

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**

Факультет естественных и математических наук

УТВЕРЖДЕНО  
решением ученого совета ННГУ  
протокол № 6 от 31.05.2023 г.

### **Рабочая программа дисциплины**

#### **Методы и средства защиты информации**

*(наименование дисциплины)*

Уровень высшего образования

бакалавриат

*(бакалавриат / магистратура / специалитет)*

Направление подготовки / специальность

44.03.01 Педагогическое образование

*(указывается код и наименование направления подготовки / специальности)*

Направленность образовательной программы

Информатика

*(указывается профиль / магистерская программа / специализация)*

Форма обучения

заочная

*(очная / очно-заочная / заочная)*

Год начала подготовки 2020

Арзамас

2023 год

## 1. Место дисциплины (модуля) в структуре ООП

Дисциплина Б1.В.05 «Методы и средства защиты информации» относится к части, формируемой участниками образовательных отношений образовательной программы направления подготовки 44.03.01 Педагогическое образование, направленность (профиль) Информатика.

Дисциплина предназначена для освоения студентами заочной формы обучения на 3 курсе.

## 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 (дескрипторы компетенции)	
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.	<i>Знать</i> необходимые для осуществления профессиональной деятельности правовые нормы в области защиты информации	Вопросы для устного опроса, тест
		<i>Уметь</i> выбирать оптимальные способы решения поставленных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений в сфере защиты информации	Вопросы для устного опроса
		<i>Владеть</i> методикой организации проектной деятельности связанной с информационной безопасностью	Вопросы для устного опроса
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; 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.	<i>Знать</i> содержание, сущность, закономерности, принципы и особенности организации информационной безопасности	Вопросы для устного опроса, тест
		<i>Уметь</i> анализировать базовые научно-теоретические представления о сущности, закономерностях, принципах и особенностях организации информационной безопасности	Вопросы для устного опроса
		<i>Владеть</i> различными методами анализа основных категорий информационной безопасности	Вопросы для устного опроса

### 3. Структура и содержание дисциплины

#### 3.1. Структура дисциплины

Трудоемкость	очная форма обучения
<b>Общая трудоемкость</b>	3 з.е.
часов по учебному плану, из них	108
<b>Контактная работа</b> , в том числе: аудиторные занятия:	
– занятия лекционного типа	
– занятия семинарского типа	4
контроль самостоятельной работы	1
<b>Промежуточная аттестация</b> зачет	4
<b>Самостоятельная работа</b>	99

#### 3.2. Содержание дисциплины

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

Наименование разделов (Р) или тем (Т) дисциплины (модуля),  Форма(ы) промежуточной аттестации по дисциплине	Всего (часы)		Контактная работа (работа во взаимодействии с преподавателем), часы, из них						Самостоятельная работа обучающегося, часы, в период			
			Занятия лекционного типа		Занятия семинарского типа (в т.ч. текущий контроль успеваемости)		Контроль самостоятельной работы		промежуточной аттестации (контроля)		теоретического обучения	
					семинары, практические занятия	лабораторные работы						
	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная
Тема1. Угрозы безопасности информации в информационно-вычислительных системах. Правовые и организационные методы защиты информации в информационно-вычислительных системах.		24						1				23
Тема 2. Административный уровень информационной безопасности в информационно-вычислительной системе. Криптографическая защита информации.		28						1				27
Тема 3. Системы безопасности операционных систем. Вирусные угрозы. Антивирусные системы безопасно-		26						1				25

сти.													
Тема 4. Защита информации в корпоративных сетях.		25						1					24
В том числе текущий контроль		1								1			
Зачет		4										4	
<b>ИТОГО</b>		<b>108</b>						<b>4</b>		<b>1</b>		<b>4</b>	<b>99</b>

Текущий контроль успеваемости реализуется в рамках занятий практического типа, консультаций.

#### 4. Учебно-методическое обеспечение самостоятельной работы студентов

Самостоятельная работа является важнейшей составной частью учебного процесса и обязанностью каждого студента.

Для обеспечения самостоятельной работы обучающихся используется электронный курс Методы и средства защиты информации, <https://e-learning.unn.ru/course/view.php?id=9981>, созданный в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>.

Самостоятельная работа студентов по дисциплине «Методы и средства защиты информации» осуществляется в следующих видах:

- работа над учебным материалом (учебниками, конспектами лекций, дополнительной литературой);
- подготовка к занятиям семинарского типа (лабораторным занятиям);
- подготовка к тестированию;
- подготовка к зачёту.

