Негосударственное аккредитованное некоммерческое

частное образовательное учреждение высшего образования

«Академия маркетинга и социально-информационных технологий – ИМСИТ»

(г. Краснодар)

Институт информационных технологий и инноваций

Кафедра математики и вычислительной техники

|  |  |
| --- | --- |
| Рассмотрено и одобрено на заседании кафедры математики и вычислительной техники Академии ИМСИТ, протокол №8 от 11 апреля 2020 года,  зав. кафедрой МиВТ, доцент  \_\_\_\_\_\_\_\_\_\_ Н.С. Нестерова | УТВЕРЖДАЮ  Проректор по учебной работе, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_ Н.И. Севрюгина  13 апреля 2020 г. |

**Б1.Б.14**

**ЗАЩИТА ИНФОРМАЦИИ**

АННОТАЦИЯ

УЧЕБНОЙ ДИСЦИПЛИНЫ

для студентов направления подготовки

09.03.01Информатика и вычислительная техника

Направленность (профиль) образовательной программы

«Автоматизированные системы обработки информации и управления»

Квалификация (степень) выпускника

«Бакалавр»

Краснодар

2020

|  |  |
| --- | --- |
| **Цель и задачи изучения дисциплины:** | **Целью** учебной дисциплины «Защита информации» является приобретение студентами знаний, навыков и умений, связанных с правовыми и программно-техническими проблемами защиты информации государственных и негосударственных организаций и учреждений.  **Задачи** дисциплины:  - определение понятийного аппарата, используемого в области обеспечения безопасности информации в компьютерных системах;  - систематизация теоретических знаний по обеспечению безопасности информации в системах управления, использующих современные информационные технологии;  - выявление сущности, целей, задач и места методов и средств защиты информационных процессов в компьютерных системах в общей системе обеспечения безопасности информации на объектах информатизации;  - изучение основных принципов применения методов и средств защиты информации при организации защиты информационных процессов в компьютерных системах;  - изучение нормативно-руководящих документов, регламентирующих вопросы обеспечения безопасности информации в автоматизированных системах;  - развитие у обучаемых управленческих и инженерных навыков обоснованного принятия решений по организации комплексной защиты информации, оценке защищенности и управления процессами защиты в автоматизированных системах. |
| **Место дисциплины в структуре ОПОП** | Дисциплина входит в базовую часть блока Б1 учебного плана. |
| **Краткая характеристика учебной дисциплины (основные блоки, темы)** | Раздел 1. Организационные основы защиты компьютерной информации  Раздел 2. Защита компьютерной информации от несанкционированного доступа  Раздел 3. Криптографическая защита компьютерной информации  Раздел 4. Защита информации в компьютерных сетях (КС) |
| **Компетенции, формируемые в результате освоения учебной дисциплины:** | ОПК-2 Способностью осваивать методики использования программных средств для решения практических задач;  ОПК-5 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| **Знания, умения и навыки, получаемые в процессе изучения дисциплины:** | **Знать**:   * основные понятия и направления в защите компьютерной информации, * принципы защиты информации, * принципы классификации и примеры угроз безопасности компьютерным системам, * современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, * методы и средства обеспечения информационной безопасности компьютерных систем.   **Уметь**:   * конфигурировать встроенные средства безопасности в операционной системе; * проводить анализ защищенности компьютера и сетевой среды; * устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; * устанавливать и использовать один из межсетевых экранов; * организовывать регистрацию пользователей в сетевой операционной системе; * организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа; * организовывать безопасную работу в Интернет; * организовывать отправку почтовых сообщений с использованием глобальной сети Интернет; * использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.   **Владеть**:   * современными методами обеспечения защиты информации * современными функционально-ориентированными программными средствами защиты информации и использования сетевых ресурсов; * современными инструментальными средства анализа рисков и разработки политики информационной безопасности; * навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации; * типовыми средствами защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем. |
| **Формы проведения занятий, образовательные технологии:** | Лекционные занятия: проблемные лекции, лекция – визуализация, лекция-беседа, лекция - анализ ситуаций.  Практические занятия: тематические семинары, проблемные семинары, метод «круглого стола», метод «коллективной мыслительной деятельности», методы анализа проблемных ситуаций, коллоквиум, решение ситуационных задач. |
| **Используемые инструментальные и программные средства:** | Средства проекции (презентации), программированного контроля (тестирования) |
| **Формы промежуточного**  **контроля:** | Текущие оценки знаний, тестирование, доклады, самостоятельные работы |
| **Общая трудоемкость изучения дисциплины:** | 180 ч / 5 з.е. |
| **Форма итогового контроля знаний:** | Экзамен |