ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Цель освоения дисциплины

Сформировать систему компетенций бакалавра прикладной информатики в области обеспечении качества автоматизации и информатизации решения прикладных задач и создания информационных систем для решения задач обеспечения информационной безопасности компьютерных систем в проектной и производственно-технологической профессиональной деятельности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к базовой части блока дисциплин. Для освоения дисциплины «Информационная безопасность» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплины «Информационные системы и технологии», прохождения практики «Практика по получению первичных умений и навыков научно-исследовательской деятельности».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:
– 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-4).

В результате изучения дисциплины обучающийся должен:

знать
– терминологию и основные понятия теории защиты информации;
– содержание основных нормативных документов в области защиты компьютерной информации;
– виды угроз информационным системам;
– цели и задачи административного уровня обеспечения информационной безопасности;
– причины и источники случайных воздействий на информационные системы;
– классы функциональных требований и требований доверия;
– виды систем шифрования данных по способу их функционирования;

уметь
– использовать основные концептуальные положения системы защиты информации;
– квалифицировать нарушения в сфере информационной безопасности;
– выявлять угрозы информационной безопасности;
– определить политику безопасности организации;
– определять каналы несанкционированного доступа к информации;
– использовать стандарт для оценки защищенности информационных систем;
– классифицировать методы криптографического преобразования информации;

владеть
– распределением задач информационной безопасности по уровням ее обеспечения;
– навыками определения ответственности за нарушения в сфере информационной безопасности;
– навыками обосновывать организационно-технические мероприятия по защите информации в информационных системах;

– направлениями разработки политики безопасности;
– навыками выявления и классифицирования угрозы информационной безопасности;
– отличием функциональных требований от требований доверия;
– общей технологией использования метода шифрования.

4. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 5,
общая трудоёмкость дисциплины в часах – 180 ч. (в т. ч. аудиторных часов – 72 ч., СРС – 54 ч.),
распределение по семестрам – 7,
форма и место отчётности – экзамен (7 семестр).

5. Краткое содержание дисциплины

Понятия информационной безопасности, защиты информации.
Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации. Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности.

Информация как правовая категория, ее особенности.
Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Лицензирование деятельности в области информационной безопасности. Структура и состав информационного законодательства в РФ. Ответственность за нарушения в сфере информационной безопасности. Стандарты информационной безопасности.

Основные источники угроз безопасности информации.
Классификация угроз информационной безопасности. Виды злоумышленников по отношению к автоматизированной системе. Компьютерные вирусы как угроза информационной безопасности. Классификация антивирусных программ. Профилактика компьютерных вирусов.

Уровни формирования режима информационной безопасности.
Цели и задачи административного уровня обеспечения информационной безопасности. Основные направления разработки политики информационной безопасности организации. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности. Инженерно-техническая защита информации.

Методы и средства защиты информации в компьютерных системах.
Пути достижения требуемой достоверности обработки информации. Общие принципы и методы выявления технических каналов утечки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Рубежи защиты и компоненты системы охраны объекта. Разграничение доступа в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.

Особенности защиты информации в распределенных компьютерных системах.
Функциональные требования и требования доверия, изложенные в «Общих критериях». Сервисы безопасности и администрирование средств безопасности в вычислительных сетях в соответствии с «Рекомендациями X.800». Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Подтверждение

подлинности взаимодействующих процессов. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Электронная цифровая подпись. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.

Классификация методов криптографического преобразования информации. Шифрование. Методы шифрования с симметричным ключом. Методы замены. Методы перестановки. Аналитические методы шифрования. Аддитивные методы шифрования. Системы шифрования с открытым ключом. Российский стандарт на шифрование информации ГОСТ 28147-89.

6. Разработчик

Карякина Татьяна Ивановна, кандидат педагогических наук, доцент кафедры информатики и методики преподавания информатики ФГБОУ ВО «ВГСПУ».