##### Методические рекомендации по работе над учебным материалом

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

##### Методические рекомендации по подготовке к занятиям семинарского типа

Подготовка к занятиям семинарского типа (лабораторным занятиям) – традиционная форма самостоятельной работы обучающихся, включает отработку лекционного материала, изучение рекомендованной литературы, конспектирование предложенных источников.

Подготовка к опросу, проводимому в рамках практического занятия, требует уяснения вопросов, вынесенных на конкретное занятие, подготовки выступлений, повторения основных терминов, запоминания формул и алгоритмов.

Серьезная теоретическая подготовка необходима для выполнения лабораторных работ. Предварительное изучение методических рекомендаций «Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата // ЭБС Юрайт [сайт]. — код доступа: <https://urait.ru/book/informacionnaya-bezopasnost-434171>.» по выполнению работ с определением цели, хода их выполнения позволит Вам проявить самостоятельность и творческую инициативу.

##### Методические рекомендации по подготовке к тестированию

Тестирование является одним из обязательных видов самостоятельной работы студентов. Целью тестирования является выработка умений и навыков самостоятельной работы; формирование навыков работы со специальной литературой и умения применять свои знания к конкретным ситуациям.

1. Внимательно прочитайте материал по конспектам, составленным на учебных занятиях.

2. Прочитайте тот же материал по учебнику, учебному пособию.
3. Если вопрос вынесен на самостоятельное изучение, постарайтесь разобраться с непонятными, в частности, с новыми терминами.
4. Ответьте на контрольные вопросы для самопроверки, имеющиеся в учебнике.
5. Кратко перескажите содержание изученного материала «своими словами».
6. Заучите «рабочие определения» основных понятий, законов.
7. Освоив теоретический материал, приступайте к выполнению заданий, упражнений; решению задач, расчетов самостоятельной работы, составлению графиков, таблиц и т.д.

Подготовка к аудиторной контрольной работе аналогична предыдущей форме, но требует более тщательного изучения материала по теме или блоку тем, где акцент делается на изучение причинно-следственных связей, раскрытию природы явлений и событий, проблемных вопросов.

### **Методические рекомендации по подготовке к зачету**

Зачет проводится в традиционной форме (тестирование, а также учет результатов выполнения лабораторных работ).

Подготовка к зачету начинается с первого занятия по дисциплине. При этом важно с самого начала планомерно осваивать материал, руководствуясь требованиями, конспектировать важные для решения учебных задач источники, обращаться к преподавателю за консультацией по неусвоенным вопросам.

Для подготовки к сдаче зачета необходимо первоначально прочитать лекционный материал, а также соответствующие разделы рекомендуемых изданий. Лучшим вариантом является тот, при котором при подготовке используется несколько источников информации. Это способствует разностороннему восприятию каждой конкретной темы дисциплины.

В обобщённом варианте подготовка к сдаче зачета включает в себя:

- просмотр программы учебной дисциплины, перечня вопросов к зачету;
- подбор рекомендованных преподавателем источников (учебников, дополнительной литературы и т.д.),
- использование конспектов лекций, материалов занятий и их изучение;
- консультирование у преподавателя.

### **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](https://arz.unn.ru/pdf/Metod_all_all.pdf)

## **5. Фонд оценочных средств для промежуточной аттестации по дисциплине**

### **5.1. Описание шкал оценивания результатов обучения по дисциплине**

В ходе промежуточной аттестации по дисциплине осуществляется оценка сформированности компонентов компетенций (полнота знаний/ наличие умений/ навыков), т.е. результатов обучения, указанных в таблице п.2 настоящей рабочей программы, на основе оценки усвоения содержания дисциплины.

Обобщенная оценка сформированности компонентного состава компетенции в ходе промежуточной аттестации по дисциплине проводится на основе учета текущей успеваемости в ходе освоения дисциплины и учета результата сдачи промежуточной аттестации.

Выявленные признаки несформированности компонентов (индикаторов) хотя бы одной компетенции не позволяют выставить интегрированную положительную оценку сформированности компетенций и освоения дисциплины на данном этапе обучения.

Обобщенная оценка сформированности компонентного состава компетенций на промежуточной аттестации, которая вносится в зачетно-экзаменационную ведомость по дисциплине и зачетную книжку студента, осуществляется по следующей оценочной шкале.

