«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Б1.В.ДВ.3.2

Дисциплина «Информационная безопасность» предназначена для студентов, обучающихся по направлению подготовки 41.03.01 – «Зарубежное регионоведение» профиль «Азиатские исследования», квалификации (степени) «бакалавр»; входит в вариативную часть дисциплин по выбору блока Б1.

1. Цели освоения дисциплины

Целью преподавания дисциплины является ознакомление студентов с основными понятиями и определениями, относящихся к области информационной безопасности, получение знаний по основам теории и практики безопасности информационных систем, о различных подходах к защите информации, реализуемых в современных компьютерных системах.

Задача дисциплины – получение базовых знаний в вопросах, связанных с обеспечением информационной безопасности информационных систем на стадии их проектирования и эксплуатации.

Конечным результатом изучения учебной дисциплины «Информационная безопасность» является овладение современными методами и инструментарием, применяемым в сфере информационной безопасности, достаточном для использования в практической деятельности.

Изучение дисциплины позволяет овладеть как теоретической базой, так и конкретными практическими навыками решения указанных задач на компьютере.

Основными задачами дисциплины являются:

– проведение обследования прикладной области в соответствии с профилем подготовки;

– моделирование прикладных и информационных процессов;

– формирование требований к информатизации и автоматизации прикладных процессов;

– технико-экономическое обоснование проектных решений, составление технических заданий на автоматизацию и информатизацию решения прикладных задач, техническое проектирование ИС в соответствии со спецификой профиля подготовки;

– программирование, тестирование и документирование приложений;

– аттестация и верификация ИС.

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Информационная безопасность» (Б1.В.ДВ.3.2) относится к дисциплинам по выбору блока 1 «Дисциплины (модули)».

Приступая к изучению данной дисциплины, студент должен иметь базовые знания по дисциплинам «История», «Безопасность жизнедеятельности», «Основы права», «Информатика и информационные технологии», «Основы регионоведения», «Основы экономических знаний».

Знания и умения, полученные в результате освоения дисциплины «Информационная безопасность», являются необходимыми для изучения следующих дисциплин: «Внешняя политика стран (ы) региона специализации», «Религиозный фактор в современных международных отношениях».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих общепрофессиональных компетенций в соответствии с ФГОС ВО и образовательной программой по данному направлению подготовки:

ОПК-1 - уметь применять знания в области социальных, гуманитарных и экономических наук, информатики и математического анализа для решения прикладных профессиональных задач.

ПК-9 – владением основами социологических методов (интервью, анкетирование, наблюдение), готовность принять участие в планировании и проведении полевого исследования в стране (регионе) специализации.

В результате освоения дисциплины «Информационная безопасность» обучающийся должен:

• Знать:

- назначение и использование прикладных программных продуктов для решения задач информационной безопасности и защиты данных;

- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационных системах;

- современные антивирусные программы;

- методы шифрования данных;

- виды угроз информационных систем и методы обеспечения информационной безопасности;

- общие принципы анализа защищенности корпоративной информационной среды.

• Уметь:

- использовать защитные механизмы; имеющиеся в прикладных офисных программах;

- настраивать антивирусные программы;

- выбирать программы криптографического закрытия информации; исходя из реальных угроз и требований по защите информации;

- самостоятельно осваивать новые направления в информационных технологиях, связанных с информационной безопасностью и защитой данных.

• Владеть:

- методами организации и средствами обеспечения информационной безопасности и защиты данных;
- способами защиты корпоративной информационной среды;
- принципами анализа защищенности корпоративной информационной среды;
- концепциями развития процессов по защите данных;
- методами работы с современными программными продуктами, которые используются для защиты информации.

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.