Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Арзамасский филиал ННГУ - Факультет естественных и математических наук

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 10 от 02.12.2024 г.

Рабочая программа дисциплины

Современные методы обеспечения информационной безопасности в информационных системах

Уровень высшего образования
Магистратура

Направление подготовки / специальность
09.04.03 - Прикладная информатика

Направленность образовательной программы
Разработка и управление проектами в области информационных технологий

Форма обучения
очная, заочная, очно-заочная

г. Арзамас

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.10 Современные методы обеспечения информационной безопасности в информационных системах относится к части, формируемой участниками образовательных отношений образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
ПК-5: Способен планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС)	*ПК-5.1: Демонстрирует знание основных этапов жизненного цикла ИС (ИИС).* *ПК-5.2: Демонстрирует умение планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС).* *ПК-5.3: Имеет практический опыт планирования и организации аналитической деятельности.*	*ПК-5.1:* *Знать об основных этапах жизненного цикла ИС (ИИС) в предметной области, в рамках коммуникативной деятельности.* *Уметь использовать знания об основных этапах жизненного цикла ИС (ИИС).* *Владеть навыками использования знаний об основных этапах жизненного цикла ИС (ИИС).* *ПК-5.2:* *Знать основы планирования и организации аналитической деятельности на всех этапах жизненного цикла ИС (ИИС)* *Уметь планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС) с учетом области коммуникации и взаимодействия с клиентами* *Владеть способностью продемонстрировать практический опыт планирования и организации аналитической деятельности в сфере коммуникации.* *ПК-5.3:* *Знать основы практического*	*Задания* *Реферат* *Тест*	*Экзамен:* *Контрольные вопросы*

		опыта планирования и организации аналитической деятельности *Уметь использовать практический опыт планирования и организации аналитической деятельности* *Владеть навыками использования практического опыта планирования и организации аналитической деятельности*		
ПК-9: Способен руководить проектами по созданию и модернизации гибридных ИИС, базирующихся на концепции системы, основанной на знаниях, и современных нейросетевых технологиях принятия решений	*ПК-9.1: Демонстрирует знание базовых принципов концепции системы, основанной на знаниях, и нейросетевой парадигмы принятия решений при планировании проектов гибридных ИИС.* *ПК-9.2: Демонстрирует умение организовать командный подход к созданию и модернизации гибридных ИИС.* *ПК-9.3: Имеет опыт разработки в команде конкретного проекта по созданию оболочки гибридной ИИС.*	*ПК-9.1:* *Знать требования к системе в целом и к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения информационной безопасности, порядок контроля и приемки системы, значения технических, технологических, производственно-экономических или других показателей объекта автоматизации, которые должны быть достигнуты в результате создания ИС; критерии оценки достижения целей создания системы.* *Уметь формулировать состав и содержание работ, в том числе, и по обеспечению информационной безопасности обозначить назначение и цели разработки информационной системы, вырабатывать требования к системе в целом, к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения ее информационной безопасности, определять порядок контроля и приемки системы* *Владеть навыками определения состава и содержания работ, обозначения назначения и цели*	*Задания* *Реферат* *Тест*	*Экзамен: Контрольные вопросы*

		разработки информационной системы, выработки требований к системе в целом, к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения ее информационной безопасности, определения порядок контроля и приемки системы *ПК-9.2:* *Знать основы командного подхода к созданию и модернизации гибридных ИИС.* *Уметь организовать командный подход к созданию и модернизации гибридных ИИС.* *Владеть навыками по организации командного подхода к созданию и модернизации гибридных ИИС.* *ПК-9.3:* *Знать основы руководства конкретными проектами по созданию и модернизации гибридных ИИС.* *Уметь руководить конкретными проектами по созданию и модернизации гибридных ИИС.* *Владеть навыками руководства конкретными проектами по созданию и модернизации гибридных ИИС.*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная	**очно-заочная**	**заочная**
Общая трудоемкость, з.е.	**4**	**4**	**4**
Часов по учебному плану	**144**	**144**	**144**
в том числе			
аудиторные занятия (контактная работа):			
- занятия лекционного типа	**16**	**8**	**6**
- занятия семинарского типа (практические занятия /	**32**	**16**	**6**

