

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)

УТВЕРЖДАЮ:

Декан _____ Матросов В.В.

« 29 » _____ июня 2020 г.

Рабочая программа дисциплины

Б1.Б.28 Программно-аппаратные средства
обеспечения информационной безопасности

(наименование дисциплины (модуля))

Уровень высшего образования

специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

10.05.02 Информационная безопасность телекоммуникационных систем

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

(указывается профиль / магистерская программа / специализация)

Квалификация (степень)

специалист

(бакалавр / магистр / специалист)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2018

1. Место и цели дисциплины в структуре ОПОП

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» относится к дисциплинам базовой части основной профессиональной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», преподается в 9 семестре.

Изучение студентами дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Сети и системы передачи информации», «Архитектура вычислительных систем», «Операционные системы», «Основы информационной безопасности».

Целями освоения дисциплины являются:

Содержание дисциплины направлено на:

- ознакомление студентов с основными законодательными и нормативными документами в области защиты информации (в т.ч. с использованием криптографических методов);
- получение практических навыков в работе со средствами криптографической защиты информации.

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

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-7. Способность применять нормативные правовые акты в своей профессиональной деятельности. (этап освоения: базовый, завершающий)	31 (ОПК-7). Основные положения доктрины информационной безопасности РФ, нормативно-правовых актов в части касающейся средств криптографической защиты информации. В1 (ОПК-7). Навыками работы с нормативно-правовыми актами. В2 (ОПК-7). Профессиональной терминологией в области информационной безопасности.
ПК-1. Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем. (этап освоения: базовый)	31 (ПК-1). Источники угроз информационной безопасности и методы их нейтрализации. У1 (ПК-1). Оценивать угрозы информационной безопасности для объекта информатизации. У2 (ПК-1). Получать информацию из открытых источников о существующих и перспективных разработках в части средств криптографической защиты информации. В1 (ПК-1). Навыками работы с технической и эксплуатационной документацией.

3. Структура и содержание дисциплины «Программно-аппаратные средства обеспечения информационной безопасности»

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из которых 65 часов составляет контактная работа обучающегося с преподавателем (32 часа занятия лекционного типа, 32 часа лабораторные работы, в том числе 2 часа – мероприятия текущего контроля успеваемости, 1 час – мероприятия промежуточной аттестации), 43 часа 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.	30	16			16	14
2. Средства криптографической защиты информации.	77	16		32	48	29
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.

используемые на занятиях практического типа:

- 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 «Организация юридически значимого электронного документооборота с использованием электронной подписи». Контроль за процессом усвоения материала осуществляется с помощью контрольных вопросов.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), 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»
<u>Знания</u>	Наличие грубых ошибок в основном материале	Знание основного материалом, возможно с рядом погрешностей
<u>Умения</u>	Наличие грубых ошибок при выполнении стандартных заданий	Способность выполнения всех стандартных заданий, возможно с незначительными погрешностями
<u>Навыки</u>	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.
Незачтено	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-7»:

1. Указать порядок получения лицензии на работу с шифровальными (криптографическими) средствами.
2. Перечислить перечень документов, необходимый для получения лицензии на работу с шифровальными (криптографическими средствами).
3. Перечислить и кратко указать содержание нормативно-правовых документов, регламентирующих работу удостоверяющего центра.

Типовые задания (оценочные средства), выносимые на зачет.

6.4.2. Задания для оценки компетенции «ОПК-7»:

1. «Стратегия национальной безопасности Российской Федерации до 2020г», утвержденная указом Президента Российской Федерации от 12.05.2009 № 537.
2. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи".
3. Федеральный закон «О лицензировании отдельных видов деятельности» от 4.05.2011 № 99-ФЗ.
4. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313.
5. Кодекс РФ «Об административных правонарушениях», статьи 13.12, 13.13.
6. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
7. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
8. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

6.4.3. Задания для оценки компетенции «ПК-1»:

1. Классификация шифров.
2. Сервисы безопасности Рекомендаций X.800.
3. Некриптографические механизмы безопасности.
4. Криптографические механизмы безопасности.
5. Основные системы, в которых применяется РКІ.
6. Основные компоненты РКІ.
7. Сервисы РКІ.

8. Архитектуры PKI. Взаимодействие компонентов PKI.
9. Функции PKI.
10. Жизненный цикл сертификата.

6.5. Методические материалы, определяющие процедуры оценивания.

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

Положение о фонде оценочных средств, утвержденное приказом ректора ННГУ от 10.06.2015 №247-ОД.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Лукацкий А.В. Обнаружение атак. 2003 г.

б) дополнительная литература:

1. «Стратегия национальной безопасности Российской Федерации до 2020г», утвержденная указом Президента Российской Федерации от 12.05.2009 № 537.
2. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи".
3. Федеральный закон «О лицензировании отдельных видов деятельности» от 4.05.2011 № 99-ФЗ.
4. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313.
5. Кодекс РФ «Об административных правонарушениях», статьи 13.12, 13.13.
6. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
7. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
8. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
9. Документация по использованию КриптоПро УЦ.

в) программное обеспечение и Интернет-ресурсы:

1. <https://www.cryptopro.ru/support/docs>
2. <https://msdn.microsoft.com/ru-ru/>

8. Материально-техническое обеспечение дисциплины

Аудиторный фонд ННГУ для проведения лекций.

Компьютерные класс лаборатории «Средства коммуникаций и безопасность информационных систем».

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ С.В.Калинин
_____ Д.В.Демьяненко

Рецензент (ы) _____ С.Н.Жуков

Заведующий кафедрой _____ Л.Ю.Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» июня 2020 года, протокол № 03/20.