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

Методы и средства защиты информации

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
44.03.01 - Педагогическое образование

Направленность образовательной программы
Информатика и образовательная робототехника

Форма обучения
очно-заочная

г. Арзамас

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.03 Методы и средства защиты информации 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**
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	*ИУК-2.1: Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологию принятия управленческих решений; экономические основы профессиональной деятельности.* *ИУК-2.2: Умеет разрабатывать план, определять целевые этапы и основные направления работы, выбирать оптимальные способы решения поставленных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.* *ИУК-2.3: Владеет методикой организации проектной деятельности.*	*ИУК-2.1:* *Знать необходимые для осуществления профессиональной деятельности правовые нормы в области защиты информации* *ИУК-2.2:* *Уметь выбирать оптимальные способы решения поставленных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений в сфере защиты информации* *ИУК-2.3:* *Владеть методикой организации проектной деятельности связанной с информационной безопасностью*	*Опрос* *Тест*	*Зачёт:* *Контрольные вопросы*
ПКР-4: Способен осваивать и анализировать базовые научно-теоретические представления о сущности, закономерностях, принципах и особенностях явлений и процессов в предметной области	*ИПКР-4.1: Знает содержание, сущность, закономерности, принципы и особенности изучаемых явлений и процессов, базовые теории в предметной области, а также роль учебного предмета/образовательной области в формировании научной картины мира;*	*ИПКР-4.1:* *Знать содержание, сущность, закономерности, принципы и особенности организации информационной безопасности* *ИПКР-4.2:* *Уметь анализировать базовые научно-теоретические представления о сущности,*	*Опрос* *Тест*	*Зачёт:* *Контрольные вопросы*

	основы общетеоретических дисциплин в объеме, необходимом для решения профессиональных задач. ИПКР-4.2: Умеет анализировать базовые научно-теоретические представления о сущности, закономерностях, принципах и особенностях изучаемых явлений и процессов в предметной области знаний. ИПКР-4.3: Владеет различными методами анализа основных категорий предметной области знаний.	*закономерностях, принципах и особенностях организации информационной безопасности* *ИПКР-4.3: Владеть различными методами анализа основных категорий информационной безопасности*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очно-заочная
Общая трудоемкость, з.е.	**3**
Часов по учебному плану	**108**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**8**
- занятия семинарского типа (практические занятия / лабораторные работы)	**16**
- КСР	**1**
самостоятельная работа	**83**
Промежуточная аттестация	**0** **Зачёт**

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	
	очно-заочная форма	очно-заочная форма	очно-заочная форма	очно-заочная форма	очно-заочная форма
Тема 1. Угрозы безопасности информации в информационно-	27	2	4	6	21

вычислительных системах. Правовые и организационные методы защиты информации в информационно-вычислительных системах					
Тема 2. Административный уровень информационной безопасности в информационно-вычислительной системе. Криптографическая защита информации.	27	2	4	6	21
Тема 3. Системы безопасности операционных систем. Вирусные угрозы. Антивирусные системы безопасности.	27	2	4	6	21
Тема 4. Защита информации в корпоративных сетях.	26	2	4	6	20
Аттестация	0				
КСР	1			1	
Итого	108	8	16	25	83

Содержание разделов и тем дисциплины

Тема1. Угрозы безопасности информации в информационно-вычислительных системах. Правовые и организационные методы защиты информации в информационно-вычислительных системах.
Понятие угрозы безопасности. Классификация угроз информационной безопасности. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации. Правовое регулирование в области безопасности информации. Государственная политика России в области безопасности информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты информации
Тема 2. Административный уровень информационной безопасности в информационно-вычислительной системе. Криптографическая защита информации.
Понятие политики безопасности. Анализ риска. Угрозы, видимость и доступность информации. Уязвимость информации и последствия утечки информации. Учет информационных ценностей. Модели основных типов политик безопасности. Понятие криптографическая защита информации. Классификация криптографических методов защиты информации. Основные криптографические модели. Симметричные а ассиметричные методы шифрования
Тема 3. Системы безопасности операционных систем. Вирусные угрозы. Антивирусные системы безопасности.
Механизмы защиты операционных систем. Система безопасности Windows. Система безопасности Unix. Система безопасности Makintosh. Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения, защиты и лечения от компьютерных вирусов
Тема 4. Защита информации в корпоративных сетях.
Управление доступом. Идентификация и установление подлинности. Проверка полномочий пользователей. Реагирование на несанкционированные действия. Межсетевые экраны. Типы межсетевых экранов

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:

Методы и средства защиты информации, https://e-learning.unn.ru/course/view.php?id=9981.

