МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности
(название кафедры)

Добржинский Ю.В.
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (РПД)
«Криптографические методы защиты информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки очная

курс 4 семестр 7
лекции 34 час.
практические занятия не предусмотрено
лабораторные работы 26 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 60 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 66 час.
в том числе на подготовку к экзамену 54 час.
контрольные работы (количество) не предусмотрено
курсовая работа / курсовой проект не предусмотрено
зачет не предусмотрен
экзамен 7 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол 10 о « 15 » июня 2019 г.
№ ____ т ____ _____

И.о. заведующего кафедрой : Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Корнюшин П.Н., д.ф.-м.н., профессор

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации»

Рабочая программа по курсу «Криптографические методы защиты информации» разработана для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность».

Общая трудоемкость освоения дисциплины составляет 180 часов (5з.е.). Учебным планом предусмотрены лекционные занятия (34 час.), лабораторные работы (26 час.), самостоятельная работа студентов (66 час.), контроль качества обучения студентов (54 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

В настоящем учебном пособии представлен учебно-методический материал по организации аудиторных занятий и самостоятельной работы студентов, а также различные виды тестовых заданий в полном соответствии с программой этого курса для студентов данной специальности.

Цели: ознакомление студентов с основными принципами и методами, применяемыми при синтезе и анализе криптосистем.

Задачи:

- дать студентам представление о наиболее известных криптоалгоритмах с симметричным и асимметричным ключом, о функциях хэширования;

- ознакомление студентов с универсальными методами криптоанализа и условиями их применения;

- обучить студентов методам криптографических алгоритмов и криптографических параметров, обеспечивающих необходимую стойкость.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные, общепрофессиональные, профессионально-специализированные компетенции (элементы компетенций).

Код и формулировка	Этапы формирования компетенции

компетенции		
(ПК-1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает	основные криптопротоколы
	Умеет	применять полученные знания к исследованию простых шифров
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ПК-12) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает	основные методы анализа и синтеза криптоалгоритмов
	Умеет	решать основные задачи на применение криптографических алгоритмов в области защиты информации
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ПК-15) способностью разрабатывать планы и программы проведения научных исследований и технических разработок	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ОПК-7) способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает	угрозы безопасности информации и возможные пути их реализации
	Умеет	определять информационные ресурсы, подлежащие защите
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации
(ПСК-3.3) способностью разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и	Знает	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации

технических средств, организовать внедрение и		

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические методы защиты информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Модуль 1. Введение в криптологию(криптографию). (4 час.)

Тема 1. Первые понятия криптологии. Этапы развития. (1 час.)

Тема 2. Некоторые поясняющие примеры из истории. (1 час.)

Тема 3. Теория информации в криптологии. (1 час.)

Тема 4. Теория сложности и криптология. (1 час.)

Модуль 2. Основные понятия и методы современной криптологии. (20 час.)

Тема 5. Криптографические протоколы. (2 час.)

Тема 6. Однонаправленная функция. (2 час.)

Тема 7. Открытое распределение ключей. Схема Диффи-Хеллмана. (2 час.)

Тема 8. Односторонняя функция с секретом. (2 час.)

Тема 9. Открытое шифрование, криптосистема с открытым ключом. (2 час.)

Тема 10. Криптосистема RSA. (2 час.)

Тема 11. Цифровая подпись. (2 час.)

Тема 12. Схема цифровой подписи Эль Гамаля. (2 час.)

Тема 13. Управление ключами. (2 час.)

Тема 14. Криптографические хэш-функции. Аутентификация. (2 час.)

Модуль 3. Стандартизация криптографических методов (10 час.)

Тема 15. Организации, разрабатывающие стандарты по криптологии. (2 час.)

Тема 16. Первые варианты стандартов цифровой подписи США и России. (2 час.)

Тема 17. Развитие американских стандартов хэш-функции. (2 час.)

Тема 18. Российский стандарт хэш-функции ГОСТ Р 34.11-94. (2 час.)

Тема 19. Использование эллиптических кривых в криптологии. Новые стандарты цифровой подписи. (2 час.)

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (26 час.)

Лабораторная работа № 1. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. (2 часа)

Лабораторная работа № 2. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. (2 часа)

Лабораторная работа № 3. Изучение устройства и принципа работы шифровальной машины Энигма. (4 часа)

Лабораторная работа № 4. Стандарт симметричного шифрования AES RIJNDAEL. (4 часа)

Лабораторная работа № 5. Генерация простых чисел, используемых в асимметричных системах шифрования. (4 часа)

Лабораторная работа № 6. Электронная цифровая подпись. (4 часа)

Лабораторная работа № 7. Шифрование методом скользящей перестановки. (2 часа)

Лабораторная работа № 8. Изучение программных продуктов защиты информации. Программа PGP (Pretty Good Privacy). (2 часа)

Лабораторная работа № 9. Шифр Плейфера. (2 часа)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические методы защиты информации» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Модуль 1. Введение в криптологию(криптография).	ПК-1 ПК-2 ПК-12 ПК-15 ОПК-7 ПСК-3.2	Знает	ПР-6	1-5
			Умеет	ПР-6	1-5
			Владеет	ПР-6	1-5
2	Модуль 2. Основные понятия и методы современной криптологии.	ПК-1 ПК-2 ПК-12 ПК-15 ОПК-7 ПСК-3.2	Знает	ПР-6	6-15
			Умеет	ПР-6	6-15
			Владеет	ПР-6	6-15
3	Модуль 3. Стандартизация криптографических методов.	ПК-1 ПК-2 ПК-12 ПК-15 ОПК-7 ПСК-3.2	Знает	ПР-6	16-22
			Умеет	ПР-6	16-22
			Владеет	ПР-6	16-22

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Орлов, В.А. Теория чисел в криптографии [Электронный ресурс]: учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева. — Электрон. дан. — Москва: МГТУ им. Н.Э. Баумана, 2011. — 223 с. — Режим доступа: https://e.lanbook.com/book/106532.

