

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

Уральский филиал Финуниверситета

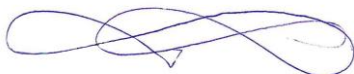
Кафедра «Экономика, финансы и управление»

СОГЛАСОВАНО

УТВЕРЖДАЮ

Начальник Главного контрольного
управления Челябинской области

Директор Уральского филиала
Финуниверситета



Д.В. Агеев



Д.А. Циринг

«22» февраля 2023 г.

«22» февраля 2023 г.

Каткова С.Г.

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

Рабочая программа дисциплины

Для студентов, обучающихся по направлению
38.03.04 «Государственное и муниципальное управление»
профиль «Государственное и муниципальное управление»

*Рекомендовано Ученым советом
Уральского филиала Финуниверситета
(Протокол № 50 от «21» февраля 2023 г.)*

*Одобрено кафедрой «Экономика, финансы и управление»
(Протокол № 06 от «14» февраля 2023 г.)*

Челябинск, 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	4
4. Объем дисциплины(модуля) 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
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	9
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	13
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	16
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	18
10. Методические указания для обучающихся по освоению дисциплины	19
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	19
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	19

1. Наименование дисциплины

Дисциплина «Защита информации в системе государственного и муниципального управления» Б.1.2.2.1.7. направления подготовки бакалавров 38.03.04 «Государственное и муниципальное управление».

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

В результате изучения дисциплины студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПКН-7	Способность применять информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах акционирования 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	Знание: информационно-коммуникационных технологий, основных положений законодательства о персональных данных, об общих принципах акционирования системы электронного правительства; Умение: оперативно применять на практике информационно-коммуникационные технологии, информационной безопасности и защиты информации, основных положений законодательства
		2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций.	Знание: принципов и методов сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций; Умение: демонстрировать и владеть навыками сбора, обработки информации и в информатизации деятельности соответствующих органов власти и организаций

		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 государственных органов власти и управления	Знание: информационно коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства; Умение: применяет информационно коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства
ПКП-4	Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований	1 Способность проводить анализ и оценку промежуточных и итоговых результатов проектов и программ в органах государственного управления	Знание: общенаучных методов и математического аппарата при создании комплексных систем информационной безопасности органов государственного и муниципального управления; Умение: демонстрировать знания методов математического моделирования при создании комплексных систем информационной безопасности органов государственного и муниципального управления
		2. Владеть структурированными знаниями по всем областям проектной деятельности в органах власти	Знание: методологии в области инструментов качественного и количественного анализа при оценке результатов работы органов государственного и муниципального управления Умение: демонстрирует навыки выявления рисков нарушения информационной безопасности в органах государственного и муниципального управления, способность принятия оперативных решений по их устранению;

3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системе государственного и муниципального управления» является обязательной дисциплиной по направлению подготовки 38.03.04 «Государственное и муниципальное управление».

Изучению дисциплины "Защита информации в системе государственного и муниципального управления" предшествует освоение следующих дисциплин: «Система государственного и муниципального управления», «Анализ данных», «Правовая система Российской Федерации», «Информационные технологии в профессиональной деятельности», «Стратегическое государственное управление».

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

Форма обучения: *очная*

Общая трудоемкость дисциплины составляет *7 зачетн. ед.*

Вид промежуточной аттестации – Экзамен.

- очная форма обучения

Вид учебной работы	Всего (в з/е и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	180	180
<i>Аудиторные занятия</i>	68	68
Лекции (Л)	34	34
Практические занятия (ПЗ)	34	34
<i>Самостоятельная работа</i>	112	112
<i>Вид текущей аттестации</i>	Контрольная работа	
Вид промежуточной аттестации	Экзамен	

-очно – заочная форма обучения

Вид учебной работы	Всего (в з/е и часах)	Семестр 7 (в часах)
Общая трудоемкость дисциплины	180	180
<i>Аудиторные занятия</i>	32	68
Лекции (Л)	12	34
Практические занятия (ПЗ)	20	34
<i>Самостоятельная работа</i>	148	112
<i>Вид текущей аттестации</i>	Контрольная работа	
Вид промежуточной аттестации	Экзамен	

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

5.1. Содержание дисциплины

Тема 1. Преступления в органах государственного и муниципального управления с применением высоких информационных технологий

Информационная сфера и информационная безопасность в в органах государственного и муниципального управления. Специфика защиты информационных систем в органах государственного и муниципального управления. Особенности и виды нарушений безопасности информационных систем. Типовой алгоритм удаленного несанкционированного доступа к автоматизированной системе. Вредоносные программы. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.