лабораторные работы)			
- КСР	**2**	**2**	**2**
самостоятельная работа	**58**	**82**	**121**
Промежуточная аттестация	**36** **Экзамен**	**36** **Экзамен**	**9** **Экзамен**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)			в том числе											
				Контактная работа (работа во взаимодействии с преподавателем), часы из них									Самостоятельная работа обучающегося, часы		
				Занятия лекционного типа			Занятия семинарского типа (практические занятия/лабораторные работы), часы			Всего					
	оф о	оз ф о	зф о	оф о	оз ф о	зф о	оф о	оз ф о	зф о	оф о	оз ф о	зф о	оф о	оз ф о	зф о
Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей	12	13	17	2	2	2	4	2	0	6	4	2	6	9	15
Тема 2. Виды противников или «нарушителей». Понятие о видах вирусов	12	13	19	2	2	2	4	2	2	6	4	4	6	9	15
Тема 3. Три вида возможных нарушений информационной системы. Защита.	12	13	15	2	2	0	4	2	0	6	4	0	6	9	15
Тема 4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	14	13	19	2	2	2	4	2	2	6	4	4	8	9	15
Тема 5. Криптографические методы защиты информации. Использование защищенных компьютерных систем	14	12	17	2		0	4	2	2	6	2	2	8	10	15
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	14	14	15	2		0	4	2	0	6	2	0	8	12	15
Тема 7. Анализ способов нарушений информационной безопасности	14	14	15	2		0	4	2	0	6	2	0	8	12	15
Тема 8. Место информационной безопасности экономических систем в национальной безопасности страны	14	14	16	2		0	4	2	0	6	2	0	8	12	16
Аттестация	36	36	9												
КСР	2	2	2							2	2	2			
Итого	144	144	144	16	8	6	32	16	6	50	26	14	58	82	121

Содержание разделов и тем дисциплины

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей

Введение в тему: объяснение важности информационной безопасности в современном мире и необходимость соблюдения международных стандартов.
Определение понятия угрозы информационной безопасности и ее классификация. Рассмотрение основных видов угроз: вирусы, хакеры, кибератаки и т.д.
Роль международных стандартов в обеспечении информационной безопасности. Рассмотрение основных стандартов и рекомендаций: ISO/IEC 27001, GDPR, HIPAA и др.
Особенности информационной безопасности в России в условиях функционирования глобальных сетей. Анализ законодательной базы и мер по защите информации.
Практические рекомендации по обеспечению информационной безопасности в организации или личной жизни. Разработка стратегии защиты данных и регулярное обновление безопасности. Обсуждение вопросов и ответы на вопросы участников занятия. Заключение и подведение итогов занятия. Оценка полученных знаний и планы дальнейших действий по обеспечению информационной безопасности.
Тема 2. Виды противников или «нарушителей». Понятие о видах вирусов
Введение и обзор темы: что такое вирус и какие виды вирусов существуют. Типы вредоносных программ: вирусы, черви, троянские программы.
Виды вирусов:
Файловые вирусы: заражают исполняемые файлы.
Сетевые вирусы: распространяются через сети.
Полиморфные вирусы: изменяют свою структуру для избегания обнаружения.
Макровирусы: заражают документы и таблицы.
Boot-вирусы: заражают загрузочные секторы диска.
Примеры известных вирусов и последствия от их действий.
Защита от вирусов:
Антивирусное программное обеспечение.
Регулярное обновление антивирусных баз данных.
Осторожность при открытии вложенных файлов и ссылок.
Обсуждение вопросов и ответы на вопросы участников.
Тема 3. Три вида возможных нарушений информационной системы. Защита.
Обзор основных видов нарушений информационной системы:
Внедрение вредоносного программного обеспечения (вирусы, троянские программы)
Сетевые атаки (DDoS, перехват трафика)
Нарушение конфиденциальности данных (уязвимости в системе безопасности)
Методы защиты от нарушений информационной системы:
Установка антивирусного ПО и регулярное обновление баз данных
Настройка брандмауэра для блокирования нежелательного трафика
Шифрование данных и управление доступом к информационной системе
Практические упражнения:
Прохождение тестов на определение уровня защищенности информационной системы
Симуляция сетевых атак и разработка плана действий по предотвращению
Работа с инструментами мониторинга безопасности (например, IDS/IPS)
Обсуждение случаев реальных нарушений информационной системы и способов их предотвращения.
Заключительные рекомендации по обеспечению безопасности информационной системы и план действий в случае обнаружения угрозы.
Тема 4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
Основные нормативные руководящие документы
Нормативно-справочные документы
Классификация информации по степени секретности
Организация работы с документами, содержащими государственную тайну
Ответственность за нарушение законодательства о государственной тайне

