Аннотация рабочей программы дисциплины «Защита информации»
для направления подготовки 09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы - Автоматизированные системы обработки информации и управления

1. Цели и задачи освоения дисциплины

Цель дисциплины изучение методов и средств защиты информации, исключающих несанкционированный доступ к информации, хранящейся и обрабатываемой в ЭВМ, обеспечение информационной безопасности организации, обеспечение комплексной защиты объектов информации от различных угроз.

Задачами дисциплины являются: освоение средств защиты компьютерной информации, изучение методов защиты программ от несанкционированного доступа, построение комплексных систем защиты.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Вместе с другими дисциплинами ОП дисциплина «Защита информации» обеспечивает формирование следующих компетенций бакалавров:

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникционных технологий и с учетом основных требований информационной безопасности (ОПК-5);

способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности (ПК-3).

В результате освоения дисциплины обучающийся должен:

знать правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты, модели и методы шифрования, методы идентификации пользователей, методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации;

уметь применять известные методы и средства поддержки информационной безопасности в компьютерных системах, решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникционных технологий и с учетом основных требований информационной безопасности, проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах;

владеть навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации, навыками построения программных систем, способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.

3. Содержание дисциплины

Основные понятия и определения в области защиты информации. Угрозы информационной безопасности. Вредоносное ПО. Компьютерные вирусы и средства защиты от них. Правовое обеспечение защиты информации. Стандарты информационной безопасности. Формальные модели безопасности. Организационные методы защиты информации. Программно-технические методы защиты