Тема 2. Мошенничество в сфере конфиденциального документооборота

Виды документопотоков. Основные свойства систем электронного документооборота. Общая классификация систем электронного документооборота. Каналы утечки информации ограниченного доступа. Условия и факторы, способствующие утечке информации ограниченного доступа. Организация и ведение секретного делопроизводства. Специфика защиты и обработки документов ограниченного доступа. Порядок работы со съемными носителями конфиденциальной информации. Систематизация документов ограниченного доступа. Условия, способствующие повышению эффективности защиты информации в сфере конфиденциального документооборота.

Тема 3. Противодействие инсайдерам в органах государственного и муниципального управления

Организационные методы защиты информации. Обеспечение безопасности компьютерных сетей. Обеспечение безопасности электронных платежей. Применение специализированных программ контроля действий персонала в органах государственного и муниципального управления. Отбор персонала в органах государственного и муниципального управления. Проверка персонала в органах государственного и муниципального управления.

Тема 4. Структура и функции подразделения по защите информации

Структура, задачи, функции и права службы защиты информации. Обеспечение внутри объектового и контрольно-пропускного режима на объекте. Обеспечение программно-аппаратной защиты информации.

Обеспечение инженернотехнической защиты информации. Организация конфиденциального делопроизводства. Обеспечение организационной и правовой защиты информации. Проведение служебных расследований по фактам утечки информации.

Тема 5. Защита информации в автоматизированных системах обработки данных

Основные понятия и положения защиты информации в автоматизированных системах. Современное состояние безопасности автоматизированных систем. Реализация политики безопасности в автоматизированных системах. Модель нарушителя безопасности автоматизированных систем. Методы и средства защиты данных от несанкционированного доступа. Защита информации в информационно - телекоммуникационных сетях. Технологии обеспечения сетевой безопасности автоматизированных систем.

5.2 Учебно-тематический план

- очная форма обучения

№ п/ п	Наименование темы (раздела) дисциплины	Трудоемкость в часах						Формы текущего контроля успеваемости
		Всего	Аудиторная работа				Самост оатель ная работа	
			Обща я, в т.ч.:	Лекци и	Семинар ы, практиче ские занятия	Занятия в интеракт ивных формах		
1.	Преступления в органах государственного и муниципального управления с применением высоких информационных технологий	18	4	2	2	2	14	Устный опрос, решение тестовых заданий по теме
2.	Мошенничество в сфере конфиденциального документооборота	20	6	2	4	4	14	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
3.	Противодействие инсайдерам в органах государственного и муниципального управления	22	8	4	4	6	14	Устный опрос, решение тестовых заданий по теме
4.	Структура и функции подразделения по защите информации	24	8	4	4	6	16	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
5.	Защита информации в автоматизированных системах обработки данных	24	8	4	4	6	16	Решение практико-ориентированных задач и их обсуждение, тестовых заданий

Итого	180	68	34	34	24/ 35%	112	
-------	-----	----	----	----	------------	-----	--

- очно - заочная форма обучения

№ п/ п	Наименование темы (раздела) дисциплины	Трудоемкость в часах						Формы текущего контроля успеваемости
		Всего	Аудиторная работа				Сам осто ятел ьная рабо та	
			Обща я, в т.ч.:	Лекци и	Семинар ы, практиче ские занятия	Занятия в интерактив ных формах		
1.	Преступления в органах государственного и муниципального управления с применением высоких информационных технологий	32	4	2	2	2	28	Устный опрос, решение тестовых заданий по теме
2.	Мошенничество в сфере конфиденциального документооборота	36	6	2	4	2	30	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
3.	Противодействие инсайдерам в органах государственного и муниципального управления	36	6	2	4	4	30	Устный опрос, решение тестовых заданий по теме
4.	Структура и функции подразделения по защите информации	36	6	2	4	4	30	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
5.	Защита информации в автоматизированных системах обработки данных	40	10	4	6	4	30	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
Итого		180	32	12	20	14/ 43%	148	