### Шкала оценки сформированности компонентного состава компетенций на промежуточной аттестации

Оценка		Уровень подготовки
Зачтено	Отлично	сформированность компонентного состава (индикаторов) компетенций соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, студент готов самостоятельно решать стандартные и нестандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
	Хорошо	сформированность компонентного состава (индикаторов) компетенций соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, но студент готов самостоятельно решать только различные стандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
	Удовлетворительно	сформированность компонентного состава (индикаторов) компетенций соответствует в целом требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, но студент способен решать лишь минимум стандартных профессиональных задач в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
Не зачтено	Неудовлетворительно	сформированность компонентного состава (индикаторов) компетенций не соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, студент не готов решать профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы

### Шкала оценивания сформированности компетенции

Уровень сформированности компетенции (индикатора достижения компетенции)				
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
<b><u>Знания</u></b>	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 требованиям программы подготовки, без ошибок.
<b><u>Умения</u></b>	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными незначительными недочетами, выполнены все задания в полном объеме.
<b><u>Навыки</u></b>	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.

## **5.2 Критерии и процедуры оценивания результатов обучения по дисциплине**

### **Критерии оценки тестирования**

**Оценка «отлично»** 80 – 100 % правильных ответов;

**Оценка «хорошо»** 60 – 79 % правильных ответов;

**Оценка «удовлетворительно»** 40 – 59% правильных ответов.

**Оценка «неудовлетворительно»** менее 40 % правильных ответов.

### **Критерии устного ответа студента при опросе на занятии / на зачёте**

**Оценка «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.

**Оценка «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.

**Оценка «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.

**Оценка «неудовлетворительно»** выставляется студенту, в ответе которого обнаружались существенные пробелы в знании основного содержания учебной программы дисциплины и / или неумение использовать полученные знания.

## **5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения и для контроля формирования компетенции**

### **Вопросы для собеседования (Вопросы для устного опроса) 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.

### **для оценки сформированности компетенции ПКР-4**

9. Методы разграничения доступа.
10. Регистрация и аудит.
11. Межсетевое экранирование.
12. Технология виртуальных частных сетей.
13. Основные виды DDos-атак.
14. Способы защиты от DDos-атак.
15. Основные характеристики и модели облачных сервисов.
16. Методы защиты данных в облачных сервисах.

**Типовые тестовые задания  
для оценки сформированности компетенции УК-2**

Выберите один из предложенных вариантов ответа.

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:  
А) Профессиональной тайной  
Б) Служебной тайной  
В) Коммерческой тайной  
Г) Личной тайной
2. Бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена, называется:  
А) Утечкой информации  
Б) Кражей информации  
В) Потерей информации  
Г) Угрозой информации
3. Главной причиной утечки конфиденциальной информации является:  
А) Ошибки проектирования автоматизированных информационных систем  
Б) Ошибки систем защиты  
В) Несоблюдения персоналом норм, требований и правил эксплуатации автоматизированных информационных систем  
Г) Ведение конкурентами технической и агентурной разведки
4. К основополагающим документам в области информационной безопасности относятся:  
А) Оранжевая книга  
Б) Радужная серия  
В) Голубая линия  
Г) ГОСТ ИСО 9000 «Защита информации»
6. Комплект документов, определяющих основные принципы, правила, процедуры и иные действия в сфере информационной безопасности компании называется:  
А) Политикой информационной безопасности компании  
Б) Правилами внутренней информационной деятельности компании  
В) Зеленой линией информации  
Г) Концепцией защиты информации компании
6. Искусственные угрозы безопасности информации вызваны:  
А) деятельностью человека  
Б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения  
В) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека  
Г) корыстными устремлениями злоумышленников
7. К основным непреднамеренным искусственным угрозам АСОИ относится:  
А) физическое разрушение системы путем взрыва, поджога и т.п.  
Б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи  
В) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.  
Г) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.



9. К посторонним лицам нарушителям информационной безопасности относится:

- А) персонал, обслуживающий технические средства
- Б) пользователи
- В) сотрудники службы безопасности
- Г) представители конкурирующих организаций.

10. Защита данных с помощью шифрования называется

- А) Шифровой защитой
- Б) Криптографической защитой
- В) Имитозащитой данных
- Г) Шифрованной посылкой

11. Вредоносная 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:

- А) Червем
- Б) Троянским конем
- В) Логической бомбой
- Г) Вирусом

**для оценки сформированности компетенции ПКР-4**

12. 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 неблагоприятных целях), называется:

- А) Троянской программой или троянским конем
- Б) Вирусом
- В) Ревизором
- Г) Червем

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

- А) черный пиар
- Б) фишинг
- В) нигерийские письма
- Г) источник слухов

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

- А) черный пиар
- Б) фишинг
- В) нигерийские письма
- Г) источник слухов

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

- А) детектор
- Б) доктор
- В) сканер
- Г) ревизор

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

- А) детектор
- Б) доктор
- В) сканер
- Г) ревизор

17. 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:

- А) детектор
- Б) доктор
- В) сканер
- Г) ревизор

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

- А) доктор
- Б) сканер
- В) ревизор
- Г) сторож.