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 - Опрос) для оценки сформированности компетенции УК-2:

1. Вредоносное программное обеспечение и информационная безопасность.
2. Классификация вредоносного программного обеспечения.
3. Особенности работы антивирусных программ.
4. Методы защиты от вредоносных программ.
5. Классификация угроз для мобильных устройств.
6. Защита мобильных устройств.
7. Механизмы обеспечения информационной безопасности в информационных системах.
8. Идентификация и аутентификация.

5.1.2 Типовые задания (оценочное средство - Опрос) для оценки сформированности компетенции ПКР-4:

1. Методы разграничения доступа.
2. Регистрация и аудит.
3. Межсетевое экранирование.
4. Технология виртуальных частных сетей.
5. Основные виды DDos-атак.
6. Способы защиты от DDos-атак.
7. Основные характеристики и модели облачных сервисов.
8. Методы защиты данных в облачных сервисах.

Критерии оценивания (оценочное средство - Опрос)

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

Оценка	Критерии оценивания
	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

5.1.3 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции УК-2:

1. Охраняемая законом конфиденциальная информация в области производственно-хозяйственной, управленческой, финансовой деятельности организации представляющую собой ценность в силу неизвестности ее третьим лицам и к которой нет свободного доступа на законном основании называется:

- Профессиональной тайной
- Служебной тайной
- Коммерческой тайной
- Личной тайной

2. Бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена, называется:

- Утечкой информации
- Кражей информации
- Потерей информации
- Угрозой информации

3. Главной причиной утечки конфиденциальной информации является:

- Ошибки проектирования автоматизированных информационных систем
- Ошибки систем защиты
- Несоблюдения персоналом норм, требований и правил эксплуатации автоматизированных информационных систем
- Ведение конкурентами технической и агентурной разведки

4. К основополагающим документам в области информационной безопасности относятся:

- Оранжевая книга
- Радужная серия
- Голубая линия
- ГОСТ ИСО 9000 «Защита информации»

5. Комплект документов, определяющих основные принципы, правила, процедуры и иные действия в сфере информационной безопасности компании называется:

- Политикой информационной безопасности компании
- Правилами внутренней информационной деятельности компании
- Зеленой линией информации
- Концепцией защиты информации компании

6. Искусственные угрозы безопасности информации вызваны:

- деятельностью человека
- ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
- воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
- корыстными устремлениями злоумышленников

7. К основным непреднамеренным искусственным угрозам АСОИ относится:

- физическое разрушение системы путем взрыва, поджога и т.п.
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи
- изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

8. К посторонним лицам нарушителям информационной безопасности относится:

- персонал, обслуживающий технические средства
- пользователи
- сотрудники службы безопасности
- представители конкурирующих организаций.

9. Защита данных с помощью шифрования называется

- Шифровальной защитой
- Криптографической защитой
- Имитозащитой данных
- Шифрованной посылкой

10.Вредоностная программа, способная создавать копии самой себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи называется:

- Червем
- Троянским конем
- Логической бомбой
- Вирусом

5.1.4 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПКР-4:

1. Вредоносная программа, распространяемая людьми под видом обычных программ, осуществляющая различные несанкционированные пользователем действия (сбор информации и её передачу злоумышленнику, её разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях), называется:

