МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Радиофизический факультет
(факультет / институт / филиал)

УТВЕРЖДАЮ:

Декан _____ Матросов В.В.

«____» _____ 2017 г.

Рабочая программа дисциплины

Б1.Б27 Основы информационной безопасности
(наименование дисциплины (модуля))

Уровень высшего образования
бакалавриат
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
02.03.02 Фундаментальная информатика и информационные технологии
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Информационные системы и технологии
(указывается профиль / магистерская программа / специализация)

Квалификация (степень)
бакалавр
(бакалавр / магистр / специалист)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород

2017 г.

1. Место и цели дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к дисциплинам базовой части основной профессиональной образовательной программы по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии», преподается в 8 семестре.

Изучение студентами дисциплины «Основы информационной безопасности» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Компьютерные сети», «Архитектура вычислительных систем», «Операционные системы».

Цели освоения дисциплины

Содержание дисциплины направлено на ознакомления студентов с основными законодательные и нормативные документы в области защиты информации, моделями и механизмами реализации политики безопасности автоматизированных систем обработки информации (АСОИ).

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Формируемые компетенции (Код компетенции, этап формирования)	**Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций**
ОПК-3. Способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям. (Этап формирования базовый)	З1 (ОПК-3). Знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России. В1 (ОПК-3). Владеть навыками работы с нормативными правовыми актами. В2 (ОПК-3). Владеть профессиональной терминологией в области информационной безопасности.
ОПК-4. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. (Этап формироывания базовый)	З1 (ОПК-4). Знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих. З2 (ОПК-4). Знать источники и классификацию угроз информационной безопасности. У1 (ОПК-4). Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. У2 (ОПК-4). Уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. В1 (ОПК-4). Навыками работы с нормативными правовыми актами.

3. Структура и содержание дисциплины «Основы информационной безопасности»

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа, из которых 23 часа составляет контактная работа обучающегося с преподавателем (22 часа занятия лекционного типа, в том числе 2 часа – мероприятия текущего контроля успеваемости, 1 час – мероприятия промежуточной аттестации), 49 часов составляет самостоятельная работа обучающегося.

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. Нормативная база в области информационной безопасности	6	2			2	4
2. Основные понятия безопасности автоматизированных систем обработки информации (АСОИ)	10	4			4	6
3. Характеристики наиболее распространенных угроз безопасности АСОИ	16	4			4	12
4. Политика безопасности. Модели политики безопасности	19	4			4	15
5. Достоверная вычислительная база	12	4			4	8
6. Критерии оценки безопасности АСОИ	8	4			4	4
В т.ч. текущий контроль	2	2			2	
Промежуточная аттестация – **зачет**						

4. Образовательные технологии

Образовательные технологии, способствующие формированию компетенций.

***используемые на занятиях лекционного типа*:**

- лекции с изложением учебного материала;
- решение конкретных проблемных ситуаций в сфере информационной безопасности с использованием технологии коллективной мыслительной деятельности.

5. 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.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине, включающий:

6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.

Индикаторы компетенции	Критерии оценивания	
	«незачтено»	«зачтено»
Знания	Наличие грубых ошибок в основном материале	Знание основного материалом, возможно с рядом погрешностей
Умения	Наличие грубых ошибок при выполнении стандартных заданий	Способность выполнения всех стандартных заданий, возможно с незначительными погрешностями
Навыки	Отсутствие навыка	Достаточное владение навыком

6.2. Описание шкал оценивания.

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде зачета.

Критерии оценок.

Оценка	**Уровень подготовки**
Зачтено	В целом хорошая подготовка с возможными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы. Студент работал на лабораторных занятиях.
Не зачтено	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы.

6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.

Для оценивания результатов обучения в виде **знаний** используются следующие процедуры и технологии:

Зачет, проводимый в письменной форме с дальнейшим индивидуальным собеседованием.

Для оценивания результатов обучения в виде **умений** и **навыков** используются следующие процедуры и технологии:

Проверка отчета, составляемого по результатам выполнения заданий лабораторного практикума.

6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

Типовые задания для текущего контроля успеваемости.

6.4.1. Задачи для оценки компетенции «ОПК-4»:
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.

6.4.2. Задания для оценки компетенции «ОПК-3»:
Задача 1. Реализовать политику разграничения доступа «Конфиденциальное делопроизводство» для двух пользователей Userl и User2 с домашними каталогами D:\U1 и D:\U2.
Задача 2. Разработать набор испытаний реализации правил разграничения доступа из задания 1.
Задача 3. Исследовать содержимое журналов комплекса «Аккорд». Выделить в них сеансы работы всех пользователей системы. Детально описать один сеанс любого пользователя.

Типовые задания (оценочные средства), выносимые на зачет.

6.4.3. Задания для оценки компетенции «ОПК-3»:
1. Основные понятия безопасности АСОИ
2. Классификация угроз информационной безопасности
3. Система документов США. Классы защищенности компьютерных систем МО США. Европейские критерии безопасности
4. 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"
5. Закон Российской Федерации №63-ФЗ "Об электронной подписи"
6. Закон Российской Федерации №152-ФЗ "О персональных данных"

6.4.4. Задания для оценки компетенции «ОПК-4»:
1. Характеристики наиболее распространенных угроз безопасности
2. Вредоносные программы
3. Избирательная политика безопасности
4. Полномочная политика безопасности.
5. Достоверная вычислительная база
6. Идентификация, аутентификация и авторизация субъектов и объектов системы
7. Контроль входа пользователя в систему и управление паролями
8. Регистрация и протоколирование. Аудит
9. Контроль целостности субъектов.

10. Практическое внедрение электронной цифровой подписи
11. Принципы и мероприятия обеспечения информационной безопасности при обработке персональных данных

6.5. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утверждённое приказом ректора ННГУ от 13.02.2014 г. №55-ОД.

Положение «О фонде оценочных средств», утвержденное приказом ректора ННГУ от 10.06.2015 г. №247-ОД.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. - Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001. - 376 с.
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"
3. Малюк А. А., Пазизин С. В., Погожин Н. С - Введение в защиту информации в автоматизированных системах: учеб. пособие. - М.: Горячая линия - Телеком, 2001. - 148 с.

б) дополнительная литература:

1. Садердинов А. А., Трайнев В. А., Федулов А. А. - Информационная безопасность предприятия: учеб. пособие. - М.: Изд.-торговая корпорация "Дашков и К", 2005. - 336 с.
2. 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.
3. Технологии электронных коммуникаций. Т. 45. - М.: Россия, 1993. - 120 с.
4. Барсуков В.С. - Безопасность: технологии, средства, услуги. - М.: КУДИЦ-Образ, 2001. - 496 с.
5. Гайдамакин Н. А. - Разграничение доступа к информации в компьютерных системах. - Екатеринбург: Изд-во Урал. ун-та, 2003. - 328 с.

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/)

8. Материально-техническое обеспечение дисциплины

Аудиторный фонд ННГУ для проведения лекций.
Компьютерные класс лаборатории «Средств коммуникаций и безопасности информационных систем».

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии».

Автор (ы) _____ Л.Ю. Ротков

_____А.А. Горбунов

Рецензент _____ С.Н. Жуков

Заведующий кафедрой «Безопасность информационных систем» _____Л.Ю. Ротков

Программа одобрена на заседании методической комиссии Радиофизического факультета. Протокол № 04/17 от «30» августа 2017 года.