5.3 Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9	Формы проведения занятий
Преступления в органах государственного и муниципального управления с применением высоких информационных технологий	Особенности и виды нарушений безопасности информационных систем. Типовой алгоритм удаленного несанкционированного доступа к автоматизированной системе. Вредоносные программы. Общая характеристика технических средств несанкционированного получения информации и технологий их применения. <i>Рекомендуемые источники:</i> Раздел 8: 1, 3, 4. Раздел 9:	Устный опрос, решение тестовых заданий по теме

	2, 3.	
Мошенничество в сфере конфиденциального документооборота	Виды документопотоков. Основные свойства систем электронного документооборота. Каналы утечки информации ограниченного доступа. Организация и ведение секретного делопроизводства. Порядок работы со съемными носителями конфиденциальной информации. Систематизация документов ограниченного доступа <u>Рекомендуемые источники:</u> Раздел 8: 1, 2, 5. Раздел 9: 1, 3.	Решение практико-ориентированных задач и их обсуждение, тестовых заданий
Противодействие инсайдерам в органах государственного и муниципального управления	Знакомство со специализированной программой контроля действий персонала «Фотография рабочего времени». <u>Рекомендуемые источники:</u> Раздел 8: 1, 2, 5. Раздел 9: 1, 3.	Устный опрос, решение тестовых заданий по теме
Структура и функции подразделения по защите информации	Задачи службы защиты информации по обеспечению программно-аппаратной защиты информации. Обеспечению инженерно-технической защиты информации. Обеспечению организационной и правовой защиты информации <u>Рекомендуемые источники:</u> Раздел 8: 1, 2, 5. Раздел 9: 1, 3.	Устный опрос, решение тестовых заданий по теме
Защита информации в автоматизированных системах обработки данных	Реализация политики безопасности в автоматизированных системах. Модель нарушителя безопасности автоматизированных систем. Защита информации в информационно-телекоммуникационных сетях. Технологии обеспечения сетевой безопасности автоматизированных систем <u>Рекомендуемые источники:</u> Раздел 8: 1, 2, 5. Раздел 9: 1, 3.	Опрос, тестирование, обсуждение научных докладов

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

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

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное обучение	Форма внеаудиторной самостоятельной работы
Преступления в органах государственного и муниципального управления с применением высоких информационных технологий	Вредоносные программы. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.	Работа с учебной и справочной литературой. Изучение нормативных правовых актов. Работа со справочно-правовой системой. Поиск информации в Интернете по заданной

		теме. Подготовка доклада по выбранной теме. Подготовка к научной дискуссии
Мошенничество в сфере конфиденциального документооборота	Порядок работы со съемными носителями конфиденциальной информации. Систематизация документов ограниченного доступа.	Работа с учебной и справочной литературой. Изучение нормативных правовых актов. Работа со справочно-правовой системой. Поиск информации в Интернете по заданной теме. Подготовка доклада по выбранной теме. Подготовка к научной дискуссии. Решение практических ситуаций
Противодействие инсайдерам в органах государственного и муниципального управления	Отбор и проверка персонала учреждений.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Структура и функции подразделения по защите информации	Обеспечение программноаппаратной защиты информации.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Защита информации в автоматизированных системах обработки данных	Модель нарушителя безопасности автоматизированных систем	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме

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

Самостоятельная работа является неотъемлемой частью учебной деятельности студентов. Она выполняет важные функции: способствует усвоению знаний, формированию профессиональных умений и навыков, обеспечивает формирование профессиональной

компетенции;

формирует потребность в самообразовании, максимально развивает познавательные и творческие способности личности;

формирует навыки планирования и организации рабочего времени, расширяет кругозор.

Целью самостоятельной работы студентов является формирование у студентов способности к саморазвитию, творческому применению полученных знаний, формирование умения использовать нормативную, правовую документацию и специальную литературу.