- Троянской программой или троянским конем
- Вирусом
- Ревизором
- Червем

2. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

- черный пиар
- фишинг
- нигерийские письма
- источник слухов

3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

- черный пиар
- фишинг
- нигерийские письма

- источник слухов

4. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

- детектор
- доктор
- сканер
- ревизор

5. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

- детектор
- доктор
- сканер
- ревизор

6. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

- детектор
- доктор
- сканер
- ревизор

7. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

- доктор
- сканер
- ревизор
- сторож

8. Активный перехват информации это перехват, который:

- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
- неправомерно использует технологические отходы информационного процесса
- осуществляется путем использования оптической техники
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

9. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- активный перехват
- пассивный перехват
- аудиоперехват
- просмотр мусора

10. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

- активный перехват
- пассивный перехват
- аудиоперехват
- видеоперехват

11. Перехват, который осуществляется путем использования оптической техники называется:

- активный перехват
- пассивный перехват
- аудиоперехват
- видеоперехват

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
отлично	80 – 100 % правильных ответов
хорошо	60 – 79 % правильных ответов
удовлетворительно	40 – 59% правильных ответов
неудовлетворительно	менее 40 % 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	**неудовлетворит**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».

зачтено	**ельно**	

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 УК-2

1. Понятие угрозы безопасности в информационно-вычислительных системах.
2. Классификация угроз информационной безопасности.
3. Классификация злоумышленников.
4. Основные методы реализации угроз информационной безопасности.
5. Причины, виды и каналы утечки информации в информационно-вычислительных системах.
6. Правовое регулирование в области безопасности информации.
7. Государственная политика России в области безопасности информационных технологий.
8. Структура государственных органов, обеспечивающих безопасность информационных технологий.
9. Общая характеристика организационных методов защиты информации.
10. Понятие политики безопасности. Анализ риска.
11. Угрозы, видимость и доступность информации.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-4

1. Уязвимость информации и последствия утечки информации.
2. Учет информационных ценностей.
3. Модели основных типов политик безопасности.
4. Понятие криптографическая защита информации.
5. Классификация криптографических методов защиты информации.
6. Основные криптографические модели.
7. Симметричные а ассиметричные методы шифрования.
8. Механизмы защиты операционных систем. Система безопасности Windows.
9. Механизмы защиты операционных систем. Система безопасности Unix.
10. Механизмы защиты операционных систем. Система безопасности Makintosh.
11. Вредоносные программы.
12. Классификация компьютерных вирусов.
13. Профилактика и лечение информационных инфекций.
14. Программы обнаружения, защиты и лечения от компьютерных вирусов.
15. Управление доступом.
16. Идентификация и установление подлинности.
17. Проверка полномочий пользователей.
18. Реагирование на несанкционированные действия.
19. Межсетевые экраны. Типы межсетевых экранов.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	Ответ полный и правильный на основании изученной теории; теоретический материал и решение поставленных задач изложены в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный. Могут быть допущены две-три несущественные ошибки, исправленные по требованию преподавателя

Оценка	Критерии оценивания
не зачтено	Ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя

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

Основная литература:

1. Баранова Елена Константиновна. Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2022. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=832410&idb=0.
2. 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.
3. Нестеров С. А. Информационная безопасность : учебник и практикум / С. А. Нестеров. - Москва : Юрайт, 2018. - 321 с. - (Профессиональное образование). - ISBN 978-5-534-07979-1. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=840366&idb=0.

Дополнительная литература:

1. Гришина Наталия Васильевна. Информационная безопасность предприятия : Учебное пособие / Российский государственный гуманитарный университет РГГУ. - 2. - Москва : Издательство "ФОРУМ", 2022. - 239 с. - Среднее профессиональное образование. - ISBN 978-5-00091-545-5. - ISBN 978-5-16-108896-8. - ISBN 978-5-16-013930-2., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=834585&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.

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

Свободно распространяемое программное обеспечение:

программное обеспечение LibreOffice;
программное обеспечение Yandex Browser;

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 44.03.01 - Педагогическое образование.

Автор(ы): Володин Андрей Михайлович, кандидат педагогических наук, доцент.

Рецензент(ы): Фролов Иван Валентинович, доктор педагогических наук.

Заведующий кафедрой: Нестерова Лариса Юрьевна, кандидат педагогических наук.

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