
10. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности.
11. Принципы организации работ с информацией, составляющей коммерческую тайну.
12. Подходы к классификации угроз угрозы информации по степени защиты.
13. Уязвимости электронного документооборота.
14. Основные принципы системной классификации угроз безопасности информации.
15. Риски при идентификации и аутентификации пользователей.
16. Риски утечки акустической информации.
17. Риски утечки информации по техническим каналам.
18. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях.
19. Определение криптографии, ее методы и алгоритмы.
20. Определение стеганография, ее достоинства и недостатки.
21. Системы криптографической защиты информации в России.
22. Специфика программно-аппаратных, криптографических средств защиты информации банковских карт.
23. Основные подходы к оценке рисков атак на информационные системы.
24. Типы компьютерных вирусов и специфических для них рисков.
25. Модели оценки рисков.
26. Наиболее актуальные подходы к управлению процессом защиты информации.
27. Наиболее значимые нормативные документы, регулирующие процессы управления защитой информации.
28. Специфика рисков банковских угроз информационной безопасности.
29. Типы угроз банковской безопасности.
30. Наиболее уязвимые для банков каналы передачи информации.
31. Основные методы защиты от перехвата информации в банковских системах.
32. Перспективы использования блокчейна для защиты банковской информации.

Примеры тестовых заданий

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

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

2. 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.

3. Длина исходного ключа у алгоритма шифрования DES (бит)

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

4. 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.

5. 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.

Критерии балльной оценки различных форм текущего контроля успеваемости

Организация текущего контроля успеваемости обучающихся по итогам семестра (модуля), по программам бакалавриата и магистратуры в соответствии с учебными планами по направлениям подготовки высшего образования утверждена приказом ректора 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».

Таблица 5 - Виды работ обучающегося, формирующие текущий контроль по дисциплине

№ п/п	Вид учебной деятельности	Баллы	Максимум за семестр (модуль)
	Выполнение и защита контрольной работы	10	10
	Аудиторная контрольная/срезовая работа	5	10
	Тестирование/блиц опросы	0,2	10
	Посещение занятий, ведение конспекта лекции/семинара и работа с ним	0,1	4
	Активное участие в интерактивном процессе выполнения практических заданий на семинарском занятии	0,1	6
	Всего за семестр (модуль)		40

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

Состав компетенций, характеризующих перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы, представлен в разделе 2 РПД.

7.1. Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

компетенция	типовые задания
ПКН-7 Способность применять информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления	Индикатор 1. Демонстрирует знания в сфере информационно-коммуникационных технологий, информационной безопасности и защиты информации, основных положений законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления. Знать правовой базис применения информационных технологий в государственном управлении, важнейшие источники знаний и лучшие мировые практики в сфере информационных технологий и государственных и муниципальных информационных систем. Уметь соотносить правовой базис применения информационных технологий в государственном управлении с практикой, работать с важнейшими источниками знаний, применять лучшие мировые практики в сфере информационных технологий и государственных и муниципальных информационных систем. Задание 1. Выявить основные принципы управления при решении задач в области информационной безопасности. Задание 2. Проанализировать и выбрать наиболее эффективные для решения проблем информационной

	безопасности информационные ресурсы. Индикатор 2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций. Знать основные методы выявления основных проблем в практическом применении ИКТ в государственном и муниципальном управлении. Уметь выявлять основные проблемы в практическом применении ИКТ в государственном и муниципальном управлении. Задание 1. Определить риски и степень ответственности при решении задач информационной безопасности. Задание 2. Провести анализ возможных стратегий сбора информации для решения профессиональных задач информационной безопасности. Индикатор 3. Применяет информационно-коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления. Знать: существующие модели информационной безопасности в информационных система, используемых для управления регионом. Уметь: обосновывать решения задач в области информационной безопасности региона. Задание 1. Разработать алгоритм выбора и использования имеющихся новых социальных сетевых технологий для обеспечения информационной безопасности Задание 2. Разработать алгоритм и критерии отбора информации для решения профессиональных задач в глобальных компьютерных сетях.
ПКП-4 Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований	Индикатор 1. Демонстрирует знание методов инструменты для управления развитием субъектов Российской Федерации и муниципальных образований. Знать основные принципы и средства обработки информации из различных источников, в том числе в глобальных компьютерных сетях. Уметь использовать современные технологии обеспечения информационной безопасности. 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. Индикатор 2. Владеет навыками подготовки решений и мероприятий с использованием современных методов инструментов для управления развитием субъектов Российской Федерации и муниципальных образований. Знать основы управления и особенности коммуникации при решении задач в области информационной безопасности. Уметь разрабатывать и обосновывать принципы организационно-управленческих решений в области информационно безопасности в профессиональной деятельности в сфере государственного и муниципального управления. Задание 1. Провести анализ возможных стратегий при решении задач в области информационной безопасности. Задание 2. Разработать стратегию эффективного управления для решения задач обеспечения информационной безопасности. Задание 3. Разработать этапы реализации стратегии и определить сопутствующие риски при решении задач обеспечения информационной безопасности.
--	---

Перечень контрольных вопросов для экзамена

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.

Пример экзаменационного билета по дисциплине

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным? (10 баллов)
2. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности. (10 баллов)

Практикоориентированное задание

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. (40 баллов)

7.2. Иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Порядок проведения промежуточной аттестации и система оценивания результатов промежуточной аттестации по итогам семестра (модуля) по программам бакалавриата и магистратуры в соответствии с учебными планами по направлениям подготовки высшего образования утверждена приказом ректора Финуниверситета по основной деятельности № 0557/о от 23.03.2017.

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:

5. Основы защиты информации в системе государственного и муниципального управления (с практикумом) [Электронный ресурс]: учебник / С. Е. Прокофьев [и др.]. М.: КноРус, 2022. 215 с. <https://book.ru/book/943134> (дата обращения: 16.06.2023).

6. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]: учебник. М.: Юрайт, 2023. 309 с. <https://urait.ru/bcode/511998> (дата обращения: 16.06.2023).

7. Информационные технологии в государственном и муниципальном управлении [Электронный ресурс]: учебник / О.С. Волгин [и др.]. М.: КноРус, 2024. 287 с. <https://book.ru/book/950546> (дата обращения: 16.06.2023).

Дополнительная литература:

8. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум / под ред. Т. А. Поляковой, А. А. Стрельцова. М.: Юрайт, 2023. 325 с. <https://urait.ru/bcode/511239> (дата обращения: 16.06.2023).

9. Баранова Е. К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие. 4-е изд., перераб. и доп. М.: РИОР; ИНФРА-М, 2022. 336 с. <https://znanium.com/catalog/product/1861657> (дата обращения: 16.06.2023).

10. Панарина М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании [Электронный ресурс]: учебное пособие. М.: Юрайт, 2023. 158 с. <https://urait.ru/bcode/520423> (дата обращения: 16.06.2023).

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. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
7. Национальная электронная библиотека <http://нэб.пф/>
8. «Государственные стандарты» <http://meganorm.ru/list/14-0.htm>
9. «Академия информационной безопасности» <http://www.iwars.ru/>
10. «Информационная безопасность» <http://www.itsec.ru/main.php/>

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов проходит аудиторно и внеаудиторно. Организации самостоятельной работы служит учебно-тематический план изучения дисциплины а также тексты лекций и семинарских занятий вместе с набором дополнительных задач, решение которых фиксируется по окончанию семинаров.

При подготовке к лекции целесообразно предварительно познакомиться с ее содержанием по и выделить наиболее трудные вопросы. Во время лекций следует конспектировать содержание лекции. После занятий следует провести работу с конспектом: отредактировать записи, оформить конспект. При оформлении целесообразно выделять специальным образом названия тем и формулировки вопросов, основные определения, формулировки теорем и примеры. Сделанные записи нужно сверить с учебниками и учебными пособиями и в случае расхождений проконсультироваться с преподавателем.

При подготовке к практическому занятию необходимо повторить или, если это требуется, изучить соответствующий теоретический материал. Во время занятия нужно точно записывать формулировки решаемых задач, вопросы, указания преподавателя к решению и разбираемые решения. После занятий необходимо просмотреть записанные решения и восстановить в решениях имеющиеся пробелы. В случае затруднений отметить соответствующие задания и обратиться за консультацией к преподавателю. Практические занятия проходят, как правило, в интерактивной форме и преподаватель учитывает активность студентов, направленную на решение предложенных задач, и в поиске ответов на вопросы. Не следует бояться дать неверный ответ или допустить иную ошибку: исправление и анализ ошибок в режиме общения с преподавателем и сокурсниками в ходе практического занятия способствуют освоению учебного материала и предупреждают появление ошибок в дальнейшем.