Перечень вопросов к контрольной работе

1. Виды вредоносных программ.
2. Виды технических средств несанкционированного получения информации.
3. Классификация систем электронного документооборота.
4. Этапы организация и ведение секретного делопроизводства.
5. Порядок работы со съемными носителями конфиденциальной информации.
6. Методы обеспечения безопасности электронных платежей.
7. Виды проверок персонала государственных муниципальных учреждений.
8. Задачи службы защиты информации.
9. Порядок проведения служебных расследований по фактам утечки информации.
10. Классификация нарушителей безопасности автоматизированных систем.
11. Сравнительный анализ троянских программ и компьютерных вирусов.
12. Сравнительный анализ вирусов- шифровальщиков и логических бомб.
13. Разработка функциональной модели процесса защиты рабочей станции от вредоносного ПО
14. Разработка функциональной модели защиты сетевого сервера от вредоносного ПО.
15. Разработка функциональной модели защиты мобильного устройства от вредоносного ПО.
16. Построение схемы классификации вредоносного программного обеспечения.
17. Описание схемы жизненного цикла компьютерного вируса.
18. Процессинговые системы. Принцип работы, основные производители процессинговых систем.
19. Политика информационной безопасности в государственном муниципальном управлении. Основные положения.

20. Разграничение прав доступа к объектам информационной инфраструктуры.

Примерный перечень вопросов для дискуссий

1. Состояние безопасности информационных систем.
2. Последствия удаленного несанкционированного доступа к автоматизированной системе.
3. Преимущества и недостатки электронного документооборота.
4. Уязвимость электронных платежей.
5. Применение полиграфа для отбора и проверки персонала.
6. Какие задачи решает внутри объектовый и контрольно-пропускной режим на объекте.
7. Роль инженерно-технической защиты информации в структурах государственного муниципального управления.

Тематика докладов

1. Принципы организации деятельности контрольно-счетных органов субъектов Российской Федерации.
2. Этические нормы (требования), предъявляемые к сотруднику органов государственного (муниципального) финансового контроля.
3. Какие методы используются при проведении контрольных мероприятий?
4. В чем отличие деятельности органов внешнего и внутреннего контроля на федеральном уровне в Российской Федерации?
5. Сравните понятия «Защита информации в системе государственного и муниципального управления и государственный аудит.

Примеры ситуационных задач

1. В сети организации находится сервер под управлением операционной системы Linux. Какие способы защиты от воздействия вредоносного кода вы можете предложить.
2. Предположим Вы – руководитель отдела информационной безопасности финансовой организации и подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети. Опишите и оцените риски кибербезопасности.
3. Предложите методы проведения тестирования сотрудников организации на знания принципов политики информационной безопасности организации

Основные требования к результатам освоения дисциплины

Требования к результатам освоения дисциплины	Оценка	Баллы (рейтинговая оценка)
Глубокое усвоение всего материала в соответствии с рабочей программой дисциплины, логически стройное его изложение, умение	<i>отлично / зачтено</i>	<i>86-100</i>

применить теоретические знания для решения прикладных задач, свободное решение задач и обоснование принятого решения, выполнение текущей работы в семестре.		
Твердые знания всего материала в соответствии с рабочей программой дисциплины, грамотное его изложение, допустимы некоторые неточности в ответе на вопросы, правильное применение теоретических положений при решении практических вопросов и задач, выполнение текущей работы в семестре.	<i>хорошо / зачтено</i>	<i>70-85</i>
Знание только базового материала курса, допустимы неточности в ответе на вопросы, недостаточно правильные формулировки, нарушение логической последовательности в изложении теоретического материала, затруднения при решении практических задач, выполнение текущей работы в семестре.	<i>удовлетворительно / зачтено</i>	<i>50-69</i>
Незнание значительной части всего материала в соответствии с рабочей программой дисциплины, неумение сформулировать правильные ответы на вопросы экзаменационного билета, невыполнение практических заданий.	<i>неудовлетворительно / не зачтено</i>	<i>0-49</i>

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

7.1. Перечень компетенций, формируемых в процессе освоения дисциплины

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в разделе 2 «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения общеобразовательной программы».

