

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

Уральский филиал Финуниверситета

Кафедра «Экономика, финансы и управление»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

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

Направление подготовки

38.03.04 «Государственное и муниципальное управление»
(код и наименование направления подготовки)

Государственное и муниципальное управление
(наименование направленности (профиля) образовательной программы)

Разработан в соответствии с рабочей программой «ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ», одобренной кафедрой «Экономика, финансы и управление» протокол № 06 от «30» января 2024 г., рекомендованной Ученым советом Уральского филиала Финуниверситета протокол № 10 от «20» февраля 2024 г.

1. Перечень компетенций, формируемых в процессе освоения дисциплины

Компетенция **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

Компетенция **ПКП-4**. Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований

2. Перечень компетенций, с указанием этапов их формирования в процессе освоения дисциплины

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-4 способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований	1. Демонстрирует знания методов и инструментов для управления развитием субъектов Российской Федерации и муниципальных образований.	Знать: методы и инструменты защиты информационных ресурсов в рамках 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.	Теоретические вопросы: 1. Признаки присутствия вредоносного ПО в 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 о персональных данных, об общих принципах функционирования системы электронного правительства для обеспечения деятельности государственных и муниципальных органов власти и управления	1. Владеет навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций	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: Подготовьте аналитическую записку, обосновывающую необходимость внедрения режима защиты служебной информации в 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	Знать: источники, методы сбора и обработки информации о деятельности органов	Практико-ориентированное задание: Сформируйте полный перечень субъектов, обеспечивающих режим

	деятельности	государственного и муниципального управления Уметь: собирать и обрабатывать информатизацию о деятельности соответствующих органов власти и организаций	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 положения при разработке и реализации управленческих решений	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.

3. Описание показателей и критериев оценивания компетенций, описание шкалы оценивания

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

Показатели оценивания	Критерии оценивания компетенций	Шкала оценивания
знать: информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах акционирования системы электронного правительства; уметь: демонстрировать знания и применять информационно коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства	знать: информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах акционирования системы электронного правительства;	Пороговый уровень от 50 баллов
	знать: информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах акционирования системы электронного правительства; уметь: демонстрировать знания информационно коммуникационных технологий, инструментов и методов информационной безопасности и защиты информации, основные положения законодательства;	Продвинутый уровень от 70 баллов
	знать: информационно-коммуникационные технологии, основные положения законодательства о персональных данных, об общих принципах акционирования системы электронного правительства; уметь: демонстрировать знания и применять информационно коммуникационные технологии, инструменты и методы информационной безопасности и защиты информации, основные положения законодательства;	Высокий уровень от 86 баллов

ПКП-4. Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований

Показатели оценивания	Критерии оценивания	Шкала оценивания
Знать: общенаучные методы и математического аппарата при создании комплексных систем информационной безопасности органов государственного и муниципального управления Уметь: демонстрировать знания методов математического моделирования при создании комплексных систем информационной безопасности органов государственного и муниципального управления, навыки выявления рисков нарушения информационной безопасности в органах государственного и муниципального управления,	Знать: общенаучные методы математического аппарата при создании комплексных систем информационной безопасности органов государственного и муниципального управления	Пороговый уровень от 50 баллов
	Знать: общенаучные методы математического аппарата при создании комплексных систем информационной безопасности органов государственного и муниципального управления Уметь: демонстрировать знания методов математического моделирования при создании комплексных систем информационной безопасности органов государственного и муниципального управления	Продвинутый уровень от 70 баллов
	Знать: общенаучные методы математического аппарата при создании	Высокий уровень от 86

способность принятия оперативных решений по их устранению.	комплексных систем информационной безопасности органов государственного и муниципального управления Уметь: демонстрировать знания методов математического моделирования при создании комплексных систем информационной безопасности органов государственного и муниципального управления, навыки выявления рисков нарушения информационной безопасности в органах государственного и муниципального управления, способность принятия оперативных решений по их устранению	баллов
--	---	---------------

4. Шкала оценки сформированных компетенций

Код компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	Пороговый	Продвинутый	Высокий
	Оценка		
	Удовлетворительно	Хорошо	Отлично
ПКН-7			
	Обсуждение вопросов по темам	Обсуждение вопросов по темам	Обсуждение вопросов по темам
			Решение задач. Тест
ПКП-4			
	Обсуждение вопросов по темам	Обсуждение вопросов по темам	Обсуждение вопросов по темам
			Решение задач. Тест

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных работ. Основными формами текущего контроля знаний являются:

- участие в дискуссиях по проблемным темам дисциплины;
- выполнение тестовых заданий и их обсуждение;
- выполнение контрольной работы.

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Оценка знаний студентов-бакалавров осуществляется в баллах с учетом:

- оценки за работу в семестре/модуле (участие в дискуссиях, написание контрольной работы и т.д.);
- оценки, полученной на зачете.

Оценка знаний по 100-балльной шкале реализуется в соответствии с критериями балльно-рейтинговой системы Финансового университета.

Требования к результатам освоения дисциплины	Оценка или	Баллы
--	------------	-------

	зачет	(рейтинговая оценка)
Глубокое усвоение программного материала (высокий уровень сформированности компетенций), логически стройное его изложение, умение связать теорию с практикой, свободное Решение задач. Тест и обоснование принятого решения, выполнение текущей работы в семестре.	Отлично/ Зачтено	86-100
Твердые знания программного материала (продвинутый уровень сформированности компетенций), грамотное и по существу его изложение, допустимы не существенные неточности в ответе на вопрос, правильное применение теоретических положений при решении практических вопросов и задач, выполнение текущей работы в семестре	Хорошо/ Зачтено	70-85
Знание только основного материала (пороговый уровень сформированности компетенций), допустимы неточности в ответе на вопрос, недостаточно правильные формулировки, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач, выполнение текущей работы в семестре.	Удовлет. / Зачтено	50-69
Незнание значительной части программного материала (не сформирован пороговый уровень компетенций), неумение даже с помощью преподавателя сформулировать правильные ответы на вопросы экзаменационного билета, невыполнение практических заданий.	Неудовлет. / Незачтено	менее 50

5. Типовые контрольные задания и иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (оценочные средства).

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 кредитно-финансовых 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.

Предложите методы проведения тестирования сотрудников организации на знания принципов политики информационной безопасности организации

Тематика контрольных работ

1. Раскройте значение государственного (муниципального) финансового контроля для обеспечения социально-экономического развития страны на современном этапе.
2. Классификация нарушений бюджетного законодательства: понятие, необходимость и значение для реализации превентивной функции государственного (муниципального) финансового контроля.
3. Результаты деятельности Союза контрольно-счетных органов в Российской Федерации.
4. Участники бюджетного процесса, наделенные контрольными полномочиями.
5. Взаимодействие контрольно-счетных органов с правоохранительными и другими контрольными органами.

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 «государственный финансовый контроль и государственный аудит».

Вопросы к экзамену по дисциплине «Защита информации в системе государственного муниципального управления»

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 вредоносное 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.

6. Примеры оценочных средств для проверки каждой компетенции

<u>Компетенция</u>	<u>Типовые задания</u>
<p>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</p>	<p>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</p> <p>Теоретические вопросы.</p> <ol style="list-style-type: none"> 1. Провести классификацию и краткий анализ каналов утечки информации ограниченного доступа. 2. Провести классификация систем электронного документооборота. <p>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</p> <p>Практико-ориентированные задание. 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</p>

<p>ПКП-4. Способность использовать современные методы и инструменты для управления развитием субъектов Российской Федерации и муниципальных образований</p>	<p>оцените риски кибербезопасности.</p> <p>Знание методологии в области инструментов качественного и количественного анализа при оценке результатов работы органов государственного и муниципального управления</p> <ol style="list-style-type: none"> 1. Выявить специфику защиты информационных систем учреждений государственного сектора. 2. Перечислить и охарактеризовать различные виды вредоносных программ. <p>Демонстрирует навыки выявления рисков нарушения информационной безопасности в органах государственного и муниципального управления, способность принятия оперативных решений по их устранению</p> <p>Практико-ориентированные задание.</p> <p>В сети государственного учреждения находится сервер под управлением операционной системы Linux. Какие способы защиты от воздействия вредоносного кода вы можете предложить</p>
---	---