2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва: Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192.

3. Панкратова, И.А. Булевы функции в криптографии [Электронный ресурс]: учебное пособие / И.А. Панкратова. — Электрон. дан. — Томск: ТГУ, 2014. — 88 с. — Режим доступа: https://e.lanbook.com/book/76702.

4. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс]: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза: ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755.

Дополнительная литература

(печатные и электронные издания)

1. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс]: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза:

ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755.
2. Боровков А.А. Математическая статистика. М.: «Наука», 1984.

2. Туганбаев, А.А. Теория вероятностей и математическая статистика [Электронный ресурс]: учебное пособие / А.А. Туганбаев, В.Г. Крупин. — Электрон. дан. — Санкт-Петербург: Лань, 2011. — 320 с. — Режим доступа: https://e.lanbook.com/book/652.

3. Боровков, А.А. Математическая статистика [Электронный ресурс]: учебник / А.А. Боровков. — Электрон. дан. — Санкт-Петербург: Лань, 2010. — 704 с. — Режим доступа: https://e.lanbook.com/book/3810.

4. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений [Электронный ресурс] / Е.Г. Кукина, В.А. Романьков. — Электрон. дан. — Омск: ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394

5. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 152 с. – Режим доступа: https://elib.dvfu.ru/vital/access/manager/Repository/fefu:5176

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Сайт СГЮА (www.ssla.ru).

2. Информационная система «Сетевой учебно-методический массив академии» (ИС СУММА)

3. кафедры информатики СГЮА на сервере [Электронный ресурс], 2011. Электронные

4. учебники, пособия, задания, тесты, контрольные работы.

5. Сайт "Эффективные системы безапасности" www.efsb.ru

6. Сайт "Защита от утечек корпоративной информации"

7. www.securion.ru

8. Сайт "Библиотека интернет индустрии"

9. www.i2r.ru

10. Страница крипто-новостей на сайте Санкт-петербургского университета

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения семинарского занятия. Работу с теоретическим материалом по теме с использованием учебника или конспекта лекций можно проводить по следующей схеме:

- название темы;
- цели и задачи изучения темы;
- основные вопросы темы;
- характеристика основных понятий и определений, необходимых для усвоения данной темы;
- список рекомендуемой литературы;

– наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.;

– краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

В ходе работы над теоретическим материалом достигается:

– понимание понятийного аппарата рассматриваемой темы;

– воспроизведение фактического материала;

– раскрытие причинно-следственных, временных и других связей;

– обобщение и систематизация знаний по теме.

При подготовке к экзамену рекомендуется проработать вопросы, рассмотренные на лекционных и практических занятиях и представленные в рабочей программе, используя основную литературу, дополнительную литературу и интернет-ресурсы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная

Приложение 1 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Криптографические методы защиты информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	10 неделя	Изучение теоретического курса.	28	ПР-6
2	17 неделя	Решение задач по заданию (индивидуальному где требуется) преподавателя	38	ПР-6
3	19 неделя	экзамен	54	УО-1

Самостоятельная работа студентов включает:

- освоение лекционного материала;
- выполнение индивидуального домашнего задания;
- оформление выполненного индивидуального домашнего задания;
- подготовку к защите выполненного индивидуального домашнего задания.

Изучение теоретического курса – выполняется самостоятельно каждым студентом по итогам каждой из лекций, результаты контролируются преподавателем на лекционных занятиях, используются конспект (электронный) лекций, учебники, рекомендуемые данной программой.

Решение задач по заданию (индивидуальному где требуется) преподавателя – решаются задачи, выданные преподавателем по итогам лекционных занятий и сдаются в конце семестра, используются конспект (электронный) лекций, учебники, рекомендуемые данной программой, а также сборники задач, включая электронные.

Приложение 2 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Криптографические методы защиты информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Обучающиеся должны выполнять индивидуальные задания. Задания должны быть выполнены в процессе изучения соответствующего раздела курса. При выполнении заданий возможно использование учебно-методической литературы и электронных лекций курса.

Вопросы к экзамену

1. Основные понятия и определения криптографии
2. Криптография и криптоанализ
3. Принципы криптографической защиты информации
3. Шифры перестановок
4. Шифры простой замены
5. Шифры сложной замены
6. Шифрование методом гаммирования
7. Современные симметричные криптосистемы
8. Американский стандарт DES
9. Американский стандарт AES
10. Отечественный стандарт шифрования
11. Блочные и поточные шифры
12. Асимметричные криптосистемы
13. Концепция двухключевой схемы. Однонаправленные функции
14. Криптосистема RSA
15. Комбинированный метод шифрования
16. Идентификация и проверка подлинности
17. Идентификация и проверка подлинности
18. Взаимная проверка подлинности
19. Протоколы идентификации с нулевой передачей знаний
20. Проблема аутентификации данных
21. Однонаправленные хеш функции
22. Алгоритмы электронной цифровой подписи
23. Федеральный закон РФ № 63-ФЗ "Об электронной подписи"
24. Управление криптографическими ключами