АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Кибербезопасность технологических процессов

по направлению подготовки: 18.03.02 «Энерго-и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии»
по профилю «Рациональное использование материальных и энергетических ресурсов»
Квалификация выпускника: БАКАЛАВР
Выпускающая кафедра: ХК

Кафедра-разработчик рабочей программы: «Химической кибернетики»

1. Цели освоения дисциплины

Целями освоения дисциплины «Кибербезопасность технологических процессов» являются:
а) формирование компетенций, позволяющих соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности;
б) обучение технологиям обеспечения информационной безопасности в области управления объектами различного уровня, которые связаны с информационными технологиями, используемыми на этих объектах;
в) обучение основным этапам решения задач кибербезопасности технологических процессов;
г) формирование компетенций, позволяющих проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач.

2. Содержание дисциплины «Кибербезопасность технологических процессов»:

Кибербезопасность (информационная безопасность): основные понятия и определения. Общие сведения о защите информации.
Правовые основы обеспечения и стандарты информационной безопасности.
Проблемы информационной безопасности сетей.
Технологии защиты от вирусов. Технологии аутентификации.
Криптографические методы защиты информации.
Программно-аппаратные методы защиты в сети. Защита в Интернет.

3. В результате освоения дисциплины обучающийся должен:

1) Знать:
а) политику безопасности, сущность информационной безопасности информационных систем;
б) состав и методы организационно-правовой защиты информации;
в) методы антивирусной защиты информации;
г) современные методы криптографической защиты информации;
д) процедуры аутентификации данных и постановки электронной цифровой подписи.
2) Уметь:
а) применять организационно-правовые методы защиты информации в информационных системах;
б) обеспечивать антивирусную защиту информации;
в) использовать методы и средства криптографической защиты информации;
г) применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах.
3) Владеть:
а) приемами антивирусной защиты и информационной защиты;
б) основными методами, способами и средствами получения, хранения, переработки информации;

в) методами анализа и оценки состояния обеспечения информационной безопасности в учреждении.

Зав. кафедрой ХК  Кутузов А.Г.