# Аннотация к рабочей программе дисциплины

Б1.О.11.03 Основы информационной безопасности

**Направление подготовки:** 35.03.08 Водные биоресурсы и аквакультура

**Квалификация выпускника:** Бакалавр

**Цель освоения дисциплины:** является формирования у студентов знаний и навыков по вопросам информационной безопасности, а также навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах организаций и учреждений.

**Объем дисциплины:** 2 з.е. 72 ч**.**

# Семестр: 1

**Краткое содержание основных разделов дисциплины:**

|  |  |
| --- | --- |
| № п/праздела | Краткое содержание разделов дисциплины |
| **1** | Основные понятия и анализ угроз информационной безопасности. Тема 1.1. Основные понятия информационной безопасности и защиты ин-формации.Основные термины и определения. Обеспечение информационной безопас- ности компьютерных систем. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность не- санкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умыш- ленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективныеТема 1.2. Политика информационной безопасностиОсновные понятия политики безопасности. Структура политики безопасно- сти. Разработка политики организации безопасности организации.Тема 1.3. Стандарты информационной безопасностиРоль стандартов информационной безопасности. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Евро- пейские критерии безопасности информационных технологий. Федеральные крите- рии безопасности. Канадские критерии безопасности компьютерных систем. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ. Функциональные требования безопасности. Требования доверия к безопасно- сти. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000). Стандарты по менеджменту информационной безопасности ISO/IEC 27001-27040. Немецкие стандарты BSI. Стандарты SysTrust, SCORE, GIAC. Стандарты для беспроводных сетей. Отечест- венные стандарты информационной безопасности. Стандарты обеспечение инфор- мационной безопасности организаций банковской системы. Российской Федера- ции. ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2 – 2018. Стандарты информационной безопасности в Интернете (IETF, RFC) |
| **2** | Раздел 2. Понятие национальной безопасности, виды безопасности. Инфор- мационная безопасность РФОрганы, обеспечивающие национальную безопасность РФ, цели, задачи. На- циональные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной полити- ки государств и ведомств. Государственная тайна. |
| **3** | Раздел 3. Международная, национальная и ведомственная нормативная пра- вовая база в области информационной безопасностиОбщие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, ка- сающиеся охраны интеллектуальной собственности. Положения Гражданского ко- декса РФ по защите информации. Международное сотрудничество. Кодекс об ад- министративных правонарушениях. Уголовный кодекс и защита информации. Ос- новные подзаконные акты в области информационной безопасности. Указы Прези- дента РФ, постановления Правительства РФ, ведомственная нормативная база. |
| **4** | Раздел 4. Инженерно-техническая защита информацииПонятие криптографии. Критерий надежности шифрования. Основные крип- тографические приемы: блочное шифрование, схема поточного шифрования. Сим- метричные криптосистемы шифрования. Ассиметричные криптосистемы шифро- вания. Функции хэширования. Основные процедуры цифровой подписи. Управле- ние криптоключами. Идентификация, аутентификация и управление доступом: ме- тоды аутентификации, использующие пароли, строгая аутентификация, биометри- ческая аутентификация. Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок Особенности взаимодействия с программно- аппаратными средствами защиты. Методика применения средств борьбы с вредо- носными закладками на этапе эксплуатации систем. Системы разграничения досту- па и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ. Краткая характеристика мер защиты: юридические, административные и организа- ционные, аппаратно-программные. Компьютерные вирусы. Классификация. Жиз- ненный цикл. Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных анти- вирусных программ. Средства защиты от копирования. Примеры средств и техно- логий. Вопросы правовой защиты |
| **5** | Раздел 5. Организационно-правовое обеспечение защиты информации Сущность и роль организационно-правовых аспектов информационной безо-пасности. Человек как главное звено в системе защиты информации и как зло- умышленник. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”. Ви- ды и категории информации ограниченного доступа: государственная и другие ви- ды тайн. Закон РФ “О государственной тайне”, “О коммерческой тайне”, “О персо- нальных данных”, “О национальной платежной системе”, “О безопасности крити- ческой информационной инфраструктуры Российской Федерации”. Государствен- ная система лицензирования и сертификации деятельности в области защиты ин- формации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”. Закон РФ “Об электронной цифровой подписи”. Уголовно- правовое регулирование защиты ин- формации. |

# Форма промежуточной аттестации: зачет