Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

# РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

*«Б1.Д.Б.22 Основы информационной безопасности»*

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
*10.05.01 Компьютерная безопасность*
(код и наименование специальности)

*специализация №3 «Разработка защищенного программного обеспечения»*
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
*Специалист по защите информации*

Форма обучения
*Очная*

Год набора 2021

Рабочая программа дисциплины «*Б1.Д.Б.22 Основы информационной безопасности*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
*наименование кафедры*

протокол № 10 от "21" 06 2021 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
*наименование кафедры* *подпись* И.В. Влацкая *расшифровка подписи*

*Исполнители:*
доцент *должность* *подпись* И.В. Влацкая *расшифровка подписи*

*должность* *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

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

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

№ регистрации 117856

© Влацкая И.В., 2021
© ОГУ, 2021

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины:

изучение комплекса проблем информационной безопасности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации.

**Задачи:**

овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

## 2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика, Б1.Д.Б.19 Операционные системы*

Постреквизиты дисциплины: *Б1.Д.Б.24 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.26 Основы построения защищенных компьютерных сетей, Б1.Д.Б.27 Основы построения защищенных баз данных, Б1.Д.Б.28 Защита программ и данных, Б1.Д.Б.31 Техническая защита информации, Б1.Д.Б.35 Защита информации от утечки по техническим каналам, Б1.Д.Б.36 Стандарты информационной безопасности, Б1.Д.В.2 Технология построения защищенных автоматизированных систем, Б1.Д.В.3 Защита информации в высокопроизводительных системах, Б1.Д.В.5 Управление программными проектами, Б2.П.Б.У.1 Ознакомительная практика, Б2.П.Б.П.1 Научно-исследовательская работа, Б2.П.В.П.1 Производственная практика (по специализации)*

## 3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | ОПК-1-В-1 Знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики | **Знать;**<br>– сущность и понятие информационной безопасности, характеристику ее составляющих;<br>– виды, источники и носители защищаемой информации;<br>– факторы, |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>**Уметь:**<br>– определять факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>**Владеть:**<br>– навыками определения источников угроз безопасности информации;<br>– владеть основными приемами предотвращения угроз безопасности. |
| ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | ОПК-5-В-2 Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России<br>ОПК-5-В-3 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации | **Знать:**<br>– место информационной безопасности в системе национальной безопасности страны;<br>– основы законодательства Российской Федерации;<br>– методические документы в обласим информационной безопасности;<br>– организацию защиты государственной тайны и конфиденциальной информации;<br>– правовую характеристику преступлений в области компьютерной информации;<br>– меры ответственности за разглашение защищаемой информации<br>**Уметь:**<br>– применять нормативные и прововые акты и |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | методические документы при проектировании средств защиты информации.<br>**Владеть:**<br>– навыками защиты конфиденциальной информации |
| ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ОПК-6-В-4 Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем<br>ОПК-6-В-5 Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем | **Знать:**<br>– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;<br>– современные средства и способы обеспечения информационной безопасности;<br>– основные методики анализа угроз и рисков информационной безопасности;<br>**Уметь:**<br>– разрабатывать модели угроз информационной безопасности; разрабатывать модели нарушителей информационной безопасности<br>**Владеть:**<br>– навыками построения модели угроз, модели нарушителя;<br>– навыками определения актуальных угроз информационной безопасности. |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 5 семестр | всего |

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 5 семестр | всего |
| **Общая трудоёмкость** | **108** | **108** |
| **Контактная работа:** | **68,25** | **68,25** |
| Лекции (Л) | 34 | 34 |
| Лабораторные работы (ЛР) | 34 | 34 |
| Промежуточная аттестация (зачет, экзамен) | 0,25 | 0,25 |
| **Самостоятельная работа:**<br>*- выполнение индивидуального творческого задания (ИТЗ);*<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.)* | **39,75** | **39,75** |
| **Вид итогового контроля (зачет, экзамен, дифференцированный зачет)** | **зачет** | |

Разделы дисциплины, изучаемые в 5 семестре

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 1 | Нормативно-правовая база обеспечения информационной безопасности | 12 | 4 | | 4 | 4 |
| 2 | Экономические аспекты информационной безопасности. Ответственность за нарушение требований в области информационной безопасности | 14 | 4 | | 4 | 6 |
| 3 | Модель нарушителя. Модели анализа угроз информационной безопасности | 22 | 6 | | 8 | 8 |
| 4 | Методы защиты информации | 22 | 8 | | 6 | 8 |
| 5 | Модели разграничения доступа к компьютерным системам | 20 | 6 | | 6 | 8 |
| 6 | Защита информации при межсетевом взаимодействии | 18 | 6 | | 6 | 6 |
| | Итого: | 108 | 34 | | 34 | 40 |
| | Всего: | 108 | 34 | | 34 | 40 |

**4.2 Содержание разделов дисциплины**

**1 Нормативно-правовая база обеспечения информационной безопасности**

Доктрина информационной безопасности Российской Федерации

Государственная система защиты информации

Защита информации ограниченного доступа

Нормативные акты ФСТЭК и ФСБ России.

