Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
**Б1.В.ДВ.01.02.0 «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»**

| | |
|---|---|
| Направление подготовки | 44.03.04 Профессиональное обучение (по отраслям) |
| Профиль программы | «Информационные технологии (по элективным модулям*)» |


| | | |
|---|---|---|
| Автор(ы): | ст. преп. | С.В. Ченушкина |
| | ст. преп. | Т.П. Телепова |


Одобрена на заседании кафедры информационных систем и технологий. Протокол от «20» января 2022 г. №5.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ИПО РГППУ. Протокол от «26» января 2022 г. №6.




Екатеринбург
2022

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Криптографические методы защиты информации»: изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике; знакомство с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью.

Задачи:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- изучить математические методы, используемых в криптографии;
- изучить основные алгоритмы симметричного и асимметричного шифрования;

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Криптографические методы защиты информации» относится к формируемой участниками образовательных отношений части учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Математика.
2. Прикладная математика и математическая логика.

Перечень учебных дисциплин, для которых необходимы знания, умения и владения, формируемые данной учебной дисциплиной:

1. Программные средства защиты информации.
2. Компьютерные коммуникации и сети.
3. Соадминистрирование баз данных и серверов.

## 3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ПКС-2.2 Способен обеспечить бесперебойную работу средств связи сетей электросвязи (СССЭ), а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа (НСД).

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:
З1. Основные термины и понятия криптографии;
З2. Требования к шифрам и их основные характеристики;
З3. Классификацию шифров;
З4. Типовые шифры замены и перестановки;
З5. Принципы построения современных криптосистем;
З6. Типовые поточные и блочные шифры;
З7. Системы шифрования с открытыми ключами;
З8. Возможности криптографии в решении задач аутентификации;
З9. Методы построения цифровой подписи.

Уметь:
У1. Выполнять шифрование и дешифрование с помощью различных криптоалгоритмов;
У2. Осуществлять программирование используемых алгоритмов;
У3. Проводить математическую проверку стойкости шифра.

Владеть:
В1. Методами криптографической защиты информации;
В2. Способами построения типовых криптографических алгоритмов;
В3. Основными понятиями криптографии.

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### *4.1 Объем дисциплины и виды контактной и самостоятельной работы*

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 час.), семестр изучения – 5, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

| Вид работы | Форма обучения |
|---|---|
| | очная |
| | Семестр изучения |
| | 5 сем. |
| | Кол-во часов |
| Общая трудоемкость дисциплины по учебному плану | 108 |
| Контактная работа, в том числе: | 34 |
| Лекции | 8 |
| Лабораторные работы | 26 |
| Самостоятельная работа студента | 74 |
| Промежуточная аттестация, в том числе: | |

| | |
|---|---|
| Экзамен | 5 сем. |

**Распределение трудоемкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*

### *4.2 Содержание и тематическое планирование дисциплины*

Таблица 2. Тематический план дисциплины

| Наименование разделов и тем дисциплины (модуля) | Сем. | Всего, час. | Вид контактной работы, час. | | | СРС |
|---|---|---|---|---|---|---|
| | | | Лекции | Практ. занятия | Лаб. работы | |
| 1. Основные термины и понятия | 5 | 16 | 2 | - | 2 | 12 |
| 2. Требования к криптосистемам. Классификация методов криптографического шифрования информации | 5 | 16 | 2 | - | 4 | 10 |
| 3. Симметричные методы шифрования | 5 | 21 | 1 | - | 6 | 14 |
| 4. Блочные симметричные шифросистемы | 5 | 17 | 1 | - | 4 | 12 |
| 5. Поточное шифрование | 5 | 17 | 1 | - | 4 | 12 |
| 6. Ассиметричные методы шифрования | 5 | 21 | 1 | - | 6 | 14 |

**Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

### *4.3 Содержание разделов (тем) дисциплин*

**Раздел 1. Основные термины и понятия**

Понятие криптографии, конфиденциальность, целостность, аутентификация, шифр, ключи зашифрования и расшифрования, симметричные и ассиметричные криптосистемы, расшифрование, дешифрование, цифровая подпись

**Раздел 2. Требования к криптосистемам. Классификация методов криптографического шифрования информации**

По типу ключей: симметричные криптоалгоритмы; асимметричные криптоалгоритмы; по размеру блока информации: потоковые шифры; блочные шифры; по характеру воздействий, производимых над данными: метод замены (перестановки), метод подстановки; аналитические методы, аддитивные методы (гаммирование), комбинированные методы

### Раздел 3. Симметричные методы шифрования

Понятие, базовые симметричные криптосистемы: шифры замены (подстановки), шифр сдвига, шифры Цезаря и Вижинера, шифры перестановок

### Раздел 4. Блочные симметричные шифросистемы

Понятие, шифр Фейстеля, стандарты шифрования, алгоритм шифрования DES (раунды, генерация ключей), проблемы ключей DES, режимы работы DES, понятие идеально стойкого криптоалгоритма, шифр AES, безопасность AES, вопросы реализации и применения AES

### Раздел 5. Поточное шифрование

Стандартный способ генерирования потока битов (регистра сдвига с линейной обратной связью), шифр RC4.

### Раздел 6. Ассиметричные методы шифрования

Принципы, формирование ключей, шифрование/дешифрование, криптографическая система RSA

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Традиционные образовательные технологии, которые ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

2. Для поддержки самостоятельной работы обучающихся использованы информационно-коммуникационные образовательные технологии, в частности, облачные технологии, электронная информационно-образовательная среда (ЭИОС), электронные средства обучения и электронно-библиотечные системы. При этом результативность организации самостоятельной работы обучающихся существенно повышается за счет доступности материалов, упорядоченности работ и возможности получения консультации преподавателя.

3. Технология обучения в сотрудничестве применяются при проведении семинарских, практических и лабораторных занятий, нацелены на совместную работу в командах или группах и достижение качественного образовательного результата.

4. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли

занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

### *6.1 Основная литература*

1. Торстейнсон, П. Криптография и безопасность в технологии. NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш. — Электрон. дан. — Москва : Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: https://e.lanbook.com/book/70724. — Загл. с экрана.

2. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 c. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html.— ЭБС «IPRbooks»

3. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 c. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html.— ЭБС «IPRbooks»

### *6.2 Дополнительная литература*

1. Рябко, Б.Я. Криптографические методы защиты информации [Электронный ресурс] : учеб. пособие / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 229 с. — Режим доступа: https://e.lanbook.com/book/5193. — Загл. с экрана.

2. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет

Информационных Технологий (ИНТУИТ), 2016. — 282 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52158.html.— ЭБС «IPRbooks»

3. 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. — Загл. с экрана.

4. Масленников М. Практическая криптография / М. Масленников. - Санкт-Петербург : БХВ-Петербург, 2015. - 465 с. - ISBN 5-94157-201-8. - URL: https://ibooks.ru/bookshelf/335092/reading

5. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 232 с. — Режим доступа: https://e.lanbook.com/book/63244. — Загл. с экрана.

### *6.3 Программное обеспечение и Интернет-ресурсы*

Программное обеспечение:

1. Операционная система Windows.
2. Офисная система Office Professional Plus.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».
2. Информационная система «Таймлайн».
3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий лекционного типа.
2. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.
3. Компьютерный класс.
4. Помещения для самостоятельной работы.