19. Активный перехват информации это перехват, который:

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

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

- А) активный перехват
- Б) пассивный перехват
- В) аудиоперехват
- Г) просмотр мусора

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

- А) активный перехват
- Б) пассивный перехват
- В) аудиоперехват
- Г) видеоперехват

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

- А) активный перехват
- Б) пассивный перехват
- В) аудиоперехват
- Г) видеоперехват

### Контрольные вопросы для промежуточной аттестации (к зачету)

№	Вопрос	Код формируемой компетенции
1.	Понятие угрозы безопасности в информационно-вычислительных системах.	УК-2
2.	Классификация угроз информационной безопасности.	УК-2
3.	Классификация злоумышленников.	УК-2
4.	Основные методы реализации угроз информационной безопасности.	УК-2
5.	Причины, виды и каналы утечки информации в информационно-вычислительных системах.	УК-2
6.	Правовое регулирование в области безопасности информации.	УК-2
7.	Государственная политика России в области безопасности информационных технологий.	УК-2
8.	Структура государственных органов, обеспечивающих безопасность информационных технологий.	УК-2
9.	Общая характеристика организационных методов защиты информации.	УК-2
10.	Понятие политики безопасности. Анализ риска.	УК-2
11.	Угрозы, видимость и доступность информации.	УК-2
12.	Уязвимость информации и последствия утечки информации.	ПКР-4
13.	Учет информационных ценностей.	ПКР-4
14.	Модели основных типов политик безопасности.	ПКР-4
15.	Понятие криптографическая защита информации.	ПКР-4
16.	Классификация криптографических методов защиты информации.	ПКР-4
17.	Основные криптографические модели.	ПКР-4
18.	Симметричные а ассиметричные методы шифрования.	ПКР-4
19.	Механизмы защиты операционных систем. Система безопасности Windows.	ПКР-4
20.	Механизмы защиты операционных систем. Система безопасности Unix.	ПКР-4
21.	Механизмы защиты операционных систем. Система безопасности Makintosh.	ПКР-4
22.	Вредоносные программы.	ПКР-4
23.	Классификация компьютерных вирусов.	ПКР-4
24.	Профилактика и лечение информационных инфекций.	ПКР-4
25.	Программы обнаружения, защиты и лечения от компьютерных вирусов.	ПКР-4
26.	Управление доступом.	ПКР-4
27.	Идентификация и установление подлинности.	ПКР-4
28.	Проверка полномочий пользователей.	ПКР-4
29.	Реагирование на несанкционированные действия.	ПКР-4
30.	Межсетевые экраны. Типы межсетевых экранов.	ПКР-4

### 6. Учебно-методическое и информационное обеспечение дисциплины

#### а) основная литература:

**Информационная безопасность и защита информации:** Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: - (Высшее образование) Адрес доступа: <http://znanium.com/catalog/product/957144>

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Серия

: Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — Адрес доступа: <https://urait.ru/book/informacionnaya-bezopasnost-434171> .

#### **б) дополнительная литература:**

Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2016. - 240 с. // ЭБС «Znaniy» [Электронный ресурс]. — Адрес доступа: <http://znaniy.com/catalog.php?bookinfo=544554>

Ищейнов В.Я. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. // ЭБС «Znaniy»: [Электронный ресурс]. — Адрес доступа: <http://znaniy.com/catalog.php?bookinfo=508381>

#### **в) программное обеспечение и Интернет-ресурсы:**

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](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 "Znaniy" <http://znaniy.com/>

Электронно-библиотечная система Университетская библиотека ONLINE <http://biblioclub.ru/>

Фундаментальная библиотека ННГУ [www.lib.unn.ru/](http://www.lib.unn.ru/)

Сайт библиотеки Арзамасского филиала ННГУ. — Адрес доступа: [lib.arz.unn.ru](http://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)**

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: ноутбук, проектор, экран.

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

Программа дисциплины **Методы и средства защиты информации** составлена в соответствии с образовательным стандартом высшего образования (ОС ННГУ) по направлению подготовки 44.03.01 Педагогическое образование (уровень бакалавриата) (приказ ННГУ от 17.05.2023 года № 06.49-04-0214/23)

Автор(ы):

к.п.н., доцент

Володин А.М.

Рецензент (ы):

д.п.н., доцент

Фролов И.В.

Кафедра математики, физики и информатики

д.п.н., доцент

Фролов И.В.

Программа одобрена на заседании методической комиссии от 24.05.2023 года, протокол № 5

Председатель МК

к.п.н., доцент

факультета естественных и математических наук

Володин А.М.

П.6. а) СОГЛАСОВАНО:

Заведующий библиотекой

Федосеева Т.А.