**2 Экономические аспекты информационной безопасности. Ответственность за нарушение требований в области информационной безопасности.**

Критерии отнесения информации к защищаемой. Понятие и виды ущерба от НСД.

Понятие и виды ущерба от НСД. Система современного законодательства, регламентирующая вопросы защиты информации и ответственности за нарушение информационной безопасности.

**3 Модель нарушителя. Модели анализа угроз информационной безопасности**

Основные понятия и классификация угроз. Внешние и внутренние нарушители. Источники угроз. Анализ угроз информационной безопасности на сайте ФСТЭК.

**4 Методы защиты информации**

Физические, аппаратные и программные средства защиты информации. Аутентификация пользователей. Обфускация программного кода. Алгоритмы шифрования информации.

**5 Модели разграничения доступа к компьютерным системам**

Общая характеристика моделей дискреционного доступа. Модели на основе матрицы доступа.

Общая характеристика политики мандатного доступа. Модели разграничения доступа на основе ролевой политики безопасности.

**6 Защита информации при межсетевом взаимодействии**

Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии

Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

### 4.3 Лабораторные работы

| № ЛР | № раздела | Наименование лабораторных работ | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Проблема НСД к информационным системам | 4 |
| 2 | 2-3 | Анализ моделей угроз на официальном сайте ФСТЭК | 4 |
| 3 | 3 | Стадии обработки и защиты конфиденциальных документов выходного и внутреннего потоков | 6 |
| 4 | 3 | Разработка систем аутентификации пользователя | 6 |
| 5 | 4 | Защита информации методом обфускации программ | 8 |
| 6 | 5 | Модели разграничения доступа к компьютерным системам | 4 |
| 7 | 6 | Проектирование сетевой защиты | 2 |
| | | Итого: | 34 |

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

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.

### 5.2 Дополнительная литература

1. Малюк, А. А. Введение в защиту информации в автоматизированных системах [Текст]: учеб. пособие для студентов, обучающихся по спец., не входящим в группу спец. в обл. информ. безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин.- 2-е изд. - М. : Горячая линия-Телеком, 2004. - 147 с.: ил. - Библиогр.: с. 143. - ISBN 5-93517-062-0.

2. Байбурин В.Б. Введение в защиту информации [Текст]: учеб. пособие для вузов / В.Б. Байбурин [и др.]. - М.: ФОРУМ: ИНФРА-М, 2004. - 128 с. - Библиогр.: с. 124-125. - ISBN 5-89199-0130-4. - ISBN 5-16-001942-1

3. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Текст]: метод. указания к лаб. практикуму / Т. Н. Шалкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Оренбург: ГОУ ОГУ, 2007. - 44 с. - Библиогр.: с. 44.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва: Форум: ИНФРА-М, 2014. - 416 с.: ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3

### 5.3 Периодические издания

Журналы:
- Информационная безопасность;
- Вестник информационной безопасности;
- Проблемы информационной безопасности. Компьютерные системы.

### 5.4 Интернет-ресурсы

- http://www.securitylab.ru/ - «SecurityLab.ru»
- http://www.osp.ru/ - «Открытые системы»
- http://www.citforum.ru/ - «CIT FORUM»

**Стандарты:**

- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»
- ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (утв. и введен в действие Приказом Росстандарта от 15.11.2012 № 814-ст)
- ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Часть 2. Функциональные компоненты безопасности.
- ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
- ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
- ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
- ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования»
- ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения».
- ISO/IEC 27001:2005. «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». 2012 г.
- ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью». 2013 г.
- ISO/IEC 27006:2007 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью».

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

а) программное обеспечение:

- Операционная система Windows 7, Windows 10;
- Microsoft Office 2007, Office 2019;

б) базы данных, информационно-справочные и поисковые системы:

- Консультант Плюс;
- открытые поисковые системы: Yandex, Mail и др.

## 6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки на базе процессора Intel Core i5;
- системные блоки на базе процессора Intel Pentium Core 2 Duo;
- мониторы моделей Samsung, ViewSonic.

***К рабочей программе прилагаются:***

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.