

## АННОТАЦИЯ

дисциплины

### «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки -21.03.02 «Землеустройство и кадастры»

Квалификация (степень) выпускника – бакалавр

Профиль - «Кадастр недвижимости»

#### **1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Информационная безопасность» (Б1.В.ОД.9) относится к вариативной части и является обязательной дисциплиной обучающегося.

#### **2. Цель и задачи дисциплины**

Целью изучения дисциплины является ознакомление студентов с теорией защиты информации, а также с современными методами и средствами защиты информации в компьютерных системах и сетях.

Для достижения поставленной цели решаются следующие задачи:

- знакомство с нормативно-правовыми актами международного, федерального и ведомственного уровня, определяющих организационные и правовые аспекты в области информационной безопасности (ИБ);
- изучение основных понятий и принципов защиты информации;
- изучение криптографических методов защиты информации;
- изучение программных и программно-аппаратных средств защиты операционных систем, компьютерных сетей и баз данных;
- изучение методов и инструментов защиты программного обеспечения от разрушающих программных воздействий.

#### **3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-1, ПК-8.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

- основы российской правовой системы и законодательства;
- характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
- источники и классификацию угроз информационной безопасности;

- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- типовые поточные и блочные шифры;
- частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
- типовые шифры с открытыми ключами;
- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях.

#### УМЕТЬ:

- использовать в практической деятельности правовые знания;
- анализировать правовые акты и осуществлять правовую оценку информации;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
- применять средства обеспечения безопасности данных.

#### ВЛАДЕТЬ:

- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
- навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;
- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
- навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;
- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

#### **4. Содержание и структура дисциплины**

- Введение в дисциплину
- Законодательство Российской Федерации в области информационной безопасности
- Угрозы безопасности информации в информационных системах
- Защита информации в информационных системах от случайных угроз

- Методы и средства защиты информации в информационных системах от традиционного шпионажа и диверсий
- Защита информации в информационных системах от несанкционированного доступа
- Методы защиты от несанкционированного изменения структур информационных систем
- Меры и средства защиты информации в информационных системах от утечки по техническим каналам

#### **5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 2 зачетные единицы (72 час.), в том числе:

лекции – 16 час.

лабораторные работы – 16 час.

самостоятельная работа – 31 час.

контроль – 9 час.

Форма контроля знаний – зачет