Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Оренбургский государственный университет»**

Кафедра информатики

# РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

*«Б.1.В.ДВ.5.1 Методы и средства защиты информации в информационных системах»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
*09.03.02 Информационные системы и технологии*
(код и наименование направления подготовки)

*Общий профиль*
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
*Программа академического бакалавриата*

Квалификация
*Бакалавр*

Форма обучения
*Очная*

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра информатики
*наименование кафедры*

протокол № 1 от "12" 02 2018 г.

Заведующий кафедрой
Кафедра информатики _____ М.А. Токарева
*наименование кафедры* *подпись* *расшифровка подписи*

*Исполнители:*
Доцент кафедры информатики _____ А.Н. Колобов
*должность* *подпись* *расшифровка подписи*

---

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.03.02 Информационные системы и технологии _____ М.А. Токарева
*код наименование* *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Гришай
*личная подпись* *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
*личная подпись* *расшифровка подписи*

---

№ регистрации _____

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины:

*формирование у студентов теоретических знаний по современным технологиям обеспечения информационной безопасности информационных систем, математическим и техническим средствам защиты информации при реализации информационных процессов, а также получение практических навыков программной реализации алгоритмов защиты данных.*

**Задачи:**

- *ознакомиться с направлениями развития технологий обеспечения информационной безопасности и правовыми основами защиты информации в информационных системах;*
- *изучить основные принципы и методы защиты информации в сети;*
- *овладеть навыками программной реализации алгоритмов защиты данных.*

## 2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.14 Теория информационных процессов и систем, Б.1.Б.21 Основы информационной безопасности*

Постреквизиты дисциплины: *Отсутствуют*

## 3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

| Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций | Формируемые компетенции |
|---|---|
| **Знать:** принципы функционирования основных программно-аппаратных средств обеспечения информационной безопасности, методы и средства защиты информации в процессе хранения и передачи по компьютерным сетям: классификация, функции; технологии криптографической защиты информации, технологии аутентификации, модели безопасности операционных систем;<br>**Уметь:** применять технологии криптографической защиты информации, технологии аутентификации для защиты информации в компьютерных системах, выбирать инструментальные средства и методы управления средствами сетевой безопасности, уметь применять сетевые сканеры для выявления уязвимостей компьютерных систем;<br>**Владеть:** методами аутентификации на основе паролей и PIN кодов, строгой аутентификации. | ОПК-4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защита государственной тайны |
| **Знать:** математические основы криптографических методов защиты информации; современные криптографические алгоритмы; способы обеспечения информационной безопасности компьютерных систем;<br>**Уметь:** разрабатывать компоненты средств защиты информации, реализующие криптографические методы защиты компьютерной информации;<br>**Владеть:** стандартными библиотеками объектно-ориентированного языка для реализации криптографических методов защиты информации. | ПК-12 способностью разрабатывать средства реализации информационных технологий (методические, информационные, математические, алгоритмические, технические и программные) |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 академических часов).

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 8 семестр | всего |
| **Общая трудоёмкость** | **144** | **144** |
| **Контактная работа:** | **56,25** | **56,25** |
| Лекции (Л) | 24 | 24 |
| Практические занятия (ПЗ) | 16 | 16 |
| Лабораторные работы (ЛР) | 16 | 16 |
| Промежуточная аттестация (зачет, экзамен) | 0,25 | 0,25 |
| **Самостоятельная работа:**<br>*- самостоятельное изучение разделов (разделы 1, 4);*<br>*- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;*<br>*- подготовка к лабораторным занятиям;*<br>*- подготовка к рубежному контролю и т.п.)* | **87,75** | **87,75** |
| **Вид итогового контроля (зачет, экзамен, дифференцированный зачет)** | **диф. зач.** | |

Разделы дисциплины, изучаемые в 8 семестре

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 1 | Введение. Проблемы безопасности информации. | 20 | 4 | 2 | 2 | 12 |
| 2 | Математические основы криптографии. Вычислительная. сложность Криптографические методы защиты информации. | 37 | 6 | 10 | 6 | 15 |
| 3 | Технологии аутентификации. | 34 | 5 | 2 | 4 | 23 |
| 4 | Протоколы защиты информации. | 27 | 5 | 2 | 2 | 18 |
| 5 | Программные средства защиты информации в компьютерных системах. | 26 | 4 | | 2 | 20 |
| | Итого: | 144 | 24 | 16 | 16 | 88 |
| | Всего: | 144 | 24 | 16 | 16 | 88 |

### 4.2 Содержание разделов дисциплины

**Раздела № 1 Введение. Проблемы безопасности информации**

*Основные понятия защиты информации и информационной безопасности. Анализ угроз безопасности информации. Современные тенденции в области обеспечения и нарушения безопасности информации. Стандарты и правовое обеспечение информационной безопасности.*

**Раздела № 2 Математические основы криптографии. Вычислительная. сложность Криптографические методы защиты информации**

*Арифметика остатков. Расширенный алгоритм Евклида. Теорема Лагранжа. Китайская теорема об остатках. Поиск простых чисел. Основы теории вычислительной сложности. Оценка сложности алгоритмов. Односторонние функции. Основные понятия криптографии, классификация*

*криптографических алгоритмов. Исторические шифры Стеганография. Шифры замены и перестановки. Потоковые шифры. Симметричные шифры. Ассиметричные шифры. Хэш-функция. Цифровая подпись. Управление криптографическими ключами.*

**Раздела № 3 Технологии аутентификации**

*Аутентификация, авторизация, администрирование. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация. Аппаратно-программные системы идентификации и аутентификации.*

**Раздела № 4 Протоколы защиты информации**

*Протоколы аутентификации. Протоколы обмена ключами. Шифрование сетевого трафика. Анализ протоколов распределения ключей. BAN –логика.*

**Раздела № 5 Программные средства защиты информации в компьютерных системах**

*Классификация. Антивирусы. Межсетевые экраны. VPN. Системы обнаружения вторжений.*

### 4.3 Лабораторные работы

| № ЛР | № раздела | Наименование лабораторных работ | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Стеганография. | 2 |
| 2 | 1 | Поиск десятизначных простых чисел. | 2 |
| 3 | 2 | Шифры замены и перестановки. | 2 |
| 4 | 2 | Симметричные шифры. | 2 |
| 5 | 2 | Ассиметричные шифры. | 2 |
| 6 | 3 | Реализация проверки подлинности. | 2 |
| 7 | 4 | Реализация протоколов защиты информации. | 2 |
| 8 | 5 | Анализ сетевого трафика | 2 |
| | | Итого: | 16 |

### 4.4 Практические занятия (семинары)

| № занятия | № раздела | Тема | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Современные тенденции в области обеспечения и нарушения безопасности информации. | 2 |
| 2-6 | 2 | Математические основы криптографии. | 10 |
| 7 | 3 | Технологии аутентификации. | 2 |
| 8 | 4 | Протоколы защиты информации. | 2 |
| | | Итого: | 16 |

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

*1. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - Москва : ДМК Пресс, 2014. - 702 с. : ил., табл., схем. - Библиогр. в кн. - ISBN 978-5-94074-768-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=260320*

*2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. - Москва : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=86475*

### 5.2 Дополнительная литература

*1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.:*

*ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: http://znanium.com/bookread2.php?book=402686*

*2. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова.- 6-е изд., стер. - Москва : Академия, 2012. - 332 с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5.*

### 5.3 Периодические издания

- Вестник компьютерных и информационных технологий: журнал. - Москва: Агентство "Роспечать", 2016 г.;
- Программирование: журнал. - М.: АРСМИ, 2014 г.;
- Программные продукты и системы: журнал. - Москва: Агентство "Роспечать", 2016 г.
- Хакер + DVD : журнал. - Москва : Агентство "Роспечать", 2013 г.

### 5.4 Интернет-ресурсы

- http://www.securitylab.ru/ - Информационный портал по ИТ безопасности;
- http://bezopasnik.org/article - Информационный сайт: Безопасник;
- http://window.edu.ru - Портал информационно-коммуникационных технологий в образовании;
- http://www.mon.gov.ru - Официальный сайт Министерства образования и науки РФ;
- http://www.edu.ru - Федеральный портал "Российское образование";
- http://fcior.edu.ru/ - Федеральный центр информационно-образовательных ресурсов
- http://catalog.iot.ru - Каталог образовательных ресурсов сети Интернет
- http://www.citforum.ru/ – Портал, содержащий не имеющую аналогов техническую библиотеку свободно доступных материалов по информационным технологиям на русском языке.

### 5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

- Операционная система Microsoft Windows;
- Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint);
- Среда программирования MS Visual Studio.

Свободнораспространяемое ПО:

1. Кросплатформенный офисный пакет программ,включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения, OpenOffice/LibreOffice
2. Свободно распространяемая интегрированная среда разработки Pascal ABC.NET.
3. Picasa – программа просмотра и редактирования цифровых изображений. Доступ бесплатный, разработчик: Google, режим доступа: http://www.picasa.com

Профессиональные базы данных, информационные справочные системы:

1. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания SpringerCustomerServiceCenterGmbH. – Режим доступа: https://link.springer.com/ в локальной сети ОГУ.
2. Большая советская энциклопедия [Электронный ресурс]: универсальная справочная энциклопедия международного уровня. – Режим доступа: https://bigenc.ru/ в локальной сети ОГУ.
3. Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Глосис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. – Электрон.дан. и прогр. – [Москва; Санкт-Петербург], [1999–2013]. – Режим доступа осуществляется в локальной сети ОГУ.
4. SCOPUS [Электронный ресурс] : реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ. WebofScience [Электронный ресурс]: реферативная база данных / компания ClarivateAnalytics. – Режим доступа: http://apps.webofknowledge.com/ в локальной сети ОГУ.

Springer [Электронный ресурс] : база данных научных книг, журналов, справочных материалов / компания SpringerCustomerServiceCenterGmbH. – Режим доступа :https://link.springer.com/в локальной сети ОГУ.

## 6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используются компьютерные классы оснащенные: комплектами ученической мебели, доской, компьютерами, подключенными к сети «Интернет» с обеспечением доступа в электронную информационно-образовательную среду ОГУ.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.