

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Радиофизический факультет

(факультет / институт / филиал)

УТВЕРЖДЕНО

решением ученого совета ННГУ

протокол от

«31» мая 2023 г. № 6

Рабочая программа дисциплины

Организационное и правовое обеспечение
информационной безопасности

(наименование дисциплины (модуля))

Уровень высшего образования

магистратура

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

02.04.02 Фундаментальная информатика и информационные технологии

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Информационная безопасность и защита информации

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2023 год

1. Место дисциплины в структуре ООП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам части, формируемой участниками образовательных отношений, основной образовательной программы по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

№ 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.ДВ.01.01 «Организационное и правовое обеспечение информационной безопасности» относится к части ООП направления подготовки 02.04.02 «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	
ПК-1. Способен руководить научными исследованиями и опытно-конструкторскими разработками, в области фундаментальной информатики и информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	ПК-1.1. Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности	Знать: - проблематику и методы научных исследований и опытно-конструкторских разработок в области безопасности информационных технологий	Собеседование
	ПК-1.2. Умеет выполнять научные исследования и опытно-конструкторские разработки в области ФИИТ применительно к профессиональной деятельности	Уметь: - проводить научные исследования и опытно-конструкторские разработки в области безопасности информационных технологий	Собеседование
	ПК-1.3. Имеет навыки руководства исследованиями и опытно-конструкторскими	Владеть: - навыками руководства исследованиями и опытно-конструкторскими разработками в области безопасности информационных технологий	Собеседование

	разработками в области ФИИТ применительно к профессиональной деятельности, и формирования их новых направлений		
--	--	--	--

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	3 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	108		
в том числе			
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа (практические занятия / лабораторные работы)	32		
самостоятельная работа	75		
КСР	1		
Промежуточная аттестация – экзамен/зачет	зачет		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	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	
1. Основные положения руководящих документов полномочных органов государственной власти Российской Федерации в области защиты информации	33	10			10	23
2. Создание системы защиты информации. Организация защиты информации	36	10			10	26
3. Лицензирование деятельности по технической защите информации, созданию средств защиты информации. Сертификация средств защиты информации по требованиям безопасности информации	38	12			12	26
Итого:	107	32			32	75

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя изучение дополнительных разделов дисциплины с использованием учебной литературы.

Текущий контроль усвоения материала проводится путем проведения опроса.

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	При решении стандартных	Имеется минимальны	Продemonстрированы	Продemonстрированы	Продemonстрированы	Продemonстрированы

	материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	задачи не продемонстрированы базовые навыки. Имели место грубые ошибки.	набор навыков для решения стандартных задач с некоторыми недочетами	базовые навыки при решении стандартных задач с некоторыми недочетами	базовые навыки при решении стандартных задач без ошибок и недочетов.	навыки при решении нестандартных задач без ошибок и недочетов.	творческий подход к решению нестандартных задач
--	--	---	---	--	--	--	---

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
	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
зачтено	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

<i>Вопросы</i>	<i>Код формируемой компетенции</i>
1. Какие основные законы РФ используются для организации деятельности по защите информатизации	ПК-1
2. Какие нормативные и методические документы используются при организации технической защиты конфиденциальной информации (аттестации объектов информатизации, обрабатывающих конфиденциальную информацию)	ПК-1
3. Какие основные нормативные правовые акты, используются при лицензировании деятельности по технической защите информации, созданию средств защиты информации	ПК-1
4. Что собой представляет система защиты информации объекта информатизации	ПК-1
5. Какие мероприятия проводятся для обеспечения защиты информации, содержащейся в информационной системе	ПК-1
6. Какие мероприятия включает внедрение системы защиты информации информационной системы	ПК-1
7. Что собой представляют требования безопасности информации	ПК-1
8. Назовите порядок проведения организацией аттестации объектов информатизации, обрабатывающих конфиденциальную информацию	ПК-1
9. Какие бывают объекты информатизации, обрабатывающие информацию	ПК-1
10. Как осуществляется обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы	ПК-1
11. Чем достигается обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы	ПК-1
12. Дать определение лицензируемому виду деятельности	ПК-1
13. Что собой представляют лицензионные требования	ПК-1
14. Что собой представляет система сертификации средств защиты информации по требованиям безопасности информации	ПК-1

5.2.2. Типовые задания для оценки сформированности компетенции ПК-1

1. Перечислить мероприятия, проводимые для обеспечения защиты информации, содержащейся в информационной системе.
2. Перечислить мероприятия, которые включает внедрение системы защиты информации информационной системы.
3. Назвать порядок проведения организацией аттестации объектов информатизации, обрабатывающих конфиденциальную информацию.
4. Пояснить невыполнение каких требований считается грубым нарушением лицензионных требований.
5. Назвать формы осуществления лицензионного контроля.
6. Назвать порядок сертификации средств защиты информации по требованиям безопасности информации.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ярочкин В.И. Информационная безопасность : учеб. для вузов / В.И. Ярочкин. - 4-е изд. - М. Академ. проект, 2006. - 543 с.
2. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности. – М.: Издательство Юрайт, 2017. – 325 с.

б) дополнительная литература:

1. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»
2. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
3. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
4. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».
5. Распоряжение Президента Российской Федерации от 16 апреля 2005 года № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».
6. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
8. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
9. Постановление Правительства Российской Федерации от 18.09.2012 № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю».
10. Постановление Правительства Российской Федерации от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти».
11. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».
12. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

13. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».
14. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
15. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
16. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
17. Приказ ФСТЭК России от 11.02.2013 № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
18. Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
19. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.
20. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.
21. Приказ ФСТЭК России от 17.07.2017 № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».
22. Приказ ФСТЭК России от 17.07.2017 № 133 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации».
23. Приказ ФСТЭК России от 20.07.2012 № 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации»
24. Приказ ФСТЭК России от 20.07.2012 № 90 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации».
25. «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации», одобрено решением Гостехкомиссии России от 14.03.1995 № 32.
26. «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в организациях», одобрено решением Гостехкомиссии России от 14.03.1995 № 32.
27. Приказ Минздравсоцразвития России от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

28. ГОСТ Р 50922-2006 «Национальный стандарт российской федерации. Защита информации. Основные термины и определения».
29. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
30. Федеральный закон «О лицензировании отдельных видов деятельности» от 4.05.2011 № 99-ФЗ.
31. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313.
32. Кодекс РФ «Об административных правонарушениях», статьи 13.12, 13.13.
33. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
34. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
35. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

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. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) (интернет-ресурс: <http://fstec.ru/>)

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, 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 по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

Автор (ы) _____ Л.Ю. Ротков

_____ С.В. Алексеенко

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» мая 2023 года, протокол № 04/23.