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.44.1 Введение в специальность»*

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 2023

Рабочая программа дисциплины «*Б1.Д.Б.44.1 Введение в специальность*» рассмотрена и утверждена на заседании кафедры

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

протокол № 7 от "9" марта 2023 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 формирования фонда и научной обработки документов
*личная подпись* | Н.Н. Бигалиева *расшифровка подписи* С.А. Бикташева

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

№ регистрации _____

© Влацкая И.В., 2023
© ОГУ, 2023

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины:

раскрытие основных положений Государственного образовательного стандарта по специальности 10.05.01, а также структуры и организации учебного процесса и научно-исследовательской работы в рамках образовательной программы по дисциплине.

**Задачи:**

- ознакомиться с политикой государства в области информационной безопасности;
- получить представление о специальности «Компьютерная безопасность» и ее соответствию системе профессиональных стандартов в области информационной безопасности;
- ознакомиться с угрозами безопасности информации, обрабатываемой в компьютерных системах;
- получить представление об основных направлениях, методах и средствах обеспечения информационной безопасности.

## 2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Отсутствуют*

Постреквизиты дисциплины: *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<br>ОПК-1-В-2 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности | **Знать:**<br>типы защищаемой информации, источники угроз, типы нарушителей.<br>**Уметь:**<br>определять необходимые средства защиты.<br>**Владеть:**<br>навыками использования стандартных средств защиты информации. |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

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

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 1 семестр | всего |
| **Общая трудоёмкость** | **108** | **108** |
| **Контактная работа:** | **50,25** | **50,25** |
| Лекции (Л) | 34 | 34 |
| Практические занятия (ПЗ) | 16 | 16 |
| Промежуточная аттестация (зачет, экзамен) | 0,25 | 0,25 |
| **Самостоятельная работа:**<br>*- выполнение индивидуального творческого задания (ИТЗ);*<br>*- написание реферата;*<br>*- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;*<br>*- подготовка к практическим занятиям;*<br>*- подготовка к рубежному контролю и т.п.)* | **57,75** | **57,75** |
| **Вид итогового контроля (зачет, экзамен, дифференцированный зачет)** | **зачет** | |

Разделы дисциплины, изучаемые в 1 семестре

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 1 | Основные направления развития информационной безопасности в России. Доктрина информационной безопасности Российской Федерации. | 14 | 6 | 2 | | 6 |
| 2 | Угрозы информационной безопасности. Банк угроз безопасности информации сайта ФСТЭК России. | 14 | 4 | 2 | | 8 |
| 3 | Вредоносное программное обеспечение. Вирусы. Программы-шпионы. | 14 | 4 | 2 | | 8 |
| 4 | Интернет вещей. | 14 | 4 | 2 | | 8 |
| 5 | Риски и ответственность компьютерных систем. | 12 | 4 | 2 | | 6 |
| 6 | Защита интеллектуальной собственности | 14 | 6 | 2 | | 6 |
| 7 | Влияние ITна социальные процессы. Профессиональная ответственность и профессиональная этика программиста Образовательная программа «Компьютерная безопасность» | 14 | 4 | 2 | | 8 |
| 8 | Цифровизация общества. Частная жизнь и гражданские свободы | 12 | 2 | 2 | | 8 |
| | Итого: | 108 | 34 | 16 | | 58 |
| | Всего: | 108 | 34 | 16 | | 58 |

**4.2 Содержание разделов дисциплины**

**1. Основные направления развития информационной безопасности**

Виды информационных ресурсов; права граждан, юридических лиц и государства на получение, распространение и использование информации; система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.); система формирования общественного сознания (СМИ, социальные институты и т.д.). Доктрина информационной безопасности Российской Федерации как основной документ, регламентирующий обеспечение информационной безопасности в России.

**2. Угрозы информационной безопасности. Банк угроз безопасности информации сайта ФСТЭК России.**

Классификация угроз информационной безопасности. Источники угроз. Типы нарушителей. Потенциал нарушителей. ФСТЭК России – регулятор информационной безопасности. Полномочия ФСТЭК России. Банк данных угроз. Последствия реализации угроз. Паспорт угрозы. Уязвимости информационной безопасности. Поняти модели угроз. Международные банки угроз информационной безопасности.

**3. Вредоносное программное обеспечение. Вирусы. Программы-шпионы.**

Типы вредоносного программного обеспечения ( вирусы, черви, троянские программы). Программы-шпионы. Ботнет. Типы компьютерных вирусов. Логические бомбы.

