

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дзержинский филиал ННГУ

---

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

**Рабочая программа дисциплины**

Информационная безопасность

---

Уровень высшего образования

Бакалавриат

---

Направление подготовки / специальность

38.03.01 - Экономика

---

Направленность образовательной программы

Финансы и кредит

---

Форма обучения

очная, очно-заочная

---

г. Дзержинск

2024 год начала подготовки

## 1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.15 Информационная безопасность относится к обязательной части 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
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.1: Понимает принципы работы современных информационных технологий ОПК-6.2: Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности	ОПК-6.1: Знать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Уметь использовать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Владеть навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности  ОПК-6.2: Знать: основные положения экономической теории в профессиональной деятельности с учетом информационной безопасности. Уметь: оценивать экономические, социальные и	Тест	Экзамен: Тест

		<p>политические условия для реализации профессиональной деятельности с учетом информационной безопасности.</p> <p>Владеть: навыками анализа условий реализации профессиональной деятельности с учетом информационной безопасности.</p>		
<p>ПК-3: Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений</p>	<p>ПК-3.1: Формирует, анализирует и интерпретирует финансово-экономическую информацию</p> <p>ПК-3.2: Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений</p>	<p>ПК-3.1:</p> <p>Знать основные законодательные акты в сфере информационной безопасности</p> <p>Уметь использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий</p> <p>Владеть навыками соблюдения норм и правил, существующих в виртуальной среде</p> <p>ПК-3.2:</p> <p>Знать: основы разработки и реализации политики государственного управления с учетом информационной безопасности.</p> <p>Уметь: разрабатывать социально-экономические проекты с учетом информационной безопасности.</p> <p>Владеть: навыками разработки и реализации приоритетов политики государственного управления с учетом информационной безопасности.</p>	Тест	<p>Экзамен:</p> <p>Тест</p>

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	очная	очно-заочная
--	-------	--------------

<b>Общая трудоемкость, з.е.</b>	<b>4</b>	<b>4</b>
<b>Часов по учебному плану</b>	<b>144</b>	<b>144</b>
в том числе		
<b>аудиторные занятия (контактная работа):</b>		
- занятия лекционного типа	24	12
- занятия семинарского типа (практические занятия / лабораторные работы)	24	12
- КСР	2	2
<b>самостоятельная работа</b>	<b>58</b>	<b>82</b>
<b>Промежуточная аттестация</b>	<b>36</b> Экзамен	<b>36</b> 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				
				о ф о	о з ф о			о ф о		
Политика государства в области информационной безопасности	26	26	6	2	6	4	12	6	14	20
Угрозы и нарушители безопасности информации	28	26	6	4	6	2	12	6	16	20
Модель угроз безопасности информации	26	28	6	4	6	4	12	8	14	20
Политика безопасности организации	26	26	6	2	6	2	12	4	14	22
Аттестация	36	36								
КСР	2	2					2	2		
Итого	144	144	24	12	24	12	50	26	58	82

### Содержание разделов и тем дисциплины

Тема 1. Политика государства в области информационной безопасности

Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации. Модель угроз безопасности информации. Политика безопасности организации. Системы обнаружения и предотвращения компьютерных атак. Основные стандарты в области информационной безопасности.

Тема 2. Угрозы и нарушители безопасности информации

Понятие угрозы безопасности информации. Виды угроз безопасности информации. Источники угроз безопасности информации. Нарушители безопасности информации. Виды и цели нарушителей.

Потенциал и возможности нарушителей. Способы реализации угроз нарушителем.

Тема 3. Модель угроз безопасности информации

Назначение модели угроз ИБ. Идентификация угроз безопасности информации и их источников. Модель нарушителя. Принцип оценки актуальности угроз. Оценка возможности реализации угрозы. Оценка степени ущерба. Оценка актуальности угрозы.

Тема 4. Политика безопасности организации

Понятие политики безопасности. Назначение и содержание политики безопасности. Вопросы, рассматриваемые в политике безопасности. Организационные аспекты информационной безопасности. Управление активами. Безопасность, связанная с управлением персоналом. Физическая безопасность. Управление доступом. Вопросы эксплуатации информационных систем. Управление инцидентами и непрерывностью бизнеса. Соответствие требованиям обязательств организации. Жизненный цикл политики безопасности.

Практическая часть

1. Работа со средствами криптографии
2. Шифры и криптоанализ
3. Защита бланка организации от редактирования средствами MS Word
4. Аппаратные системы безопасности ПК
5. Основы информационной и компьютерной безопасности
6. Настройки безопасности ОС типа Windows

#### **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:

Информационная безопасность (Поляков Е.А.), <https://e-learning.unn.ru/course/view.php?id=2193>.

Иные учебно-методические материалы:

Теоретическая часть курса

Интерактивный курс:

Тестовые задания по всем темам курса.

Лекционный материал:

1. Политика государства в области информационной безопасности
2. Угрозы и нарушители безопасности информации
3. Модель угроз безопасности информации
4. Политика безопасности организации

Презентации:

Политика государства в области информационной безопасности

Угрозы и нарушители безопасности информации

Модель угроз безопасности информации

Политика безопасности организации

Лабораторный практикум

Практика 1. Работа со средствами криптографии

Практика 2. Шифры и криптоанализ

Практика 3. Защита бланка от редактирования средствами MS Word

Практика 4. Аппаратные системы безопасности ПК

Практика 5. Основы информационной и компьютерной безопасности

Практика 6. Первичные настройки безопасности ОС типа Windows

Контроль по курсу

Экзаменационное занятие

## **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 - Тест) для оценки сформированности компетенции ОПК-6:**

##### **1. Укажите типы угроз, относящихся к классу аспекта информационной безопасности:**

- A) угрозы нарушения конфиденциальности
- B) угрозы нарушения целостности
- C) угрозы нарушения доступности
- D) угрозы через воздействие на аппаратуру
- E) угрозы через воздействия на информацию

##### **2. В чем состоит суть Стратегии национальной безопасности РФ?**

- A) является базовым документом стратегического планирования
- B) определяются основные показатели состояния национальной безопасности
- C) в ней определяются стратегические национальные приоритеты РФ
- D) в ней определяются национальные интересы РФ
- E) в ней определяются положение России в современном мире

##### **3. Что такое Информационная сфера?**

совокупность [1] \_\_\_\_\_, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением

[2] \_\_\_\_\_, а также совокупность

[3] \_\_\_\_\_ соответствующих общественных отношений.

A) информации	D) национальной безопасности
B) правовых механизмов	E) средств коммуникации
C) информационной безопасности	F) механизмов регулирования

**4. Какой документ выражает систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере?**

- A) Конституция РФ
- B) доктрина информационной безопасности РФ
- C) Закон об информации, информационных технологиях и о защите информации
- D) Уголовный кодекс РФ
- E) стратегия национальной безопасности РФ

**5. Укажите все угрозы конфиденциальности информации:**

- A) подслушивание переговоров направленным микрофоном
- B) блокирование операционной системы вредоносной программой
- C) подбор пароля для доступа к базе данных
- D) блокирование информационной системы путем хакерской атаки
- E) использование чужой учетной записи для доступа к файлам
- F) похищение носителя с зашифрованной информацией
- G) подбор криптографического ключа для зашифрованного документа

**5.1.2 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПК-3:**

**1.** Актуальность угрозы, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., означает, что

- A) реализация угрозы нанесет ущерб владельцу или оператору информации либо субъекту персональных данных
- B) существует актуальный для данной информационной системы нарушитель с достаточным потенциалом для реализации угрозы
- C) в информационной системе существует возможность реализации угрозы
- D) в информационной системе существует достаточная вероятность реализации угрозы, а ее последствия имеют средний или высокий уровень наносимого ущерба
- E) в информационной системе существует возможность реализации угрозы нарушителем с

соответствующим потенциалом и ее реализация приведет к нанесению ущерба

**2.** Укажите, какие действия реализуются на этапе внедрения политики безопасности:

- A) происходит ознакомление сотрудников с содержанием политики безопасности
- B) разрабатывается план внедрения политики безопасности
- C) производится определение требований к системе обеспечения безопасности информации
- D) создаётся группа по внедрению политики безопасности
- E) проводится обучение сотрудников принципам работы по требованиям политики безопасности
- F) которые зависят от перечня актуальных угроз
- G) которые зависят от выработанной политики управления рисками

**3.** На этапе внедрения политики безопасности организации осуществляется...

- A) оценка рисков
- B) обеспечение наличия и функционирования систем и устройств, необходимых для обеспечения политики безопасности
- C) выбор системы мер обеспечения безопасности информации, снижающих риски до приемлемых значений
- D) определение требований к системе обеспечения безопасности информации.

**4.** Что включает в себя первый этап построения угроз информационной безопасности?

- A) определение физических и логических границ ИС
- B) описание пути прохождения информации
- C) определение области действия
- D) определение возможных способов реализации угроз безопасности информации

**5.** Укажите, какие действия реализуются на этапе первоначального аудита безопасности

- A) определение требований к системе обеспечения безопасности информации
- B) построение модели актуальных угроз
- C) идентификация угроз безопасности информации
- D) идентификация активов
- E) разработка плана внедрения политики безопасности

**Критерии оценивания (оценочное средство - Тест)**



Оценка	Критерии оценивания
зачтено	75% и более правильных ответов
не зачтено	менее 75% правильных ответов

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

### Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено			зачтено			
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	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. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	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. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи с отдельным и несущественными недочетами, выполнены все задания в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторым	Продemonстрированы базовые навыки при решении стандартных задач с некоторым и	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продemonстрированы навыки при решении нестандартных задач без ошибок и	Продemonстрирован творческий подход к решению нестандартных задач

	ответа		и недочетами	недочетами		недочетов	
--	--------	--	-----------------	------------	--	-----------	--

### Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «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».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

### 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 - Тест) для оценки сформированности компетенции ОПК-6

Билет 1.

##### 1. Что понимается под Информационной безопасностью России в Доктрине ИБ?

состояние максимально [1]\_\_\_\_\_ для Российской Федерации с точки зрения её существования и максимально благополучная также для [2]\_\_\_\_\_ с точки зрения их конституционных [3]\_\_\_\_\_, с точки зрения развития общества

А) осуществления законности и правопорядка	Д) обязанностей граждан
В) прав и свобод	Е) благополучное
С) личности и общества	Ф) защищенное

2. Назовите способы защиты документа от несанкционированных действий пользователя. Для примера можно использовать функции любого текстового редактора.

Билет 2.

**1.** Опишите реальные способы выполнения задания:

Необходимо скопировать на флешку несколько системных файлов из корневого каталога Windows (виртуальной ОС) и любой системной папки.

**2. Что такое свобода выражения мнения с точки зрения информационной безопасности России?**

А) право человека свободно распространять информацию и идеи без какого-либо ограничения

В) обязанность выполнять Конституцию РФ, федеральные законы и иные законодательные и исполнительные акты в части свободы распространения информации

С) право человека свободно выражать и придерживаться своего мнения

Д) право выполнять Конституцию РФ, федеральные законы и иные законодательные и исполнительные акты в части свободы распространения информации

### 5.3.2 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПК-3

Билет 1.

**1.** Укажите свойства методов идентификации, аутентификации и их использование при реализации криптографического преобразования информации.

В каком виде и каких типах файлов ОС типа Windows хранятся эти данные?

Ответ; Идентификация - это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация - это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Хранение данных в ОС Windows:

- Идентификационные данные:
- Идентификационные данные, такие как учетные записи пользователей, хранятся в защищенной базе данных, которая может быть локальной (Security Accounts Manager - SAM) или в доменной среде (Active Directory).
- Аутентификационные данные:
- Пароли и другие аутентификационные данные хранятся в хэшированном виде в базе данных SAM. Хэши помогают защитить данные от несанкционированного доступа в случае утечки.

Типы файлов ОС Windows:

- Идентификационные данные:
- В базе данных SAM хранятся учетные записи пользователей в файлах SAM и SYSTEM, которые обычно находятся в директории C:\Windows\System32\config.
- Аутентификационные данные:
- Аутентификационные данные, такие как пароли, не хранятся в открытом виде, но в виде хэшей в файле SAM.

**2.** Угроза безопасности информации, заключающаяся в удалении информации в базе данных ИС с помощью вредоносной программы с целью причинения ущерба, корректно описывается следующим образом:

разработчик программного обеспечения; программная закладка в разработанном ПО; НСД к

А) информации в базе данных; причинение имущественного ущерба; несанкционированное удаление информации из базы данных

В) разработчик программного обеспечения; доступ к информации на прикладном уровне; НСД к информации в базе данных; сервер базы данных; причинение имущественного ущерба

разработчик программного обеспечения; программная закладка в разработанном ПО; НСД к

С) информации в базе данных; сервер базы данных; несанкционированное удаление информации из базы данных

- D разработчик программного обеспечения; сервер базы данных; НСД к информации в базе данных;  
) программная закладка в разработанном ПО; несанкционированное удаление информации из базы данных

## Билет 2.

### 1. Какие варианты защиты поля ввода вы знаете?

Для примера можно использовать функции любого текстового редактора.