Тема 5. Криптографические методы защиты информации. Использование защищенных компьютерных систем
Криптографические основы защиты информации
Понятие криптографии
Основные алгоритмы шифрования
Принципы работы с криптографическими ключами
Использование защищенных компьютерных систем
Требования к защищенным компьютерным системам
Методы обеспечения безопасности информации в компьютерных системах
Обзор существующих защищенных компьютерных систем и их возможностей
Практические аспекты использования криптографических методов защиты информации
Применение криптографии в различных сферах деятельности
Примеры использования защищенных компьютерных систем на практике
Анализ основных проблем и сложностей в использовании криптографии для защиты информации
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности
Информационные технологии: основные понятия и определения
Организационно-правовое обеспечение информационной безопасности: основные принципы и задачи
Применение информационных технологий в изучении вопросов организационно-правового обеспечения информационной безопасности
Примеры использования информационных технологий в обеспечении информационной безопасности
Тема 7. Анализ способов нарушений информационной безопасности
Определение информационной безопасности и ее значение
Виды угроз информационной безопасности
Методы нарушения информационной безопасности
Примеры нарушений информационной безопасности
Меры предотвращения нарушений информационной безопасности
Тема 8. Место информационной безопасности экономических систем в национальной безопасности страны
Занятие посвящено значению информационной безопасности экономических систем для национальной безопасности страны. Рассматриваются компоненты информационной безопасности, их роль в защите экономики и обеспечении национальной безопасности.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:
Электронные курсы, созданные в системе электронного обучения ННГУ:

Современные методы обеспечения информационной безопасности в информационных системах, не нашел.

Иные учебно-методические материалы:
Учебно-методические документы, регламентирующие самостоятельную работу
адреса доступа к документам:

https://arz.unn.ru/sveden/document/
https://arz.unn.ru/pdf/Metod_all_all.pdf

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ПК-5:

Что такое информационная безопасность?

1. Перечислите основные угрозы информационной безопасности.
2. Какие существуют модели информационной безопасности?
3. Какие методы защиты информации выделяют?
4. Что такое правовые методы защиты информации?
5. Что такое организационные методы защиты информации?
6. Что такое технические методы защиты информации?
7. Что такое программно-аппаратные методы защиты информации?
8. Что такое криптографические методы защиты информации?
9. Что такое физические методы защиты информации?
10. Какие главные государственные органы в области обеспечения информационной безопасности?
11. Перечислите виды защищаемой информации.
12. Какие основные законы в области защиты информации в РФ?
13. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
14. Что такое концепция информационной безопасности?
15. Что такое конфиденциальная информация?
16. Что такое персональные данные?
17. В каких случаях возможно использовать персональные данные без согласия обладателя?
18. Охарактеризуйте биометрические данные как персональные данные.
19. Что такое профессиональная тайна?
20. Что такое коммерческая тайна?
21. Что такое режим коммерческой тайны?
22. Что такое государственная тайна?
23. Опишите правовой режим государственной тайны.
24. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
25. Какие основные международные стандарты в области информационной безопасности существуют?
26. Что такое "Единые критерии"
27. Как связаны международные стандарты и стандарты РФ?

28. Какие основные стандарты РФ в области информационной безопасности существуют?
29. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.

5.1.2 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ПК-9:

1. Что такое политика безопасности?
2. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
3. Что такое инженерная защита объектов?
4. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
5. Что такое технические каналы утечки информации?
6. Перечислите основные виды технических каналов утечки ин-формации?
7. Перечислите методы защиты информации от утечки по визуальному каналу.
8. Перечислите методы защиты информации от утечки по воздушному каналу.
9. Перечислите методы защиты информации от утечки по вибрационному каналу.
10. Перечислите методы защиты информации от утечки по индукционному каналу.
11. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
12. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
13. Какие виды компьютерных угроз существуют?
14. Что такое брандмауэр?
15. Что такое антивирусная программа?
16. Что такое эвристический алгоритм поиска вирусов?
17. Что такое сигнатурный поиск вирусов?
18. Методы противодействия сниффингу?
19. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
20. Что такое механизм контроля и разграничения доступа?
21. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
22. Что такое средства стеганографической защиты информации?
23. Что такое криптография?
24. Какие используются симметричные алгоритмы шифрования?
25. Какие используются ассиметричные алгоритмы шифрования?
26. Что такое криптографическая хеш-функция?
27. Какие используются криптографические хеш-функции?
28. Что такое цифровая подпись?
29. Что такое инфраструктура открытых ключей?
30. Какие российские и международные стандарты на формирование цифровой подписи существуют?
31. Какие основные криптографические протоколы используются в сетях?

