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

**ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)**

«СОГЛАСОВАНО»
Руководитель ОП
_____ Добржинский Ю.В.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. директора департамента
_____ Боршевников А.Е.
«25» марта 2022 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
Теоретико-числовые методы в криптографии
**Специальность 10.05.01 Компьютерная безопасность**
(Математические методы защиты информации)
**Форма подготовки очная**

курс 3 семестр 5
лекции 32 час.
практические занятия 34 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 66 час.
в том числе с использованием МАО 22 час.
самостоятельная работа 78 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 5 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 5а от «15» февраля 2022 г.

И.о. директора департамента информационной безопасности Боршевников А.Е.
Составитель доц. Верещагина Е.А.

Владивосток

2022

**Оборотная сторона титульного листа РПД**

**I. Рабочая программа пересмотрена на заседании департамента**:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании департамента**:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**III. Рабочая программа пересмотрена на заседании департамента**:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**IV. Рабочая программа пересмотрена на заседании департамента**:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

**Цель:** формирование у обучающихся основ теории чисел и особенностей применения теоретико-числовых алгоритмов при построении криптографических систем.

**Задачи:**

- изучить основы теории чисел;
- изучить основы теории сложности алгоритмов;
- обозначить перспективы применения результатов теории чисел в криптографической защите информации.

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют формирование следующих компетенций:

| **Наименование категории (группы) общепрофессиональных компетенций** | **Код и наименование профессиональной компетенции (результат освоения)** | **Код и наименование индикатора достижения компетенции** |
|---|---|---|
| | ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.1 Использует зарубежные и российские криптографические стандарты<br>ОПК-10.2 Применяет криптографические алгоритмы на практике при решении задач криптографическими методами<br>ОПК-10.3 Определяет подходы к разработке и анализу безопасности криптографических протоколов |

| **Код и наименование индикатора достижения компетенции** | **Наименование показателя оценивания (результата обучения)** |
|---|---|
| ОПК-10.1 Использует зарубежные и российские криптографические стандарты | Знает базовые понятия теории эллиптических кривых протоколов<br>Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях<br>Владеет навыками эффективного вычисления в кольцах |

| Код и наименование индикатора достижения компетенции | Наименование показателя оценивания (результата обучения) |
|---|---|
| | вычетов и в кольцах многочленов |
| ОПК-10.2 Применяет криптографические алгоритмы на практике при решении задач криптографическими методами | Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах<br>Умеет оценивать теоретическую сложность применяемых алгоритмов Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел |
| ОПК-10.3 Определяет подходы к разработке и анализу безопасности криптографических протоколов | Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем<br>Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств<br>Владеет подходами к разработке и анализу безопасности криптографических протоколов |

## Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 4 зачётных единицы (144 академических часа).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине являются:

| Обозначение | Виды учебных занятий и работы обучающегося |
|---|---|
| Лек | Лекции |
| ПР | Практические занятия |
| СР | Самостоятельная работа обучающегося в период теоретического обучения |
| Контроль | Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации |

## Структура дисциплины:

Форма обучения – очная.

| № | Наименование раздела дисциплины | Семестр | Количество часов по видам учебных занятий и работы обучающегося | | | | | | Формы промежуточной аттестации, текущего контроля успеваемости |
|---|---|---|---|---|---|---|---|---|---|
| | | | Лек | Лаб | Пр | ОК | СР | Контроль | |
| 1 | Элементы теории чисел | 5 | 16 | | 34 | | 24 | 54 | экзамен |
| 2 | Криптография с открытым ключом | 5 | 16 | | | | | | |
| | Итого: | | 32 | | 34 | | 24 | 54 | |

## I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

**Раздел 1. Элементы теории чисел**

Основы теории чисел. Простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Алгоритм Евклида. Применение результатов теории чисел в криптографической защите информации.

**Раздел 2. Криптография с открытым ключом**

Односторонние функции. Задача дискретного логарифмирования. Быстрый алгоритм возведения в степень и его сложность. Системы с открытым ключом. Криптографические протоколы. Общие методы взлома систем с открытым ключом. Блоковые и потоковые шифры.

## II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

### Практические занятия

**Практическая работа 1. Элементы теории чисел**

Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Алгоритм Евклида. Обобщенный алгоритм Евклида и решение диофантова уравнения. Нахождение инверсий по заданному модулю.

