

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

УТВЕРЖДЕНО
решением Ученого совета ННГУ
протокол от
30.11.2022 №13

Рабочая программа дисциплины (модуля)

Информационная безопасность

Уровень высшего образования

Бакалавриат

Направление подготовки / специальность

09.03.03 Прикладная информатика

Направленность образовательной программы

Прикладная информатика в информационной сфере

Форма обучения

Очная

Нижегород
2021

1. Место и цели дисциплины (модуля) 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.13 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**	
ПК-7. Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-7.1. Демонстрирует знание основных технологий организации ИТ-инфраструктуры, управления информационной безопасностью.	Знать: основные положения стандартов и руководящих документов в области информационной безопасности Знать: опасности и угрозы информации и информационным системам Знать: основные правила управления ИБ	Собеседование
	ПК-7.2. Демонстрирует умение разрабатывать организационное обеспечение ИТ-инфраструктуры и информационной безопасности.	Уметь: разрабатывать организационно-распорядительные документы в области информационной безопасности организации Уметь: обеспечивать информационную безопасность организации Уметь: разрабатывать правила информационной безопасности	Собеседование
	ПК-7.3. Имеет практический опыт составления документации по организации ИТ-инфраструктуры и управлению информационной безопасностью.	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.	Собеседование

3. Структура и содержание дисциплины «Программирование под Windows»

3.1. Трудоемкость дисциплины

	очная форма обучения
Общая трудоемкость	3 ЗЕТ
Часов по учебному плану	108
в том числе	
контактная работа:	34
- занятия лекционного типа	32
- текущий контроль (КСР)	2
самостоятельная работа	38
Промежуточная аттестация – экзамен	36

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	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	8	2			2	6
Тема 2. Информация с ограниченным доступом	10	4			4	6
Тема 3. Угрозы информационной безопасности	10	4			4	6
Тема 4. Обеспечение информационной безопасности организации	8	4			4	4
Тема 5. Правовые средства обеспечения информационной безопасности	8	4			4	4
Тема 6. Организационные средства обеспечения информационной безопасности	8	4			4	4
Тема 7. Инженерно-технические средства обеспечения информационной безопасности	8	4			4	4
Тема 8. Обеспечение информационной безопасности в автоматизированных информационных системах	10	6			6	4
Текущий контроль	2				2	
Промежуточная аттестация Экзамен	36					
Итого	108	32			34	38

Текущий контроль успеваемости реализуется в рамках занятий лекционного типа. Промежуточная аттестация проходит в традиционной форме (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 студента при изучении дисциплины «Информационная безопасность» включает выполнение заданий под контролем преподавателя, решение домашних заданий и подготовку к экзамену.

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, 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 ошибки.	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, 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 небольшими 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 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	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован 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 для оценки компетенции ПК-7

1. Понятие безопасности
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 (модуля)

а) основная литература:

1. Малышенко Ю. В., Федоров В. В. - Защита информации в вычислительных сетях, системах и комплексах: учеб. пособие по дисциплине "Информационные технологии". - М.: РИО РТА, 2007. - 108 с. (16 экз.)

б) дополнительная литература:

1. Мельников В. П., Клейменов С. А., Петраков А. М. - Информационная безопасность и защита информации: учеб. пособие для студентов вузов, обучающихся по специальности "Информационные системы и технологии". - М.: Академия, 2011. - 336 с. (12 экз.)

7. Материально-техническое обеспечение дисциплины

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

Помещения для самостоятельной работы 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 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
07.12.2022 протокол №4