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
отлично	Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный
хорошо	Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя
удовлетворительно	Ответ полный, но при этом допущена существенная ошибка или неполный, несвязный ответ
неудовлетворительно	Ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя

5.1.3 Типовые задания (оценочное средство - Реферат) для оценки сформированности компетенции ПК-5:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы

5.1.4 Типовые задания (оценочное средство - Реферат) для оценки сформированности компетенции ПК-9:

1. Криптоанализ, современное состояние
2. Правовые основы защиты информации
3. Технические аспекты обеспечения защиты информации. Современное состояние
4. Атаки на систему безопасности и современные методы защиты
5. Современные пути решения проблемы информационной безопасности РФ

Критерии оценивания (оценочное средство - Реферат)

Оценка	Критерии оценивания
отлично	реферативная работа полностью раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников и изданий периодической печати, приводит практические примеры, в докладе отвечает на дополнительные вопросы преподавателя и студентов
хорошо	реферативная работа частично раскрывает основные вопросы теоретического

Оценка	Критерии оценивания
	материала. Студент приводит информацию из первоисточников, отвечает на дополнительные вопросы преподавателя и студентов (при докладе), но при этом дает не четкие ответы, без достаточно их аргументации
удовлетворительно	реферативная работа в общих чертах раскрывает основные вопросы теоретического материала. Студент приводит информацию только из учебников. При ответах на дополнительные вопросы в докладе путается в ответах, не может дать понятный и аргументированный ответ
неудовлетворительно	ставится за рефераты, в которых нет информации о проблематике работы и ее месте в контек-сте других работ по исследуемой теме

5.1.5 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПК-5:

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется

a. Компилятор
b. Интернет-черви
c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется

a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд

a. Две
b. Одну
c. Сколько зададут

5.1.6 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПК-9:

1. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

a. Статическими алгоритмами
b. Алгоритмы RMS
c. Динамическими алгоритмами

2. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

a. Каталоги
b. Символьные файлы
c. Регулярные файлы

3. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

a. Вирусами
b. Руткитами
c. Червями

4. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности

5. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

a. Управление риском
b. Предупреждением рисков
c. Анализом рисков

6. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

a. Мультипроцессоры типа «хозяин-подчиненный»
b. Симметричный мультипроцессор
c. Мультипроцессор с общей памятью

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
отлично	85-100% правильных ответов
хорошо	66-84 % правильных ответов

Оценка	Критерии оценивания
удовлетворительно	50-65 % правильных ответов
неудовлетворительно	меньше 50 % правильных ответов

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
	не зачтено	**зачтено**		
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме
Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов

Шкала оценивания при промежуточной аттестации

Оценка		**Уровень подготовки**
зачтено	**отлично**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-5

1. Международные стандарты информационного обмена. Понятие угрозы.
2. Информационная безопасность в условиях функционирования в России глобальных сетей. Стандарты в области информационной безопасности.
3. Хакеры. Виды хакеров. Примеры хакерских атак.
4. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.
5. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны
6. Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности.
7. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.
8. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.
9. Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике
10. Криптография. Криптоанализ. Основные понятия криптологии.
11. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование.
12. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы.
13. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов.
14. Концепция информационной безопасности. Основные сведения и положения.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-9

1. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность.
2. Виды противников или «нарушителей». Понятие о видах вирусов. Понятие нарушителя информационной безопасности.
3. Три вида возможных нарушений информационной безопасности. Три составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

5. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.
6. Криптографические методы защиты информации. Симметричные и ассиметричные системы шифрования.
7. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
8. .Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
9. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера.
10. Программы для криптографии. Электронная цифровая подпись.
11. Правовые особенности использования средств информационной защиты.
12. Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
отлично	выставляется, когда студент глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с ситуационными заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок
хорошо	выставляется, если студент твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при анализе информации
удовлетворительно	выставляется в том случае, при котором студент освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении анализа информации
неудовлетворительно	выставляется студенту, в ответе которого обнаружились существенные пробелы в знании основного содержания учебной программы дисциплины и / или неумение использовать полученные знания

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Щеглов А. Ю. Защита информации: основы теории / Щеглов А. Ю., Щеглов К. А. - Москва : Юрайт, 2022. - 309 с. - (Высшее образование). - URL: https://urait.ru/bcode/490019 (дата обращения: 05.01.2022). - ISBN 978-5-534-04732-5 : 969.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=787163&idb=0.
2. Внуков А. А. Защита информации / Внуков А. А. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2022. - 161 с. - (Высшее образование). - URL: https://urait.ru/bcode/490277 (дата обращения: 05.01.2022). - ISBN 978-5-534-07248-8 : 569.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=784475&idb=0.
3. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для вузов / под ред. Поляковой Т.А., Стрельцова А.А. - Москва : Юрайт, 2021. - 325 с. - (Высшее образование). - ISBN 978-5-534-03600-8. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=760974&idb=0.
4. Казарин О. В. Надежность и безопасность программного обеспечения : учебное пособие / О. В. Казарин, И. Б. Шубинский. - Москва : Юрайт, 2022. - 342 с. - (Высшее образование). - URL: https://urait.ru/bcode/493262 (дата обращения: 14.08.2022). - ISBN 978-5-534-05142-1 : 1349.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=817483&idb=0.