**Практическая работа 2. Основы криптографии с открытым ключом**

Задача хранения паролей в компьютере. Система «свой – чужой» в авиации. Задача, возникающая в сетях с удаленным доступом.

Система Диффи-Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Односторонняя функция с лазейкой и шифр RSA.

«Шаг младенца, шаг великана». Теоретико-числовые алгоритмы. Алгоритм исчисления порядка.

**Практическая работа 3. Блоковые шифры. Потоковые шифры.**

Режимы функционирования блоковых шифров: ECB, CBC, OFB, CTR. Сеть Фейстеля. Шифры DES, ГОСТ, AES. Криптоанализ блоковых шифров. Сценарии атак на шифры. Основные атаки на блоковые шифры: линейный и дифференциальный криптоанализ. Связь блоковых шифров и генераторов

псевдослучайных чисел.

Криптографически стойкие генераторы псевдослучайных чисел и потоковые шифры. Классификация потоковых шифров. Основные потоковые шифры.

**Практическая работа 4. Криптографические хеш-функции**

Принципы построения и современные требования к хеш-функциям. Применение хешфункций в криптографии. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блоковых шифрах.

## III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине включает в себя план-график выполнения самостоятельной работы по дисциплине.

**План-график выполнения самостоятельной работы по дисциплине**

| № п/п | Дата/сроки выполнения | Вид самостоятельной работы | Примерные нормы времени на выполнение | Форма контроля |
|---|---|---|---|---|
| 1 | В течение семестра | Работа с литературой. Подготовка к практическим занятиям. | 24 | ПР-6 |
| 2 | В течение семестра | Подготовка к экзамену | 54 | экзамен |

### Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями,

научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем.

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

## IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

| № п/п | Контролируемые разделы / темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Элементы теории чисел<br>Элементы теории чисел | ОПК-10.1<br>ОПК-10.2<br>ОПК-10.3 | знает | ПР-6 ПР-7 | экзамен |
| | | | умеет | ПР-6 | |
| | | | владеет | ПР-6 | |
| 2 | Криптография с открытым ключом | ОПК-10.1<br>ОПК-10.2<br>ОПК-10.3 | знает | ПР-6 ПР-7 | экзамен |
| | | | умеет | ПР-6 | |
| | | | владеет | ПР-6 | |

## V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература

1. Райтман, М.А. Искусство легального, анонимного и безопасного доступа к ресурсам интернета: учебное пособие. - СПб: БХВ-Петербург, 2016. - 624 с. - Режим доступа: http://znanium.com/catalog/product/944786

2. Смирнова, Е.И. Введение в проектную деятельность. Синергетический подход / И.В. Кузнецова [и др.].— Электрон. текстовые данные.— Саратов: Вузовское образование, 2020.— 166 с.— Режим доступа: http://www.iprbookshop.ru/92644.html

3. Титова, Л.Н. Куратор информационных ресурсов / Титова Л.Н., Жилко Е.П., Миниярова Л.В.— Саратов: Вузовское образование, 2017.— 166 с.— Режим доступа: http://www.iprbookshop.ru/71734.html

4. Томас, Д. Логическое проектирование на SystemVerylog / Д. Томас. — Москва: ДМК Пресс, 2019. — 384 с. Режим доступа: https://e.lanbook.com/book/131680

**Дополнительная литература**

1. Эффективное кодирование и цифровое представление изображений [Электронный ресурс]: практикум № 37/ — Электрон. текстовые данные. — Москва: Московский технический университет связи и информатики, 2014.— 19 с.— Режим доступа: http://www.iprbookshop.ru/61581.html

**Перечень информационных технологий и программного обеспечения**

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение: Microsoft Office (Access, Excel, PowerPoint, Word и т. д), Open Office, Skype, программное обеспечение электронного ресурса сайта ДВФУ, включая ЭБС ДВФУ.

## VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием рекомендуемых источников, материалов по практическим работам.

**Методические указания для подготовки к практическим занятиям**

*Структура отчета по практической работе*

Отчеты по работам представляются в электронной форме, подготовленные как текстовые документы в редакторе MSWord.

