МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1. Цель освоения дисциплины

Сформировать у будущего учителя информатики систему компетенций в области защиты информации в компьютерных системах для решения практических задач.

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства защиты информации» относится к вариативной части блока дисциплин.
Для освоения дисциплины «Методы и средства защиты информации» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Высокоуровневые методы программирования», «Информационные системы», «Информационные технологии», «Компьютерная графика», «Операционная система Linux», «Офисные технологии», «Построение Windows-сетей», «Практикум по решению задач на ЭВМ», «Программирование», «Разработка эффективных алгоритмов», «Теория чисел и числовые системы».
Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Актуальные проблемы информатики и образования», «Архитектура компьютера», «Информационные технологии в управлении образованием», «Компьютерное моделирование», «Основы искусственного интеллекта», «Основы робототехники», «Перспективные направления искусственного интеллекта», «Перспективные направления компьютерного моделирования», «Программные средства информационных систем», «Проектирование информационных систем», «Современные языки программирования», «Специализированные математические пакеты», «Теоретические основы информатики», «Эксплуатация компьютерных систем», прохождения практики «Преддипломная практика».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:
– готовностью применять предметные и метапредметные знания фундаментальной и прикладной информатики для решения теоретических и практических задач, реализации аналитических и технологических решений в области представления и обработки информации, информатизации образования (СК-1).

В результате изучения дисциплины обучающийся должен:

знать
– различные подходы к определению понятия информационная безопасность;
– отличие компьютерной безопасности от информационной безопасности;
– нормативно-правовые основы информационной безопасности общества;
– основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации;
– классификацию угроз информационной безопасности;
– уровни формирования режима информационной безопасности;
– принципы защиты распределенных вычислительных сетей;
– причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях;
– механизм межсетевого экранирования;
– основы криптографических методов защиты информации, структуру криптосистем, методы шифрования;

уметь
– объяснить сущность проблемы информационной безопасности;
– квалифицировать нарушения в сфере информационной безопасности;
– применять антивирусные программы к защите информации;
– распределять задачи информационной безопасности по уровням ее обеспечения;
– использовать принципы защиты для разработки и реализации механизмов защиты вычисли-тельных сетей;
– анализировать причины успеха удаленных атак и принимать меры к их устранению;
– выбирать межсетевые экраны для защиты информационных систем;
– использовать электронную цифровую подпись для проверки целостности данных;

владеть
– определением информационной безопасности приводимые в руководящих документах;
– ответственность за нарушения в сфере информационной безопасности;
– навыками профилактических мер защиты от компьютерных вирусов;
– навыками получения представлений о системном подходе, обеспечивающем информационную безопасность;
– использовать механизмы идентификации и аутентификации для защиты информационных систем;
– навыками определить возможные способы защиты;
– способами управления криптосистемами.

4. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 2,
общая трудоёмкость дисциплины в часах – 72 ч. (в т. ч. аудиторных часов – 12 ч., СРС – 56 ч.),
распределение по семестрам – 4 курс, зима,
форма и место отчётности – зачёт (4 курс, зима).

5. Краткое содержание дисциплины

Понятия информационной безопасности, защиты информации.
Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации.

Государственная политика информационной безопасности.
Информация как правовая категория, ее особенности. Органы обеспечения информационной безопасности. Структура и состав информационного законодательства в РФ. Стандарты информационной безопасности.

Основные источники угроз безопасности информации.
Классификация угроз информационной безопасности. Компьютерные вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.

Уровни формирования режима информационной безопасности.
Цели и задачи административного уровня обеспечения информационной безопасности.
Группы сведений, содержащиеся в документации по политике безопасности организации.
Программно-технический уровень обеспечения информационной безопасности.

Внешнее качество информации в информационных системах.
Пути достижения требуемой достоверности обработки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Организационные и аппаратно-программные

методы повышения сохранности информации.

Особенности защиты информации в распределенных компьютерных системах.
Защита информации в каналах связи. Межсетевое экранирование. Электронная цифровая подпись. Типовые удаленные атаки и их характеристика.

Классификация методов криптографического преобразования информации.
Шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом.

6. Разработчик

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