

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Институт информационных технологий, математики и механики  
(факультет / институт / филиал)

УТВЕРЖДЕНО  
президиумом Ученого совета ННГУ  
протокол от  
14.12.2021 г. №4

**Рабочая программа дисциплины**

**Информационная безопасность**

*(наименование дисциплины (модуля))*

Уровень высшего образования

**бакалавриат**

*(бакалавриат / магистратура / специалитет)*

Направление подготовки / специальность

**09.03.03 «Прикладная информатика**

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

Направленность образовательной программы

**Прикладная информатика в области обработки данных**

*(указывается профиль / магистерская программа / специализация)*

Форма обучения

**Очно-заочная**

*(очная / очно-заочная / заочная)*

Нижний Новгород

2022

## 1. Место дисциплины в структуре ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
2	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.02 Информационная безопасность относится к части ООП направления подготовки 09.03.03 Прикладная информатика, формируемой участниками образовательных отношений.

## 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**	
<b>ПК-10.</b> <i>Способен осуществлять локальную модернизацию системы, адаптировать бизнес-процессы организации к возможностям ИС (ИИС)</i>	<b>ПК-10.1.</b> <i>Демонстрирует знание методологических основ документирования бизнес-процессов.</i>	<i>Знать основные положения стандартов и руководящих документов в области информационной безопасности Знать опасности и угрозы информации и информационным системам Знать основные правила управления ИБ</i>	<i>Собеседование</i>
	<b>ПК-10.2.</b> <i>Демонстрирует умение организовать и поддерживать репозиторий ИС, хранящий информацию о сопровождении системы в процессе ее жизненного цикла.</i>	<i>Уметь разрабатывать организационно-распорядительные документы в области информационной безопасности организации Уметь обеспечивать информационную безопасность организации Уметь разрабатывать правила информационной безопасности</i>	<i>Собеседование</i>
	<b>ПК-10.3.</b> <i>Имеет практический опыт документирования бизнес-процессов и адаптации их к возможностям конкретной ИС.</i>	<i>Владеть нормативно-методическим, аппаратным и программным инструментарием обеспечения информационной безопасности Владеть аппаратным и программным инструментарием обеспечения информационной безопасности Владеть методами разработки, сопровождения, управления информационной безопасности.</i>	<i>Собеседование</i>

## 3. Структура и содержание дисциплины

### 3.1. Трудоемкость дисциплины

	<b>Очно-заочная форма обучения</b>
<b>Общая трудоемкость</b>	<b>4 ЗЕТ</b>
<b>Часов по учебному плану</b>	<b>144</b>
<b>в том числе</b>	
<b>аудиторные занятия (контактная работа):</b>	<b>34</b>
- занятия семинарского типа	32
- текущий контроль (КСР)	2
<b>самостоятельная работа</b>	<b>74</b>
<b>Промежуточная аттестация – экзамен</b>	<b>36</b>

### 3.2. Содержание дисциплины

Наименование и краткое содержание 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	Занятия лабораторного типа	Всего	
Тема 1. Информационная безопасность в деятельности организации	15		4		4	11
Тема 2. Информация с ограниченным доступом	16		4		4	12
Тема 3. Угрозы информационной безопасности	16		4		4	12
Тема 4. Обеспечение информационной безопасности организации	17		4		4	13
Тема 5. Правовые средства обеспечения информационной безопасности	18		4		4	14
Тема 6. Организационные средства обеспечения информационной безопасности	19		4		4	15
Тема 7. Инженерно-технические средства обеспечения информационной безопасности	20		4		4	16
Тема 8. Обеспечение информационной безопасности в автоматизированных информационных системах	21		4		4	17
Текущий контроль (КСР)	2				2	
Промежуточная аттестация – экзамен	144		32		34	74

Текущий контроль успеваемости реализуется в формах опросов на занятиях семинарского типа

Промежуточная аттестация проходит в традиционных формах (экзамен)

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

Для самоконтроля у студента имеется возможность изучения материала в дистанционном управляемом курсе (требуется авторизация): <https://e-learning.unn.ru/course/view.php?id=3376>

Самостоятельная работа проходит в форме выполнения практического индивидуального задания (контрольной работы) «Моделирование системы информационной безопасности» на основе нормативных документов ФСТЭК»

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

## 5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

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

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности 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 незначительных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	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 отдельными незначительными 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 владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	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 базовые навыки при решении стандартных задач без ошибок и недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач.

### Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	Превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно»
	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»
	Очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
	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», ни одна из компетенций не сформирована на уровне «плохо»
	Плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

## 5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения

### 5.2.1 Контрольные вопросы

Вопросы к Экзамену по дисциплине «Информационная безопасность»	Код компетенции
1. Понятие безопасности	ПК-10
2. Основные объекты безопасности:	
3. Угроза безопасности организации	
4. Понятие информационной безопасности	
5. Объекты информационной безопасности организации	
6. Гриф конфиденциальности	
7. Сведения с ограниченным доступом	
8. Признаки информации, составляющей коммерческую или служебную тайну	
9. Действия и события, нарушающие информационную безопасность	
10. Каналы утечки информации	
11. Акустические сигналы как источник утечки информации	
12. Перехват как способ НСД	
13. НСД к информации	
14. Утечка информации	
15. Разглашение информации	
16. Средства обеспечения информационной безопасности	
17. Система информационной безопасности	
18. Субъекты информационной безопасности	
19. Предмет правового регулирования в сфере информационной безопасности	

20. Нормативно-правовые документы организации в сфере ИБ
21. Индивидуально-правовые документы организации в сфере информационной безопасности
22. Перечень конфиденциальных сведений
23. Основные организационные мероприятия в сфере ИБ
24. Организация обеспечения ИБ
25. Принципы обеспечения информационной безопасности на основе ИТС
26. Методы обеспечения ИБ инженерно-техническими средствами
27. Методы и средства подключения
28. Основные руководящие документы в области обеспечения безопасности автоматизированных систем
29. Организационные меры защиты компьютера от действий злоумышленников.
30. Классы защищенности автоматизированных систем от несанкционированного доступа к информации.
31. Содержание и основные этапы проведения работ по защите средств электронно-вычислительной техники.
32. Защита информации в компьютерных сетях
33. Обеспечение безопасности от угрозы вирусных атак.
34. Криптографическая защита данных.
35. Компьютерная стеганография и стеганофония

## 6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Сергеева, Ю.С. Защита информации. Конспект лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : А-Приор, 2011. — 128 с. — Режим доступа: <http://e.lanbook.com/book/3083> — Загл. с экрана.
2. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие / Е.Б. Белов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: <http://e.lanbook.com/book/5121> — Загл. с экрана.
3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. [Электронный ресурс] : учеб.-метод. пособие — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 320 с. — Режим доступа: <http://e.lanbook.com/book/5150> — Загл. с экрана.

б) дополнительная литература:

1. Малышенко Ю. В., Федоров В. В. - Защита информации в вычислительных сетях, системах и комплексах: учеб. пособие по дисциплине "Информац. тамож. технологии". - М.: РИО РТА, 2007. - 108 с. -17 экз
2. Горбунов, В.А. Математические методы в теории защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горная книга, 2004. — 82 с. — Режим доступа: <http://e.lanbook.com/book/3490> — Загл. с экрана.
3. Сергеева Ю. С. - Защита информации: пособие для подготовки к экзаменам. - М.: А-Приор, 2011. - 128 с – 5экз

## 7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой (лекционного и семинарского типа), оснащенные оборудованием и техническими средствами обучения.

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 09.03.03 Прикладная информатика.

Автор \_\_\_\_\_ профессор Карпычев В.Ю.

Рецензент \_\_\_\_\_ профессор Федосенко Ю.С.

Заведующий кафедрой \_\_\_\_\_ М.Х.Прилуцкий

Программа одобрена на заседании методической комиссии института информационных технологий, математики и механики

01.12.2021 года, протокол № 2