Отчет должен быть обобщающим документом, включать всю информацию по выполнению заданий, в том числе таблицы список литературы необходимыми пояснениями и иллюстрациями.

Структурно отчет по работе, как текстовый документ, комплектуется по следующей схеме:

✓ *Титульный лист – обязательная* компонента отчета, первая страница отчета, по принятой для лабораторных работ форме (титульный лист отчета должен размещаться в общем файле, где представлен текст отчета);

✓ *Исходные данные к выполнению заданий* – обязательная компонента отчета, с новой страницы, содержат указание варианта, темы и т.д.);

✓ *Основная часть* – материалы выполнения заданий, разбивается по рубрикам, соответствующих заданиям работы, с иерархической структурой: разделы – подразделы – пункты – подпункты и т. д.

Рекомендуется в основной части отчета заголовки рубрик (подрубрик) давать исходя из формулировок заданий, в форме отглагольных существительных;

✓ *Выводы* – обязательная компонента отчета, содержит обобщающие выводы по работе (какие задачи решены, оценка результатов, что освоено при выполнении работы);

✓ *Список литературы* – обязательная компонента отчета, с новой страницы, содержит список источников, использованных при выполнении работы, включая электронные источники (список нумерованный, в соответствии с правилами описания библиографии);

✓ *Приложения* – необязательная компонента отчета, с новой страницы, содержит дополнительные материалы к основной части отчета.

*Оформление отчета по практической работе*

Необходимо обратить внимание на следующие аспекты в оформлении отчетов работ:

- набор текста;
- структурирование работы;
- оформление заголовков всех видов (рубрик-подрубрик-пунктов-подпунктов, рисунков, таблиц, приложений);
- оформление перечислений (списков с нумерацией или маркировкой);

- оформление таблиц;
- оформление иллюстраций (графики, рисунки, фотографии, схемы, «скриншоты»);
- набор и оформление математических выражений (формул);
- оформление списков литературы (библиографических описаний) и ссылок на источники, цитирования.

*Набор текста*

Набор текста осуществляется на компьютере, в соответствии со следующими требованиями:

✓ печать – на одной стороне листа белой бумаги формата А4 (размер 210 на 297 мм.);

✓ интервал межстрочный – полуторный;

✓ шрифт – TimesNewRoman;

✓ размер шрифта – 14 пт., в том числе в заголовках (в таблицах допускается 10-12 пт.);

✓ выравнивание текста – «по ширине»;

✓ поля страницы – левое - 30 мм., правое - 10 мм., верхнее и нижнее - 20 мм.;

✓ нумерация страниц – в правом нижнем углу страницы (для страниц с книжной ориентацией), сквозная, от титульного листа до последней страницы, арабскими цифрами (первой страницей считается титульный лист, на котором номер не ставиться, на следующей странице проставляется цифра «2» и т. д.).

✓ режим автоматического переноса слов, за исключением титульного листа и заголовков всех уровней (перенос слов для отдельного абзаца блокируется средствами MSWord с помощью команды «Формат» – абзац при выборе опции «запретить автоматический перенос слов»).

Если рисунок или таблица размещены на листе формата больше А4, их следует учитывать, как одну страницу. Номер страницы в этих случаях допускается не проставлять.

Список литературы и все *приложения* включаются в общую сквозную нумерацию страниц работы.

## МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

# ДИСЦИПЛИНЫ

| Наименование специальных помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
|---|---|---|
| 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная, Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPProjectorPT-D2110XE | 1С Предприяти8 (8.2), 7-Zip, ABBYY Lingvo12,Alice 3, Anaconda3,Autodesk,CodeBlocks,CorelDRAW X7,Dia,Directum4.8,DosBox-0.74,Farmanager,Firebird 2.5,FlameRobin,Foxit Reader,Free Pascal,Geany,Ghostscript,Git,Greenfoot,gsview,Inscape0.91,Java,Java development Kit,Kaspersky,Lazarus,LibreOffice4.4,MatLab R2017b,Maxima 5.37.2,Microsoft Expression,Microsoft Office 2013,Microsoft Silverlight,Microsoft Silverlight 5SDK-русский,MicrosoftSistem Center,Microsoft Visial Studio 2012,MikTeX2.9,MySQL,NetBeans,Notepad++,Oracle VM VirtualBox,PascalABC.NET,PostgreSQL 9.4,PTC Mathcad,Putty,PyQt GPL v5.4.1 for Pythonv 3.4,Pyton2.7(3.4,3.6),QGIS Brighton,RStudio,SAM CoDeC Pack,SharePoint,Strawberry Perl,Tecnomatix,TeXnicCenter,TortoiseSVN,Unity2017.3.1f1, Veusz,Vim8.1,Visual Paradigm CE,Visual Studio2013,Windows Kits,Windows Phone SDK8.1,Xilinx Design ToolsAcrobat ReaderDC,AdobeBridge CS3,AdobeDeviceCentralCS3,Adobe ExtendScript Toolkit 2,Adobe Photoshope CS3,DVD-студия Windows,GoogleChrome,Internet Explorer,ITMOproctor,Mozilla Firefox, Visual Studio Installer,Windows Media Center, WinSCP, |
| 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус A, ауд. A1042 Аудитория для самостоятельной работы студентов | Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскопечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно- | Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0, Duxbury BrailleTranslator, Dolphin Guide (контракт № А238-14/2); Неисключительные права на использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ptt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к внутренней информационной системе документооборота и порталу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая портальные хранилища, используемой в ДВФУ: Microsoft SharePoint; - лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center. |

| | | |
|---|---|---|
| | речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой. | |

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

| Код и наименование индикатора достижения компетенции | Наименование показателя оценивания (результата обучения) |
|---|---|
| ОПК-10.1 Использует зарубежные и российские криптографические стандарты | Знает базовые понятия теории эллиптических кривых протоколов<br>Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях<br>Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов |
| ОПК-10.2 Применяет криптографические алгоритмы на практике при решении задач криптографическими методами | Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах<br>Умеет оценивать теоретическую сложность применяемых алгоритмов Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел |
| ОПК-10.3 Определяет подходы к разработке и анализу безопасности криптографических протоколов | Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем<br>Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств<br>Владеет подходами к разработке и анализу безопасности криптографических протоколов |

## Контроль достижения целей курса

| № п/п | Контролируемые разделы / темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Элементы теории чисел<br>Элементы теории чисел | ОПК-10.1<br>ОПК-10.2<br>ОПК-10.3 | знает | ПР-6 ПР-7 | экзамен |
| | | | умеет | ПР-6 | |
| | | | владеет | ПР-6 | |
| 2 | Криптография с открытым ключом | ОПК-10.1<br>ОПК-10.2<br>ОПК-10.3 | знает | ПР-6 ПР-7 | экзамен |
| | | | умеет | ПР-6 | |
| | | | владеет | ПР-6 | |

**Текущая аттестация**

**ПР-7 Конспект** - продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции.

Цели конспектирования состоят в:

- развитии умений систематизировать знания и выделять причинно-следственные связи, выявлять закономерности;
- развитии умений перерабатывать любую информацию, придавая ей иной вид, тип, форму;
- развитии навыков осмысленной переработки текста, структурирования информации, использования основных категорий анализа, работы с большими объемами информации;
- создании модели проблемы (понятийную или структурную).

**Требования к представлению и оцениванию материалов (результатов):**

В связи с объективным характером конспектирования не предлагается единых и обязательных параметров конспектируемого текста (степень сокращения информации). Объем законспектированного текста определяется самим студентом. Конспект должен быть подготовлен каждым студентом самостоятельно и отражать основные идеи изученной темы.

Перечень вопросов, необходимых для конспектирования определяется темой лекционного занятия. Конспекты выполняются во время лекционных занятий, и проверяются преподавателем в конце семестра.

***Критерии оценки:***

| Уровень освоения | Критерии оценки результатов обучения | Количество баллов / оценка |
|---|---|---|
| Повышенный | Конспекты лекций в наличии. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Логически корректное изложение материала. | 100-86<br>Зачтено |
| Базовый | Конспекты лекций в наличии. Студент показывает умение пользоваться концептуально-понятийным аппаратом. В целом логически корректное, но не всегда точное изложение материала. | 85-76<br>Зачтено |
| Пороговый | Конспекты лекций в наличии. Студент показывает затруднение с использованием научно-понятийного аппарата; частичные затруднения с выполнением конспекта. | 75-61<br>Зачтено |
| Уровень не достигнут | Конспекты лекций отсутствуют или студент показывает отрывочное представление о теме. | 60-0<br>Не зачтено |

**Практическая работа (ПР-6)** – средство для закрепления и практического освоения материала по определенной теме.

Цель практических работ – выработка у учащихся профессиональных умений применять полученные знания для решения практических задач, умений и навыков пользоваться подходами и методами информационной безопасности для осуществления профессиональной деятельности.

