

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

Тульский филиал Финуниверситета

Кафедра «Математика и информатика»

СОГЛАСОВАНО

ЗАО «Андеррайтинг»

Генеральный директор

Д.В. Аристов

30 апреля 2024 г.



УТВЕРЖДАЮ

Директор филиала

Г.В. Кузнецов

30 апреля 2024 г.



М.В. Васина

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

Рабочая программа дисциплины

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

Образовательная программа «Цифровое государство и экономика»,

Профиль «Цифровое государство и экономика»

Рекомендовано Ученым советом Тульского филиала Финуниверситета
(протокол от 23 апреля 2024 г. № 14)

Одобрено кафедрой «Математика и информатика»
(протокол от 5 марта 2024 г. № 8)

Тула 2024

СОДЕРЖАНИЕ

1. Наименование дисциплины.....	3
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	3
3. Место дисциплины в структуре основной образовательной программы.....	4
4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема 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	5
5.3 Содержание семинаров, практических занятий	6
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	7
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	7
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	8
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	9
7.1. Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний	10
7.2. Иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний	13
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	13
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	15
10. Методические указания для обучающихся по освоению дисциплины	15
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	16
11.1. Комплект лицензионного программного обеспечения	16
11.2. Современные профессиональные базы данных и информационные справочные системы	16
11.3. Сертифицированные программные и аппаратные средства защиты информации	16
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	16

1. Наименование дисциплины

Защита информации в системе государственного и муниципального управления.

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

Дисциплина «Защита информации в системе государственного и муниципального управления» обеспечивает формирование следующих компетенций:

Таблица 1

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: понятие информационной безопасности и защиты информации и их значение в деятельности организаций. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.
		2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций	Знать: способы сбора и обработки информации в органах власти. Уметь: осуществлять сбор, обработку информации и участвовать в информатизации деятельности соответствующих органов власти и организаций
		3. Применяет информационно-коммуникационные технологии, инструменты и методы	Знать: основные положения законодательства о персональных данных, об общих принципах

		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	функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления. Уметь: применять информационно-коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации.
ПКП-2	Способность выбирать и применять информационно-коммуникационные технологии в разных сферах государственного и муниципального управления, на основе сформированной цифровой культуры государственных гражданских служащих	1. Использует информационно-коммуникационные технологии в разных сферах государственного и муниципального управления.	Знать: основные стандарты, регламентирующие управление информационной безопасностью и защитой информации. Уметь: определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью и защитой информации.
		2. Решает профессиональные задачи в области цифровой трансформации государственного управления на основе сформированной цифровой культуры государственных гражданских служащих.	Знать: основные направления и тенденции развития системы государственного и муниципального управления сточки зрения информационной безопасности и защиты информации; Уметь: определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью и защитой информации.

3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Защита информации в системе государственного и муниципального управления» относится к дисциплинам профиля.

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

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/ед. и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	6 зач.ед. / 216 ч.	216
Контактная работа - Аудиторные занятия	68	68
<i>Лекции</i>	34	34
<i>Семинары, практические занятия</i>	34	34
Самостоятельная работа	148	148
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	экзамен	экзамен

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

5.1. Содержание дисциплины

Тема 1. Теоретические основы защиты информации в системе государственного и муниципального управления.

Нормативное правовое регулирование системы защиты информации в системе государственного и муниципального управления.

Тема 2. Виды защищаемой информации.

Виды защищаемой информации, формируемой в процессе функционирования органов государственной и муниципальной власти.

Тема 3. Реализация системы защиты информации.

Порядок допуска к защищаемой информации в системе государственного и муниципального управления. Режимы использования отдельных видов информационных ресурсов в государственных и муниципальных органах власти. Организация конфиденциального делопроизводства в государственных и муниципальных органах власти. Соотношение принципа открытости государственной службы и объемов и видов информации, ограниченной в обороте.

Тема 4. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Внутренние нормативные документы по защите информации. Контроль и надзор за обеспечением защиты информационных ресурсов в государственных и муниципальных органах власти.

5.2. Учебно-тематический план

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа – Аудиторная работа			Самост оательн ая работа	
			Обща я	Лекции	Семинары, практическ ие занятия		
1	Теоретические основы защиты информации в системе государственного и муниципального управления	52	16	8	8	36	Доклады, презентации, дискуссии
2	Виды защищаемой информации	54	16	8	8	38	Доклады, презентации, дискуссии
3	Реализация системы защиты информации	52	16	8	8	36	Доклады, презентации, дискуссии
4	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации	58	20	10	10	38	Доклады, презентации, дискуссии
	В целом по дисциплине	216	68	34	34	148	Согласно учебному плану: контрольная работа
Итого:		216	68	34	34	148	

5.3 Содержание семинаров, практических занятий

Таблица 4

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
Теоретические основы защиты информации в системе государственного и муниципального управления	1. Понятие информации и информационной безопасности. 2. Информация, сообщения, информационные процессы как объекты информационной безопасности. 3. Обзор защищаемых объектов и систем. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов.
Виды защищаемой информации	1.Целостность, доступность и конфиденциальность информации. 2.Классификация информации по видам тайны и степеням конфиденциальности. 3.Понятия государственной тайны и конфиденциальной информации.	Групповые дискуссии, презентация основных подходов