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-4 способность использовать современные	1. Демонстрирует знания методов и инструментов для управления развитием субъектов	Знать: методы и инструменты защиты информационных ресурсов в рамках	Теоретические вопросы: 1. Признаки присутствия вредоносного ПО в

методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований	Российской Федерации и муниципальных образований.	управления развитием субъектов Российской Федерации и муниципальных образований. Уметь: применять методы и инструменты защиты информационных ресурсов в рамках управления развитием субъектов Российской Федерации и муниципальных образований.	автоматизированной системе. 2. Каналы проникновения вредоносного ПО.
	2. Владеет навыками подготовки решений и мероприятий с использованием современных методов и инструментов для управления развитием субъектов Российской Федерации и муниципальных образований	Знать: современные методы и инструменты управления развитием субъектов Российской Федерации и муниципальных образований. Уметь: разрабатывать решения и мероприятия, направленные на защиту информации в системе государственного и муниципального управления	Практико-ориентированное задание: На примере одного из субъектов Российской Федерации выделите общие и специфические проблемы организации межведомственного обмена информацией ограниченной в обороте
ПКН-7 Способность применять информационно-коммуникационные технологии, основные положения законодательства	1. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих	Знать: источники, методы сбора и обработки информации о деятельности органов государственного и муниципального	Практико-ориентированное задание: Подготовьте аналитическую записку, обосновывающую необходимость внедрения режима защиты служебной информации в

о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления	органов власти и организаций	управления Уметь: собирать и обрабатывать информатизацию о деятельности соответствующих органов власти и организаций	Департаменте здравоохранения города Москвы, осуществляющем разработку мер для профилактики и снижения рисков распространения инфекционных заболеваний, имеющих риски летального исхода более 30% от количества заболевших
	2. Владеет навыками сбора, обработки информации и участия в информатизации деятельности	Знать: источники, методы сбора и обработки информации о деятельности органов государственного и муниципального управления Уметь: собирать и обрабатывать информатизацию о деятельности соответствующих органов власти и организаций	Практико-ориентированное задание: Сформируйте полный перечень субъектов, обеспечивающих режим защиты государственной тайны в органе государственной власти федерального уровня на текущем этапе
	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 государственных органов власти и управления.	Знать: современные информационно – коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, актуальные положения Уметь: применять современные информационно – коммуникационные технологии, инструменты и информационной безопасности и защиты информации, актуальные	Практико-ориентированное задание: На основе изученного материала разработайте инструкцию по организации конфиденциального документооборота для ФГБУ, подчиненного Министерству промышленности и торговли Российской Федерации, и участвующего в реализации оборонзаказа для проведения специальной военной операции.

		положения при разработке и реализации управленческих решений	
--	--	--	--

Перечень вопросов к экзамену

1. Принципы и методы деструктивного воздействия вредоносного программного обеспечения на автоматизированные системы
2. Методы совершенствования защиты автоматизированных систем от вредоносного программного обеспечения.
3. Понятие и классификация вредоносного ПО.
4. Признаки вредоносного ПО
5. Понятие троянской программы, банковские трояны.
6. Понятие компьютерного вируса.
7. Понятие компьютерного червя.
8. Понятие вредоносной утилиты.
9. Жизненный цикл вредоносного ПО.
10. Цели и задачи разработки вредоносного ПО нарушителем информационной безопасности
11. Безопасность технологических процессов при атаке вредоносного ПО.
12. Использование вредоносного легитимного программного обеспечения для несанкционированного доступа с точки зрения злоумышленника.
13. Правила именования и поглощения вредоносного ПО.
14. Признаки присутствия вредоносного ПО в автоматизированной системе.
15. Каналы проникновения вредоносного ПО.
16. Атаки вирусов-шифровальщиков.
17. Сайты с вредоносным ПО и средства достижения анонимности.
18. Принципы создания эшелонированной централизованной системы антивирусной защиты автоматизированной системы.
19. Организационные меры защиты от вредоносного ПО.
20. Технические меры защиты от вредоносного ПО.
21. Процедуры, выполняемые в ходе обнаружения признаков вредоносного ПО.
22. Классы средств антивирусной защиты.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений и владений

Методические материалы для оценивания знаний, умений и владений закреплены в соответствующих приказах, распоряжениях ректората о контроле уровня освоения дисциплин и сформированности компетенций студентов.

