Р А Б О Ч А Я П Р О Г Р А М М А

по дисциплине **«Защита информации»**

для основной профессиональной образовательной программы по направлению
09.03.01 «Информатика и вычислительная техника»,
направленность (профиль) – Программное обеспечение средств
вычислительной техники и автоматизированных систем
квалификация – бакалавр
программа академического бакалавриата.

Кафедра Информационных технологий (ИТ)
Разработчик: к.т.н., доцент Лесечко Владимир Николаевич

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины направлен на получение образовательных результатов освоения дисциплины, соответствующих формируемым компетенциям:

Код	Содержание компетенции	Результаты освоения
ОК-2	способностью анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции	Знает: структуру разработки баз данных; основные понятия баз данных Умеет: строить информационную и математическую модель базы данных; использовать теоретические знания при объяснении результатов экспериментов, применять знания в области информатики для освоения общепрофессиональных дисциплин и решения профессиональных задач. Владеет: языками программирования баз данных; навыками информационных исследований
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	Знает: основные понятия коммуникации; психологические особенности групп и индивидуумов Умеет: строить коммуникативное общение и взаимодействие; использовать теоретические знания при объяснении результатов взаимодействия в группе. Владеет: языками вербального и невербального взаимодействия, психологическими приемами общения; навыками информационных исследований
ОПК-2	способностью осваивать методики использования программных средств для решения практических задач	Знает: основные понятия баз данных; структуру разработки баз данных

		Умеет: использовать теоретические знания при объяснении результатов экспериментов, применять знания в области информатики для освоения общепрофессиональных дисциплин и решения профессиональных задач; строить информационную и математическую модель базы данных Владеет: навыками информационных исследований; языками программирования баз данных
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	Знает: основные понятия данных; структуру обработки данных Умеет: использовать теоретические знания при объяснении результатов экспериментов, применять знания в области информатики для освоения общепрофессиональных дисциплин и решения профессиональных задач; строить информационную и математическую модель данных Владеет: навыками информационных исследований; языками программирования данных
ПК-4	способностью готовить конспекты и проводить занятия по обучению работников применению программно-методических комплексов, используемых на предприятии	Знает: основные понятия защиты данных; структуру разработки защиты данных Умеет: строить информационную и математическую модель защиты данных; использовать теоретические знания при объяснении результатов экспериментов, применять знания в области информатики для освоения общепрофессиональных дисциплин и решения профессиональных задач. Владеет: навыками информационных исследований; языками программирования защиты данных

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информации» относится к обязательным дисциплинам вариативной части (Б1.В.ОД). Шифр дисциплины в учебном плане – Б1.В.ОД.18.

Изучению данной дисциплины предшествуют такие дисциплины как: Введение в информационные технологии, Теория информации, Вычислительная математика, Метрология, стандартизация и сертификация, Технология решения задач математического программирования, Архитектура вычислительных сетей, Информатика, Физика, Программирование, Операционные системы, Инженерная и компьютерная графика, Структуры и ал-

горитмы обработки данных, Математика, Алгебра и геометрия, ЭВМ и периферийные устройства, Интернет – технологии.

3. ОБЪЁМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины: 216 часов, 6 ЗЕ.

Форма контроля: Экзамен.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование тем (разделов) дисциплины и их содержание
Тема 1. Информационная безопасность. Основные понятия и определения, относящиеся к информационной безопасности. Модель безопасности информационной системы. Источники, риски и формы атак на информацию. Средства защиты компьютеров: средства защиты в операционных системах, дополнительные программно-аппаратные средства, обеспечивающие повышенный уровень защиты.
Тема 2. Средства достижения информационной безопасности Законодательные меры обеспечения информационной безопасности. Административный меры. Политика безопасности. Программа безопасности. Процедурные меры. Программно-технические меры.
Тема 3. Основы сетевой безопасности Модель сетевой безопасности. Классификация сетевых атак. Модель сетевого взаимодействия. Компоненты безопасной связи: конфиденциальность, аутентификация, целостность данных, контроль доступа к данным
Тема 4. Конфиденциальность. Принципы криптографии 4.1. *Алгоритмы симметричного шифрования.* Секретный ключ. Блочные и потоковые шифры. Требования к алгоритмам. Области применения. Криптоанализ. - Алгоритм шифрования DES. Принципы разработки алгоритма, шифрование, дешифрование, создание подключей. Криптостойкость алгоритма. - Алгоритм симметричного шифрования ГОСТ. Различия между алгоритмами DES и ГОСТ. - Объединение блочных шифров. - Режимы выполнения алгоритмов симметричного шифрования. 4.2. *Создание случайных чисел.* Требования к случайным числам. Источники случайных чисел. Генераторы псевдослучайных чисел. Криптографически созданные случайные числа. 4.3. *Алгоритмы шифрования с открытым ключом.* Открытый и закрытый ключ. Основные требования к алгоритмам асимметричного шифрования. Криптоанализ алгоритмов с открытым ключом. - Алгоритм обмена ключами Диффи-Хеллмана. Безопасность алгоритма. - Алгоритм шифрования RSA. Описание алгоритма. Создание ключей. Безопасность RSA.
Тема 5. Аутентификация и обмен ключами Центр распределения ключей. Сертификация ключей. Центр сертификации ключей. Алгоритм аутентификации с использованием "билета". Алгоритм аутентификации Нидхема-Шредера. Протокол Kerberos. Аутентификация на основе криптосистем с открытым ключом.

Тема 6. Целостность данных. Цифровая подпись Требования к цифровой подписи. Технология цифровой подписи. Хэш-функции. Дайджест сообщения. Алгоритм хэширования MD5. Электронная цифровая подпись RSA.
Тема 7. Контроль доступа Экранирование. Межсетевой экран. Классификация межсетевых экранов. Анализ защищённости. Архитектура корпоративных сетей.