Домашние задания следует выполнять регулярно при подготовке к практическим занятиям. В большинстве своем задания являются типовыми, и образцы их решения содержатся в рекомендованных пособиях, в материале

лекций и практических занятий. Если то или иное задание вызвало затруднение, необходимо обратиться к преподавателю на консультации или ближайшем практическом занятии. Регулярность в выполнении домашних заданий — важный фактор освоения дисциплины. Даже небольшие отклонения от графика могут спровоцировать серьезное отставание и в дальнейшем — риск получения неудовлетворительных оценок в ходе текущей и промежуточной аттестации. Для выполнения домашних заданий следует завести отдельную тетрадь. Контроль за выполнением домашних заданий осуществляется в ходе практических занятий и выборочного собеседования.

Контрольные работы (КР) являются одной из основных форм текущего контроля самостоятельной работы студентов по данной дисциплине. Каждый вариант КР содержит 4-5 заданий, выполняя которые студент должен продемонстрировать умение решать типовые задачи и проводить типовые расчеты, а также применять математические знания к решению экономических задач.

Сроки выполнения КР указываются в учебно-тематическом плане изучения дисциплины. Конкретные сроки сдачи КР устанавливаются преподавателем. Оценка за КР выставляется по итогам проверки письменного отчета и устного собеседования по работе. Эта оценка является существенной компонентой оценки самостоятельной работы студента в течение семестра.

Если студент испытывает затруднения при выполнении КР, то он может получить консультацию у своего преподавателя в регулярно отводимое для этого время.

Контрольная работа должна содержать краткое изложение теоретических положений, связанные с выполняемым студентом заданием, самостоятельные расчеты, выводы по полученным результатам. Расчеты, проводимые при выполнении конкретных индивидуальных заданий, должны быть достаточно подробными, сопровождаться указанием формул, последовательности расчетных процедур, что позволит преподавателю оценить адекватность применяемых студентом статистических методов обработки и анализа данных.

Расчетные процедуры должны выполняться с применением программы «Microsoft Excel». Результаты расчетов следует оформить в таблицах.

Заключительная часть контрольной работы (или каждого ее раздела в соответствии с индивидуальным заданием) должна содержать анализ и интерпретацию полученных результатов расчета показателей.

Каждая статистическая таблица должна иметь общее заглавие, единицы измерения отражаемых показателей, период времени, к которому относятся данные. Графики и рисунки также должны быть подписаны. Если в работе имеется несколько таблиц или графиков, то они должны быть последовательно пронумерованы (например, таблица 1, рис. 2 и т.д.).

Собственные расчеты студентов приводятся полностью. Все формулы

должны быть приведены отдельными строками, с обязательной расшифровкой обозначений, использованных в них. Графики, диаграммы, рисунки и др. наглядные изображения должны быть выполнены на компьютере.

Выполненная контрольная работа оценивается преподавателем по следующим критериям: степень самостоятельности при выполнении работы, соответствие заданию (полнота выполнения задания), структура и логика изложения материала, аргументация сделанных выводов, корректность использования методов обработки статистической информации, привлечение отечественных и зарубежных источников информации (если это предусмотрено заданием), соблюдение требований к оформлению работы, сроки выполнения и сдачи работы. После проверки работы преподавателем проводится собеседование.

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

11.1. Комплект лицензионного программного обеспечения:

1. Антивирус Kaspersky Internet Security.
2. Windows, Microsoft Office.

11.2. Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Информационно-образовательный портал Финансового университета. - <http://portal.ufrf.ru>.

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не используются.

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

Для осуществления образовательного процесса в рамках дисциплины необходимо наличие специальных помещений.

Специальные помещения представляют собой учебные аудитории для проведения лекций, семинарских и практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также

помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Проведение лекций и семинаров в рамках дисциплины осуществляется в помещениях:

- оснащенных демонстрационным оборудованием;
- оснащенных компьютерной техникой, обеспечивающей доступ к сети «Интернет» и к электронной информационно - образовательной среде Финансового университета.