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

Нормативно-правовые акты:

1. Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы. [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

2. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

3. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

4. Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью. [Электронный документ].

Режим доступа: URL: <http://www.27000.org/>.

5. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью. [Электронный документ].

Режим доступа: URL: <http://www.27000.org/>.

6. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

7. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

8. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

9. ГОСТ Р ИСО ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности.

10. ГОСТ Р 57580.1 – 2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Основная литература:

1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — URL: <https://urait.ru/bcode/469866>
2. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — URL: <https://urait.ru/bcode/470131>
3. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — URL: <https://urait.ru/bcode/477968>
4. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва: Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — URL: <https://urait.ru/bcode/467370>

Дополнительная литература:

5. Воронцова С.В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок) [Электронный ресурс]: монография /
6. С.В. Воронцова. — Москва: КноРус, 2017. — 160 с. — Режим доступа: <http://www.book.ru>
7. Малюк А.А. Введение в информационную безопасность [Электронный ресурс]: учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев;
8. Милославская Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс]: учебное пособие для вузов/ Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва:
9. Курило А.П. Вопросы управления информационной безопасностью [Электронный ресурс]: учебное пособие для вузов. Основы управления информационной безопасностью/ А.П. Курило, Н.Г Милославская, М.Ю. Сенаторов.

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

<i>Наименование ресурса</i>	<i>Электронный адрес</i>
ПРАВОВЫЕ БАЗЫ ДАННЫХ	
Кодекс. Информационно-правовая система	http://www.kodeks.net/
Парк.РУ Справочно-правовая система	http://www.park.ru/
ИНФОРМАЦИОННАЯ ПОДДЕРЖКА БИЗНЕСА И БАЗЫ ДАННЫХ	
Официальный сайт Министерства финансов Российской Федерации	www.minfin.ru
Официальный сайт Федеральной налоговой службы	www.nalog.ru
Официальный сайт Федеральной службы финансово-бюджетного надзора	www.rosfinnadzor.ru

<i>Наименование ресурса</i>	<i>Электронный адрес</i>
Официальный сайт Федерального казначейства	www.roskazna.ru
ЭКОНОМИЧЕСКИЕ ИЗДАНИЯ	
АКДИ “Экономика и жизнь”	http://www.akdi.ru/
Финансовое моделирование, бюджетирование, планирование	http://www.finmodeling.ru
ЛИТЕРАТУРА В INTERNET	
Библиотека «Полка букиниста»	http://polbu.ru/
Каталог ресурсов в помощь студенту	http://edu.uapa.ru/elibrary/
Книжная поисковая система eBdb	http://www.ebdb.ru/
Электронная библиотека экономической и деловой литературы	http://www.aup.ru/library/

10. Методические указания для обучающихся по освоению дисциплины

Обучение по дисциплине «Инновации и современные модели бизнеса» 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 практических занятий активно используются методы работы в малых группах, вовлечение в индивидуальную работу.

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) Антивирусная защита Kaspersky Endpoint Security;
- 2) Astra Linux Common Edition, Windows;
- 3) LibreOffice, Microsoft Office.

11.2. Современные профессиональные базы данных и информационные справочные системы

- 1) СПС Консультант Плюс (соглашение от 17.01.2003 г. № 24 с последующей пролонгацией)
- 2) Информационно-образовательный портал Финуниверситета и др.

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не используется.

12. Описание материально-технической базы, необходимой для

осуществления образовательного процесса по дисциплине

Филиал обеспечен учебными аудиториями для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенными оборудованием и техническими средствами обучения с Подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Финуниверситета.

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

Филиал обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- 1) Антивирусная защита Kaspersky Endpoint Security;
- 2) Astra Linux Common Edition, Windows;
- 3) LibreOffice, Microsoft Office.