**4. Интернет вещей.**

История IoT. Типовая архитектура IoT-приложений. Умный дом. Хакеры и умные вещи. Интернет «злых» вещей. Безопасность интернета вещей. Перспективы использования интернета вещей. Знакомство со студенческой научно-исследовательской лабораторией интернета вещей.

**5. Риски и ответственность компьютерных систем**

Риски, связанные с применением компьютерных систем; примеры отказов и нарушения безопасности ПО; проблемы, связанные со сложностью ПО; управление рисками и оценка рисков.

**6. Защита интеллектуальной собственности**

Основы интеллектуальной собственности; права собственности, патенты, коммерческая тайна; пиратство ПО; патентование ПО; интеллектуальная собственность и международное право.

**7. Влияние ITна социальные процессы. Профессиональная ответственность и профессиональная этика программиста. Образовательная программа «Компьютерная безопасность»**

Влияние ИТ и телекоммуникаций на социальные процессы; рост сети Интернет, организация управления сетью Интернет и доступа к ее ресурсам; международное сотрудничество и межгосударственные границы.

Оценка аспектов профессиональной деятельности с позиций этики; понимание социальных аспектов разработки ПО; учет возможных последствий и реальных ценностей.

Общественные ценности и законы этики; сущность профессионализма; ступени профессиональной подготовки и их оценка; роль профессионалов в социальных процессах; уверенность в будущем; этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и пр.); недоверие и дискриминация; всеобъемлющая информатизация и повсеместное использование ИТ.

Основы обучения в высшем учебном заведении. Организация учебного процесса в университете. Модель компетенций специалиста в области информационных технологий. Личностные качества специалиста в области информационных технологий. Образовательный стандарт 10.05.01 – Компьютерная безопасность. Характеристика направления подготовки специалиста. Задачи видов профессиональной деятельности специалиста. Требования к результатам освоения образовательной программы специалиста. Базовый учебный план.

**8. Частная жизнь и гражданские свободы**

Цифровое общество. Цифровая грамотность. Этические и законодательные основы личной безопасности; конфиденциальность персональной информации в базах данных; технологические решения для обеспечения конфиденциальности; свобода самовыражения в киберпространстве; влияние на интернациональность культуры.

### 4.3 Практические занятия (семинары)

| № занятия | № раздела | Тема | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Основные положения Доктрины информационной безопасности 2016 года. | 2 |
| 2 | 3 | Защита информации стандартными средствами WINDOWS | 4 |
| 3 | 3 | Вирусы и защита от них | 2 |
| 4 | 3 | Программы-шпионы | 2 |
| 5 | 5 | Оценка рисков | 2 |
| 6 | 6 | Защита объектов интеллектуальной собственности | 4 |
| | | Итого: | 16 |

### 4.4 Примерные темы рефератов

- Защита информации в социальных сетях;
- Фишинг;
- Клонирование сайтов;
- DDOS-атаки;
- Спам;
- Программы-шпионы;
- Вирусы

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

1. 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.

2. 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.

### 5.2 Дополнительная литература

1. 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

2. 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.

3. 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: Фо-

рум: 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, издательство компании «Гротек», г. Москва;

– Вестник информационной безопасности, издательство компании «Гротек», г. Москва;

– Проблемы информационной безопасности. Компьютерные системы, издательство СпбПУ, г. Санкт-Петербург.

### 5.4 Интернет-ресурсы

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

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

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021

2. Офисный пакет Microsoft Office (Word, Excel, Power Point) текущей версии. Доступен в рамках лицензионного соглашения OVS-ES. Разработчик: компания Microsoft. Режим доступа: https://products.office.com/en/home

3. Интегрированная среда разработки Microsoft Visual Studio текущей версии. Доступно бесплатно в рамках лицензионного соглашения Visual Studio Community. Разработчик: компания Microsoft. Режим доступа https://visualstudio.microsoft.com/ru/vs/community/

4. Базы данных, информационно-справочные и поисковые системы:

– Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. - Москва, [1992–2016]. – Режим доступа : http://www.consultant.ru/

– Законодательство России [Электронный ресурс] : информационно-правовая система. - Режим доступа : http://pravo.fso.gov.ru/ips/

– Сайт Федеральной службы по техническому и экспортному контролю Российской федерации: https://fstec.ru/

## 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.

Практические 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.