

# «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

## Б1.В.ОД.13

Дисциплина «Информационная безопасность» предназначена для студентов, обучающихся по направлению подготовки 09.03.03 «Прикладная информатика», квалификации «бакалавр», входит в вариативную часть обязательных дисциплин блока 1.

### 1. Цели освоения дисциплины

Целью преподавания дисциплины является ознакомление студентов с основными понятиями и определениями, относящихся к области информационной безопасности, получение знаний по основам теории и практики безопасности информационных систем, о различных подходах к защите информации, реализуемых в современных компьютерных системах.

Задача дисциплины – получение базовых знаний в вопросах, связанных с обеспечением информационной безопасности информационных систем на стадии их проектирования и эксплуатации.

Конечным результатом изучения учебной дисциплины «Информационная безопасность» является овладение современными методами и инструментарием, применяемым в сфере информационной безопасности, достаточном для использования в практической деятельности.

Изучение дисциплины позволяет овладеть как теоретической базой, так и конкретными практическими навыками решения указанных задач на компьютере.

Основными задачами дисциплины являются:

- проведение обследования прикладной области в соответствии с профилем подготовки;
- моделирование прикладных и информационных процессов;
- формирование требований к информатизации и автоматизации прикладных процессов;
- технико-экономическое обоснование проектных решений, составление технических заданий на автоматизацию и информатизацию решения прикладных задач, техническое проектирование ИС в соответствии со спецификой профиля подготовки;
- программирование, тестирование и документирование приложений;
- аттестация и верификация ИС.

### 2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Информационная безопасность» (Б1.В.ОД.13) относится к дисциплинам цикла «Дисциплины (модули)».

Приступая к изучению данной дисциплины, студент должен иметь базовые знания по дисциплинам «Математика», «Теория вероятностей и

математическая статистика», а также «Операционные системы» и «Информационные системы и технологии».

Знания и умения, полученные в результате освоения дисциплины «Информационная безопасность», являются необходимыми для изучения следующих дисциплин: «Вычислительные системы, сети и телекоммуникации», «Программная инженерия», «Проектный практикум «Нейрокомпьютерное моделирование», «Интеллектуальные информационные системы».

### **3. Компетенции обучающегося, формируемые в результате освоения дисциплины**

В данном разделе содержится описание перечня планируемых результатов обучения по дисциплине «Информационная безопасность», соотнесенных с планируемыми результатами освоения образовательной программы 09.03.03 "Прикладная информатика".

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование в соответствии с ФГОС ВО и образовательной программой следующих компетенций:

а) общекультурные компетенции (ОК):

- ОК-4 – способность использовать основы правовых знаний в различных сферах деятельности.

б) общепрофессиональные компетенции (ОПК):

- ОПК-1 – способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий.

- ОПК-4 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

в) профессиональные компетенции (ПК):

- ПК-5 – способность выполнять технико-экономическое обоснование проектных решений.

- ПК-10 – способность принимать участие во внедрении, адаптации и настройке информационных систем.

- ПК-16 – способность осуществлять презентацию информационной системы и начальное обучение пользователей.

- ПК-23 – способность применять системный подход и математические методы в формализации решения прикладных задач.

В результате освоения дисциплины «Информационная безопасность» обучающийся должен:

- **знать:**

- назначение и использование прикладных программных продуктов для решения задач информационной безопасности и защиты данных;
- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационных системах;
- современные антивирусные программы;
- методы шифрования данных;
- виды угроз информационных систем и методы обеспечения информационной безопасности;
- общие принципы анализа защищенности корпоративной информационной среды.

- **уметь:**

- использовать защитные механизмы; имеющиеся в прикладных офисных программах;
- настраивать антивирусные программы;
- выбирать программы криптографического закрытия информации; исходя из реальных угроз и требований по защите информации;
- самостоятельно осваивать новые направления в информационных технологиях, связанных с информационной безопасностью и защитой данных.

- **владеть:**

- методами организации и средствами обеспечения информационной безопасности и защиты данных;
- способами защиты корпоративной информационной среды;
- принципами анализа защищенности корпоративной информационной среды;
- концепциями развития процессов по защите данных;
- методами работы с современными программными продуктами, которые используются для защиты информации.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.