Обработка результатов и оформление отчета проводится в течение недели после выполнения работы. Студент, не сдавший отчета в срок, к следующей работе не допускается.

**Требования к представлению и оцениванию материалов (результатов):**

Выполнение практической работы осуществляется студентом самостоятельно в часы практических занятий.

При оценке работы студента преподаватель учитывает все этапы работы студента над отчетом. Если отчет не был принят преподавателем и возвращен для доработки, то все исправления вносятся в тот же экземпляр отчета.

При оценке учитывается правильность выполнения отчета. Выставляется дифференцированный зачет.

***Критерии оценки:***

| Уровень освоения | Критерии оценки результатов обучения | Количество баллов / оценка |
|---|---|---|
| Повышенный | Студент показал прочные знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в соответствии с требованиями, структурирован, не содержит ошибок; правильно и полно сформулирован вывод по работе. | 100 – 86<br>Зачтено<br>(отлично) |
| Базовый | Студент показал знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их | 85-76 |

| | | |
|---|---|---|
| | объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном – в соответствии с требованиями, структурирован; правильно и полно сформулирован вывод по работе. Допускаются не более 2-х недочетов в оформлении отчета. | Зачтено<br>(хорошо) |
| Пороговый | Студент показал базовые знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, демонстрирует, в целом, знание методов, используемых в работе, методики обработки результатов. При выполнении экспериментальной части работы и оформлении отчета студент в целом показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном в соответствии с требованиями, не содержит грубых ошибок, вывод по работе сформулирован. | 75-61<br>Зачтено<br>(удовлетворительно) |
| Уровень не достигнут | Студент не выполнил работу, либо показал незнание основных понятий, сущности процессов, рассматриваемых в работе, демонстрирует плохое знание или незнание методов, методики обработки результатов. Слабо сформировано или не сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками. | 60-0<br>Не зачтено<br>(неудовлетворительно) |

## Оценочные средства для промежуточной аттестации

### Вопросы на экзамен

1. Что такое односторонняя функция?
2. Что такое дискретное логарифмирование?
3. Описать алгоритм быстрого возведения в степень. Оценить его сложность.
4. Как решаются проблема хранения паролей и проблема ПВО с помощью односторонней функции?
5. Чем отличается криптосистема с открытым ключом от криптосистемы с секретным ключом?

6. Описать первую криптосистему с открытым ключом? Какие проблемы она позволяет решать?
7. Описать алгоритм Евклида и обобщенный алгоритм Евклида.
8. Дать определение инверсии.
9. Как вычислять инверсию, используя алгоритм Евклида?
10. Дать определение функции Эйлера и привести пример ее вычисления.
11. Описать алгоритм «Решето Эратосфена».
12. Описать методы дискретного логарифмирования. Оценить их сложность.
13. Как построить цифровую подпись на басе шифра RSA?
14. Как построить цифровую подпись на басе шифра Эль-Гамаля?

**Критерии выставления оценки студенту на экзамене:**

| Баллы (рейтинговой оценки) | Оценка (стандартная) | Требования к сформированным компетенциям |
|---|---|---|
| 86-100 | «отлично» | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. |
| 76-85 | «хорошо» | Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. |
| 61-75 | «удовлетворительно» | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. |
| 0-60 | «неудовлетворительно» | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без |

| | | |
|---|---|---|
| | | дополнительных занятий по соответствующей дисциплине. |

| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения по дисциплине** | | | | |
|---|---|---|---|---|
| Оценка / виды оценочных средств | 2 (не зачтено) | 3 (зачтено) | 4 (зачтено) | 5 (зачтено) |
| **Знания** *(виды оценочных средств: конспект, практическая работа)* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения** *(виды оценочных средств: практическая работа)* | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)** | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |