

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

решением Ученого совета ННГУ

протокол №13 от 30.11.2022 г.

Рабочая программа дисциплины

Основы безопасности ИТ

(наименование дисциплины (модуля))

Уровень высшего образования

Бакалавриат

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

020302 Фундаментальная информатика и информационные технологии

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Инженерия программного обеспечения

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2023 год

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.07 «Основы безопасности ИТ» относится к части ООП направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии, 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**	
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	УК-2-1. Знает необходимые для осуществления профессиональной деятельности фундаментальные основы используемой науки, а также соответствующие правовые нормы	ЗНАТЬ основные алгоритмы обеспечения безопасности при реализации программного обеспечения; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; профессиональной терминологией в области информационной безопасности	Собеседование Задача (практическое задание)
	УК-2-3. Имеет практический опыт решения задач в области избранных видов профессиональной деятельности	ВЛАДЕТЬ навыками работы с нормативными правовыми актами.	Собеседование Задача (практическое задание)

3. Структура и содержание дисциплины

3.1. Трудоемкость дисциплины

	Очная форма обучения
Общая трудоемкость	2 ЗЕТ
Часов по учебному плану	72
в том числе	
аудиторные занятия (контактная работа):	25
- занятия лекционного типа	24
- занятия семинарского типа	0
- занятия лабораторного типа	0
- текущий контроль (КСР)	1

самостоятельная работа	47
Промежуточная аттестация –зачет	

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины	Всего (часы)	В том числе				Самостоятельная работа обучающегося, часы
		Контактная работа (работа во взаимодействии с преподавателем), часы. Из них				
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Нормативная база в области информационной безопасности	12	4			4	8
2. Основные понятия безопасности автоматизированных систем обработки информации (АСОИ)	12	4			4	8
3. Характеристики наиболее распространенных угроз безопасности АСОИ	12	4			4	8
4. Политика безопасности. Модели политики безопасности	12	4			4	8
5. Достоверная вычислительная база	12	4			4	8
6. Критерии оценки безопасности АСОИ	11	4			4	7
Текущий контроль (КСР)	1					
Промежуточная аттестация – зачет						
Итого	72					47

Текущий контроль успеваемости реализуется в форме проверки задач

Промежуточная аттестация проходит в традиционной форме (зачет)

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Для студентов разработано учебно-методическое пособие «Защита от НСД с помощью ПАК АККОРД», в которое вынесены вопросы изучения политик безопасности. Материалы пособия дополняются разделами из списка рекомендованной литературы. Контроль за процессом усвоения материала осуществляется с помощью контрольных вопросов.

Виды самостоятельной работы студентов

Изучение учебной литературы и материалов учебно-методического пособия и подготовка к зачету

Образовательные материалы для самостоятельной работы студентов

1. Горбунов А.А., Ротков Л.Ю., Рябов А.А. "Защита от НСД с помощью ПАК "Аккорд". Фонд электронных образовательных ресурсов ННГУ р.№ 935.15.04 <http://www.unn.ru/books/resources.html>
2. Грибунин В. Г., Чудовский В. В. - Комплексная система защиты информации на предприятии: учеб. пособие для студентов вузов, обучающихся по специальностям "Орг. и

технология защиты информации", "Комплекс. защита объектов информатизации". – М.: Академия, 2009. – 6 экз

3. Гринберг А. С., Король И. А. - Информационный менеджмент: учеб. пособие для студентов вузов, обучающихся по специальностям "Менеджмент", "Информ. системы". - М.: Юнити, 2003. - 415 с. Более 40 экз

4. Информационный менеджмент: учебник./Абдикеев Н. М., Бондаренко В. И., Киселев А. Д., Китова О. В., Лавлинский Н. Е., Попов И. И. - М.: ИНФРА-М, 2012. - 400 с. 25 экз.

5. Технологии электронных коммуникаций. ТТ - М.: Россия, 1993-1996. – 35 экз.

6. Щебет Ю. и др. Стандарты информационной безопасности. Курс ИНТУИТ. <http://www.intuit.ru/studies/courses/30/30/info>

7. Щебет Ю. и др. Основы информационной безопасности. Курс ИНТУИТ. <http://www.intuit.ru/studies/courses/10/10/info>

8. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 05.12.2016 г. № 646 (интернет-ресурс: <http://www.kremlin.ru/acts/bank/41460>)

9. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_2481/)

10. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61798/)

11. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_112701/)

12. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61801/)

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	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	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.

