ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A2C30F99EF9D0306EA3C0F012BEB925E
Владелец: Чанкаев Мурат Хасанович
Действителен: с 02.04.2026 до 26.06.2027

**Аннотация**
**рабочей программы дисциплины**
**«Информационная безопасность»**
**направление подготовки 09.03.03 Прикладная информатика**
**профиль: «Прикладная информатика в экономике».**

| | |
|---|---|
| Цель изучения дисциплины | сформировать у студентов готовность обеспечивать информационную безопасность и систему защиты информации в современном информационном обществе и способность соблюдать основные требования информационной безопасности. |
| Место дисциплины в учебном плане | Б1.О.20 |
| Общая трудоемкость дисциплины з.е./ часов | 4/144 |
| Реализация дисциплины | по очной форме 3 курс 5 семестр, 6 семестр |
| | по заочной форме 4 курс зимняя сессия, летняя сессия |
| Формируемые компетенции | ОПК-3; ОПК-4 |
| Знания, умения и навыки, получаемые в результате освоения дисциплины | **Знать:** основы предметной области: основные разделы информационной безопасности: об информации, методах ее хранения, обработки и передачи; об основных алгоритмах обработки информации и их сложности; об архитектуре вычислительной системы и принципах её функционирования; свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность работать с научной литературой и другими источниками научно-технической информации: правильно понимать смысл текстов, описывающих методы и модели в профессиональной сфере; основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.<br>**Уметь:** работать с конспектами, учебником, учебно-методической , справочной литературой, другими источниками информации; воспринимать и осмысливать информацию развиваемых направлений информационной защиты; применять полученные знания для решения учебных задач; наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий; о методах и средствах обеспечения защиты информационной безопасности личности и общества; применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы и систем обеспечения информационной безопасности.<br>**Владеть:** культурой мышления: способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения составы преступлений в сфере компьютерной информации, предусмотренные УК РФ, и толкование специальных терминов, употребляемых в них; навыками составления технической |

| | |
|---|---|
| | документации на различных этапах жизненного цикла и систем обеспечения информационной безопасности. |
| Содержание дисциплины | **Раздел 1. Основы информационной безопасности.** Понятие информационной безопасности. Основные составляющие. Определите основные аспекты актуальности информационной безопасности в современный период. Понятия о видах вирусов. Наиболее распространенные угрозы. Основные определения и критерии классификации угроз. Правовая и техническая защита информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Законодательный уровень информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Стандарты и спецификации в области информационной безопасности. Основные положения теории информационной безопасности информационных систем. Административный уровень информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Управление рисками. Этапы управления рисками. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Процедурный уровень информационной безопасности. Физическая защита. Реагирование на нарушения режима безопасности.<br>**Раздел 2. Методы защиты информации.** Основные программно-технические меры. Методы криптографии. Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации. Идентификация и аутентификация, управление доступом. Использование защищенных компьютерных систем. Основные положения теории информационной безопасности информационных систем. Протоколирование и аудит, шифрование, контроль, целостности. Защита информации от утечки по техническим причинам. Экранирование, анализ защищенности. Международные стандарты информационного обмена. Понятие угрозы. Обеспечение высокой доступности. Туннелирование и управление. Важность и сложность проблемы информационной безопасности. |
| Виды учебной работы | Лекции, практические занятия, самостоятельная работа. |
| Форма промежуточной аттестации | Зачет |