Дополнительная литература:

1. Нетёсова О. Ю. Информационные системы и технологии в экономике / Нетёсова О. Ю. - 3-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 178 с. - (Высшее образование). - URL: https://urait.ru/bcode/491479 (дата обращения: 05.01.2022). - ISBN 978-5-534-08223-4 : 499.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=789321&idb=0.
2. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум / О. В. Казарин, А. С. Забабурин. - Москва : Юрайт, 2022. - 312 с. - (Высшее образование). - URL: https://urait.ru/bcode/491249 (дата обращения: 14.08.2022). - ISBN 978-5-9916-9043-0 : 1239.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=816575&idb=0.
3. Информационное право : учебник / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. - Москва : Юрайт, 2022. - 497 с. - (Высшее образование). - URL: https://urait.ru/bcode/489946 (дата обращения: 14.08.2022). - ISBN 978-5-534-10593-3 : 1879.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=821548&idb=0.
4. Крупский В. Н. Теория алгоритмов. Введение в сложность вычислений / Крупский В. Н. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 117 с. - (Высшее образование). - URL: https://urait.ru/bcode/492937 (дата обращения: 05.01.2022). - ISBN 978-5-534-04817-9 : 369.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=786964&idb=0.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

Лицензионное программное обеспечение: Операционная система Windows.
Лицензионное программное обеспечение: Microsoft Office.

Профессиональные базы данных и информационные справочные системы

Российский индекс научного цитирования (РИНЦ), платформа Elibrary: национальная информационно-аналитическая система. Адрес доступа: http://elibrary.ru/project_risc.asp

ГАРАНТ. Информационно-правовой портал [Электронный ресурс].– Адрес доступа: http://www.garant.ru

Свободно распространяемое программное обеспечение:
программное обеспечение LibreOffice;
программное обеспечение Yandex Browser;
программное обеспечение Paint.NET;

программное обеспечение 1С:
* "Бухгалтерия предприятия", редакция 3.0, см. http://v8.1c.ru/buhv8/ ,
* "Управление торговлей", редакция 11.1, см. http://v8.1c.ru/trade/ ,
* "Зарплата и управление персоналом", редакция 3.0, см. http://v8.1c.ru/hrm/ ,
* "Управление небольшой фирмой", редакция 1.5, см. http://v8.1c.ru/small.biz/ ,
* "ERP Управление предприятием 2.0", см. http://v8.1c.ru/erp/ .
* "Бухгалтерия государственного учреждения", редакция 1.0, см. http://v8.1c.ru/stateacc/ ,
* "Зарплата и кадры государственного учреждения", редакция 1.0, http://v8.1c.ru/statehrm/ .
программное обеспечение PascalABC.NET
Электронные библиотечные системы и библиотеки:
Электронная библиотечная система "Лань" https://e.lanbook.com/
Электронная библиотечная система "Консультант студента" http://www.studentlibrary.ru/
Электронная библиотечная система "Юрайт"http://www.urait.ru/ebs
Электронная библиотечная система "Znanium" http://znanium.com/
Электронно-библиотечная система Университетская библиотека ONLINE http://biblioclub.ru/
Фундаментальная библиотека ННГУ www.lib.unn.ru/
Сайт библиотеки Арзамасского филиала ННГУ. – Адрес доступа: lib.arz.unn.ru

Ресурс «Массовые открытые онлайн-курсы Нижегородского университета им. Н.И. Лобачевского» https://mooc.unn.ru/
Портал «Современная цифровая образовательная среда Российской Федерации» https://online.edu.ru/public/promo

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 09.04.03 - Прикладная информатика.

Автор(ы): Статуев Алексей Анатольевич, кандидат педагогических наук, доцент.

Рецензент(ы): Ямпурин Николай Петрович, доктор технических наук.

Заведующий кафедрой: Нестерова Лариса Юрьевна, кандидат педагогических наук.

Программа одобрена на заседании методической комиссии от 27.11.2024 г., протокол № №9.