	4.Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Рекомендуемые источники: 8, 1-2	
Реализация системы защиты информации	1.Понятие угрозы безопасности информации. 2.Системная классификация угроз безопасности информации. 3. Каналы и методы несанкционированного доступа к информации. 4.Анализ существующих методик определения требований к защите информации 5.Виды мер и основные принципы защиты информации. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов
Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению защитой информации. Рекомендуемые источники: 8, 1-2	Групповые дискуссии, презентация основных подходов

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 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Теоретические основы защиты информации в системе государственного и муниципального управления	1. Понятие информации и информационной безопасности. 2. Информация, сообщения, информационные процессы как объекты информационной безопасности. 3. Обзор защищаемых объектов и систем.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Виды защищаемой информации	1.Целостность, доступность и конфиденциальность информации. 2.Классификация информации по видам тайны и степеням конфиденциальности. 3.Понятия государственной тайны и конфиденциальной информации. 4.Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Реализация системы	1.Понятие угрозы безопасности информации.	Работа с учебной

защиты информации	2. Системная классификация угроз безопасности информации. 3. Каналы и методы несанкционированного доступа к информации. 4. Анализ существующих методик определения требований к защите информации 5. Виды мер и основные принципы защиты информации.	литературой. Подготовка сообщений по теме; подготовка презентаций по теме.
Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению защитой информации.	Работа с учебной литературой. Подготовка сообщений по теме; подготовка презентаций по теме.

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

Текущий контроль осуществляется в ходе учебного процесса и контроля самостоятельной работы студентов, в том числе по результатам выполнения контрольной работы. Основными формами текущего контроля знаний являются:

- обсуждение вопросов и задач, вынесенных в планах практических занятий в качестве самостоятельных заданий;
- обсуждение подготовленных презентаций;
- выполнение контрольной работы и обсуждение результатов.

Примерный перечень вопросов для дискуссий

1. Понятие «угроза информации».
2. Понятие «риска информационной безопасности».
3. Сущность функционирования системы защиты информации.
4. Защита человека от опасной информации и от неинформированности в области информационной безопасности.

Примерный перечень тем докладов с презентациями

1. Цели и задачи защиты информации.
2. Основные понятия в области защиты информации.
3. Элементы процесса менеджмента ИБ.
4. Модель интеграции информационной безопасности в основную деятельность организации.
5. Понятие Политики безопасности.
6. Уязвимости. Методы оценки уязвимости информации.
7. Определение угроз объекта информатизации и их классификация.

Примерные задания контрольной работы:

1. Виды информации, подлежащей защите в РФ.

2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений государственных и муниципальных органов власти.
5. Система сертификации РФ в области защиты информации.
6. Основные правила и документы системы сертификации РФ в области защиты информации.
7. Методика оценки модели угроз и ее применение.
8. Ключевые субъекты НПС.
9. Организационно-распорядительная защита информации.
10. Работа с кадрами и внутриобъектовый режим.
11. Принципы построения организационно-распорядительной системы.

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 по основной деятельности 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 6 - Виды работ обучающегося, формирующие текущий контроль по дисциплине

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

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».

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

Таблица 7

Компетенции	Типовые задания
ПKN-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: понятие информационной безопасности и защиты информации и их значение в деятельности организаций. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации. Задание. Охарактеризуйте понятия информационной безопасности и защиты информации. Индикатор 2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций Знать: способы сбора и обработки информации в органах власти. Уметь: осуществлять сбор, обработку информации и участвовать в информатизации деятельности соответствующих органов власти и организаций. Задание. Какие нормативные документы в сфере информационной безопасности действуют в Российской Федерации? Какие из них напрямую регламентируют работу органов государственной и муниципальной власти? 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: основные положения законодательства о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления. Уметь: применять информационно-коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации. Задание. Перечислите требования к защите информации, предъявляемые для государственных служащих.
ПКП-2 Способность выбирать и	Индикатор 1. Использует информационно-коммуникационные технологии в разных сферах государственного и

применять информационно-коммуникационные технологии в разных сферах государственного и муниципального управления, на основе сформированной цифровой культуры государственных гражданских служащих	муниципального управления Знать: основные стандарты, регламентирующие управление информационной безопасностью и защитой информации. Уметь: определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью и защитой информации. Задание 1. Составить план контроля соблюдения требований информационной безопасности на рабочем месте. Индикатор 2. Решает профессиональные задачи в области цифровой трансформации государственного управления на основе сформированной цифровой культуры государственных гражданских служащих Знать: основные направления и тенденции развития системы государственного и муниципального управления точки зрения информационной безопасности и защиты информации; Уметь: определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью и защитой информации. Задание 1. Составить план проведения тренировок по повышению соблюдения требований информационной безопасности.
--	--

Примерный перечень вопросов для подготовки к экзамену

1. Какие действия и процессы составляют стадию проверки СУИБ?
2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?
3. Что такое информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии, киберустойчивость?
4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?
5. На какие категории подразделяются персональные данные?
6. Что такое государственная тайна?
7. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?
8. Что такое идентификация и аутентификация?
9. В чем заключается процессный подход к управлению ИБ?
10. Какие действия и процессы составляют стадию планирования СУИБ?
11. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?
12. Что такое циклическая модель PDCA применительно к управлению ИБ?
13. Что включает выбор и применение организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?
14. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование компенсующих мер ЗИ? Какие условия при этом должны быть выполнены?

15. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р 57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ организации для конкретного контура безопасности?

16. Укажите стадии жизненного цикла автоматизированных систем. Чем обусловлены особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

17. Назовите основные нормативно правовые документы в области управления информационной безопасности.

18. Какие вопросы защиты информации в государственной сфере регулирует ФСБ?

19. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?

20. Укажите типы факторов аутентификации.

21. Опишите основные угрозы аутентификации.

22. Укажите плюсы и минусы парольной аутентификации.

Примеры практико-ориентированных заданий

Задача 1. Составьте модель угроз нарушения информационной безопасности для автоматизированной системы муниципального органа власти.

Задача 2. Составьте проект классификатора инцидентов ИБ.

Задача 3. Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1.

Задача 4. В ходе проведенной службой информационной безопасности банка проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

Задача 5. В корпоративной сети организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.

Задача 6. Составьте развернутый план частной политики менеджмента инцидентов ИБ.

Пример экзаменационного билета

Федеральное государственное образовательное бюджетное учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Кафедра «Математика и информатика»

Дисциплина «Защита информации в системе государственного и муниципального управления»

Филиал Тульский

Семестр: 7 Направление: Государственное и муниципальное управление.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Какие вопросы защиты информации в государственной сфере регулирует ФСТЭК? (10 баллов)
2. Укажите типы факторов аутентификации. (10 баллов)
3. В ходе проведенной службой информационной безопасности проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ. (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. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (В редакции от 02.07.2021 г.).
2. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне» (В редакции от 11.06.2021 г.)
3. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (В редакции от 09.03.2021 г.).
4. Распоряжение Правительства России от 28 июля 2017 г. №1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации»
5. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
6. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
8. ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
9. ГОСТ Р 50922 Защита информации. Основные термины и определения.
10. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

11. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

12. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

13. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

14. ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

15. ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

16. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

17. ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

18. ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

19. ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум / под ред. Т. А. Поляковой, А. А. Стрельцова. М.: Юрайт, 2024. 325 с. <https://urait.ru/bcode/536225> (дата обращения: 19.03.2024).

2. 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: 19.03.2024).

3. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]: учебник. М.: Юрайт, 2024. 309 с. <https://urait.ru/bcode/537000> (дата обращения: 19.03.2024).

Дополнительная литература

4. 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, 2024. 336 с. <https://znanium.ru/catalog/product/2082642> (дата обращения: 19.03.2024).

5. Морозова О. А., Лосева В. В., Иванова Л. И. Информационные технологии в государственном и муниципальном управлении [Электронный

ресурс]: учебное пособие. 3-е изд., перераб. и доп. М.: Юрайт, 2024. 156 с. <https://urait.ru/bcode/535359> (дата обращения: 19.03.2024).

6. Суворова Г. М. Информационная безопасность [Электронный ресурс]: учебное пособие. 2-е изд., перераб. и доп. М.: Юрайт, 2024. 277 с. <https://urait.ru/bcode/544029> (дата обращения: 19.03.2024).

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.znaniyum.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. Информационный портал www.cnews.ru [Электронный ресурс], режим доступа: www.cnews.ru

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студента в процессе освоения дисциплины включает в себя:

- подготовку к семинарским занятиям;
- изучение основной и дополнительной литературы по дисциплине;
- выполнение контрольной работы;
- индивидуальные или групповые консультации по наиболее сложным вопросам;
- подготовку к экзамену.

Требования к оформлению контрольной работы

Контрольная работа является одной из форм самостоятельной работы студентов. Целью выполнения контрольной работы является подготовка студента к творческой деятельности научного или практического характера и формирование навыков представления полученных результатов.

Контрольная работа может выполняться как индивидуально, так и в составе группы.

Контрольная работа должна включать:

- описание цели и задач работы;
- круг рассматриваемых проблем и методы их решения;
- статистические данные с указанием источника информации;

- результаты анализа статистических данных и их интерпретация;
- общие выводы.

Оформление контрольных работ и домашнего творческого задания

Контрольные работы и домашнее творческое задание выполняются на листах А4. Оформляется титульный лист, выполненная работа с титульным листом в назначенный день сдается на проверку преподавателю.

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-образовательный портал Финансового университета. - <http://www.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

Образовательный процесс по учебной дисциплине осуществляется в учебных аудиториях для проведения учебных занятий. При освоении дисциплины используются технические средства мультимедийной техники аудиторий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения в сети «Интернет» и

обеспечением доступа в электронно-образовательную среду Финансового университета.