	вследствие отказа обучающегося от ответа			ошибок	ых ошибок		
<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.	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. 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.	Продемонстрированы 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

вопросы	Код формируемой компетенции
1. Основные понятия безопасности АСОИ	УК-2
2. Классификация угроз информационной безопасности	УК-2
3. Характеристики наиболее распространенных угроз безопасности	УК-2
4. Вредоносные программы	УК-2
5. Избирательная политика безопасности	УК-2
6. Полномочная политика безопасности. Модель Белла-Лападулы	УК-2
7. Управление информационными потоками	УК-2
8. Достоверная вычислительная база	УК-2
9. Механизмы защиты. Ядро безопасности. Монитор ссылок	УК-2
10. Идентификация, аутентификация и авторизация субъектов и объектов системы	УК-2
11. Контроль входа пользователя в систему и управление паролями	УК-2
12. Регистрация и протоколирование. Аудит	УК-2
13. Противодействие «сборке мусора»	УК-2
14. Контроль целостности субъектов. Модель Биба	УК-2
15. Принципы реализации политики безопасности	УК-2
16. Система документов США. Классы защищенности компьютерных систем МО США. Европейские критерии безопасности	УК-2
17. Руководящие документы ГТК РФ: "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности". Классификация автоматизированных систем и требования по защите информации	УК-2
18. Общие критерии оценки безопасности информационных технологий. Стандарт безопасности ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий"	УК-2
19. Практическое внедрение электронной цифровой подписи. Закон Российской Федерации №63-ФЗ "Об электронной подписи"	УК-2
20. Принципы и мероприятия обеспечения информационной безопасности при обработке персональных данных. Закон Российской Федерации №152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ №1119 от 01.11.2012	УК-2

5.2.2. Типовые задания/задачи для оценки сформированности компетенции УК-2

Задача 1. Пояснить пример представленных ПРД: Пользователю разрешено работать в указанном каталоге.

Задача 2. Пояснить пример представленных ПРД: Пользователю на диске будут видны и доступны только явно описанные каталоги.

Задача 3. Пояснить пример представленных ПРД: Пользователю разрешено работать только с файлами и только в выделенном каталоге.

Задача 4. Пояснить пример представленных ПРД: Применение атрибутов наследования.

Задача 5. Пояснить по каким характеристикам СЗИ «Аккорд» отнесено к определенному классу защиты.

Задача 6. Реализовать политику разграничения доступа «Конфиденциальное делопроизводство» для двух пользователей User1 и User2 с домашними каталогами D:\U1 и D:\U2.

Задача 7. Разработать набор испытаний реализации правил разграничения доступа из задания 1.

Задача 8. Исследовать содержимое журналов комплекса «Аккорд». Выделить в них сеансы работы всех пользователей системы. Детально описать один сеанс любого пользователя.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Горбунов А.А., Ротков Л.Ю., Рябов А.А. "Защита от НСД с помощью ПАК "Аккорд". Фонд электронных образовательных ресурсов ННГУ р.№ 935.15.04 <http://www.unn.ru/books/resources.html>
2. Гринберг А. С., Король И. А. - Информационный менеджмент: учеб. пособие для студентов вузов, обучающихся по специальностям "Менеджмент", "Информ. системы". - М.: Юнити, 2003. - 415 с. Более 40 экз
3. Щебет Ю. и др. Стандарты информационной безопасности. Курс ИНТУИТ. <http://www.intuit.ru/studies/courses/30/30/info>
4. Щебет Ю. и др. Основы информационной безопасности. Курс ИНТУИТ. <http://www.intuit.ru/studies/courses/10/10/info>

б) дополнительная литература:

1. Информационный менеджмент: учебник./Абдикеев Н. М., Бондаренко В. И., Киселев А. Д., Китова О. В., Лавлинский Н. Е., Попов И. И. - М.: ИНФРА-М, 2012. - 400 с. 25 экз.
2. Технологии электронных коммуникаций. ТТ - М.: Россия, 1993-1996. – 35 экз.

в) программное обеспечение и Интернет-ресурсы:

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 05.12.2016 г. № 646 (интернет-ресурс: <http://www.kremlin.ru/acts/bank/41460>)
2. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_2481/)
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61798/)
4. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_112701/)
5. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61801/)

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 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 02.03.02 Фундаментальная информатика и информационные технологии.

Автор (ы) _____ Л.Ю. Ротков

_____ А.А. Горбунов

Рецензент (ы) _____

Заведующий кафедрой _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии института информационных технологий, математики и механики 30.11.2022 года, протокол № 3