2. Уволенный из организации за халатность системный администратор, желающий в отместку навредить бывшему работодателю и предпринимая попытку хакерской атаки на информационную систему, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК В 2015 г., описывается следующей моделью нарушителя (тип; вид; потенциал; цель (мотивация); возможные способы реализации угроз безопасности информации):

- A) внешний; администраторы информационной системы; базовый; причинение имущественного ущерба; воздействие на объекты на сетевом уровне
- B) внешний; бывшие работники; базовый повышенный; причинение имущественного ущерба; воздействие на объекты на сетевом уровне
- C) внутренний; администраторы информационной системы; базовый повышенный; месть за ранее совершенные действия; воздействие на объекты на сетевом уровне
- D) внешний; бывшие работники; базовый; месть за ранее совершенные действия; воздействие на объекты на сетевом уровне

## Билет 3.

### 1. Задача:

С помощью программ WINRAR, WINZIP и т.д. пользователь создал запароленный на 4, символов с английскими и (или) русскими символами архив текстового файла.

нужно ответить на вопрос: Какова криптостойкость программ-архиваторов, какая из них лучше защитит данные пользователя и какими методами может воспользоваться пользователь при попытке взлома с использованием ARCHPR 2.0, AAPP4.54?

Ответ:

#### **WINRAR и WINZIP:**

- Обе программы предлагают различные методы шифрования, такие как AES (Advanced Encryption Standard) с различными битовыми длинами ключа. Используйте наиболее современные и безопасные методы шифрования, если это возможно.
- WINRAR использует RAR5 формат с поддержкой AES-256, что является сильным методом шифрования.
- WINZIP также поддерживает AES с длиной ключа до 256 бит.

Рекомендации для повышения криптостойкости:

- Используйте длинные и сложные пароли, включая комбинации букв (верхнего и нижнего регистра), цифр и специальных символов.
- Предпочтительно использовать последние версии архиваторов с современными методами шифрования.
- Если возможно, выбирайте AES с длиной ключа 256 бит.
- Регулярно обновляйте программы-архиваторы и следите за выходом обновлений безопасности.

### 2. Укажите все угрозы конфиденциальности информации:

- A) использование чужой учетной записи для доступа к файлам
- B) блокирование операционной системы вредоносной программой
- C) блокирование информационной системы путем хакерской атаки
- D) подбор криптографического ключа для зашифрованного документа

- Е) подслушивание переговоров направленным микрофоном
- Ф) подбор пароля для доступа к базе данных
- Г) похищение носителя с зашифрованной информацией

### Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
превосходно	не оценивается
отлично	>95% правильных ответов
очень хорошо	не оценивается
хорошо	>85 до 95% правильных ответов
удовлетворительно	>75 до 85% правильных ответов
неудовлетворительно	менее 75% правильных ответов
плохо	не оценивается

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

Основная литература:

1. Барлаков С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие для студентов специальностей «информационная безопасность», «менеджмент», «государственное и муниципальное управление», «системный анализ и управление» / Барлаков С. А., Моисеев С. И., Порядина В. Л. - Санкт-Петербург : Интермедия, 2016. - 264 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0135-6., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=879502&idb=0>.
2. Ворона А. А. Информационно-экономическая и информационная безопасность в условиях функционирования центров электронного декларирования : учебное пособие / Ворона А. А., Коптева Л. А. - 2-е изд., доп. - Санкт-Петербург : Интермедия, 2022. - 182 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0246-9., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=881457&idb=0>.
3. Зенков А. В. Информационная безопасность и защита информации : учебное пособие / А. В. Зенков. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871683&idb=0>.

#### Дополнительная литература:

1. Информационная безопасность : лабораторный практикум. - Пермь : ПГГПУ, 2018. - 87 с. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции ПГГПУ - Информатика. - ISBN 978-5-85219-007-9., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=722553&idb=0>.
2. Информационная безопасность и защита информации : практикум / Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. - Дубна : Государственный университет «Дубна», 2020. - 85 с. - Рекомендовано учебно-методическим советом университета «Дубна» в качестве практикума для студентов, обучающихся по направлениям подготовки «Системный анализ и управление», «Прикладная информатика», «Прикладная математика и информатика (магистратура)». - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции Государственный университет «Дубна» - Информатика. - ISBN 978-5-89847-608-3., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=730800&idb=0>.
3. Стрижакова Е. А. Информационная безопасность в профессиональной деятельности: лабораторный практикум для обучающихся по специальности 38.05.01 Экономическая безопасность / Стрижакова Е. А., Пенькова Р. И. - Волгоград : Волгоградский ГАУ, 2022. - 92 с. - Книга из коллекции Волгоградский ГАУ - Информатика., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=866608&idb=0>.

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

1. Операционная система Microsoft Windows
2. Пакет прикладных программ Microsoft Office

#### **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 38.03.01 - Экономика.

Автор(ы): Поляков Евгений Артурович, кандидат педагогических наук.

Заведующий кафедрой: Поляков Евгений Артурович, кандидат педагогических наук.

Программа одобрена на заседании методической комиссии от 22.12.2023, протокол № 17.