Аннотация к рабочей программе дисциплины

Б1.В.ДВ.3.1 «Защита информации»

Направление подготовки

15.03.04 «Автоматизация технологических процессов и производств»

Профиль подготовки

«Автоматизация технологических процессов и производств в химии, нефтепереработке и энергетике»

Квалификация выпускника

бакалавр

Форма обучения

Очная, заочная

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 криптографических методов и средств защиты компьютерной информации, изучение методов защиты программ от несанкционированного доступа, построение комплексных систем защиты.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен обладать следующими компетенциями:

Общепрофессиональные компетенции (ОПК):

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-2);

способностью использовать современные информационные технологии, технику, прикладные программные средства при решении задач профессиональной деятельности (ОПК-3).

В результате изучения дисциплин студент должен:

знать правовые основы защиты компьютерной информации, основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты, модели и методы шифрования, методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей, 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, 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, содержащих криптографические алгоритмы шифрования передаваемой информации.

Трудоемкость: 2 з.е. (72 час.)

Объем занятий: лекции – 18 ч.; лабораторные работы – 18 ч.; СРС – 36 ч.

Формы самостоятельной работы студента: Усвоение пройденного лекционного материала, оформление лабораторных работ, подготовка к их защите, изучение материала, вынесенного на самостоятельную проработку, подготовка к тестам и зачету, решение домашних задач.

Формы отчетности: зачет.