НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

«УТВЕРЖДАЮ»
Проректор по научной работе
_____ Драгунов В.К.
«16» июня 2015 г.

Программа аспирантуры

Направление: 09.06.01 Информатика и вычислительная техника

Направленность (специальность): 05.13.01 Системный анализ, управление и обработка информации (приборостроение, энергетика, информатика)

РАБОЧАЯ ПРОГРАММА

дисциплины по выбору

«Информационная безопасность в компьютерных системах»

Индекс дисциплины по учебному плану: Б1.В.ДВ.4.1

Всего: 108 часов

Семестр 7, в том числе 6 часов – контактная работа,
84 часа – самостоятельная работа,
18 часов – контроль

Программа составлена на основе федерального государственного образовательного стандарта высшего образования (уровень подготовки кадров высшей квалификации) по направлению подготовки 09.06.01 «Информатика и вычислительная техника», утвержденного приказом Министерства образования и науки РФ от 30 июля 2014 г. № 875, и паспорта специальности 05.13.01 «Системный анализ, управление и обработка информации (приборостроение, энергетика, информатика)» номенклатуры специальностей научных работников утвержденной приказом Минобрнауки России от 25 февраля 2009 г. № 59.

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является изучение основных подходов и методов, обеспечивающих информационную безопасность компьютерных систем, включая криптографические схемы шифрования данных, электронную цифровую подпись и криптографические протоколы.

Задачами дисциплины являются:

− освоение базовых понятий и классификации задач информационной безопасности компьютерных систем;

− изучение симметричных и ассиметричных алгоритмов шифрования и аутентификации данных;

− приобретение навыков использования типовых криптографических схем для защиты информации в компьютерных системах и моделирования возможных видов атак противника.

В процессе освоения дисциплины **формируются следующие компетенции**:

− готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4);

− способность следовать этическим нормам в профессиональной деятельности (УК-5);

− способность планировать и решать задачи собственного профессионального и личностного развития (УК-6);

− владение методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности (ОПК-7);

− способность проводить лабораторные и практические занятия со студентами, руководить курсовым проектированием и выполнением выпускных квалификационных работ и магистерских диссертаций (ПК-3);

− способность разрабатывать и применять современные технологии создания программных комплексов и баз данных для систем управления (ПК-7);

− способность выбирать методы и разрабатывать алгоритмы решения задач управления в технических системах (ПК-8).

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать **следующие результаты образования:**

знать:

− современные технологии создания программных комплексов и баз данных для систем управления (ПК-7);

уметь:

− проводить лабораторные и практические занятия со студентами, руководить курсовым проектированием и выполнением выпускных квалификационных работ и магистерских диссертаций (ПК-3);

− планировать и решать задачи собственного профессионального и личностного развития (УК-6);

− выбирать методы и разрабатывать алгоритмы решения задач управления в технических системах (ПК-8).

владеть:

− навыками использования современных методов и технологии научной коммуникации на государственном и иностранном языках (УК-4);

− способностью следовать этическим нормам в профессиональной деятельности (УК-5);

− методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности (ОПК-7).

КРАТКОЕ СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

1. Основные понятия информационной безопасности.

Составные части информационной безопасности. Анализ угроз информационной безопасности. Понятие политики безопасности, реализация политики безопасности. Основные модели безопасности. Критерии защищенности компьютерных систем. Три уровня защиты информации. Роль и место криптографических методов в обеспечении информационной безопасности, типы криптографических систем, принцип Керкхоффа.

2. Симметрические криптосхемы.

Симметричные криптосхемы: основные понятия, структурная схема. Шифры перестановки, простой замены, сложной замены. Современные симметричные криптосхемы. Американский стандарт шифрования данных: общие сведения, структурная схема, используемые преобразования, основные режимы работы.

3. Поточные и блочные схемы шифрования.

Российский стандарт шифрования ГОСТ 28147-89: общие сведения, структурная схема, используемые преобразования, основные режимы работы. Понятия о блочных и поточных шифрах.

4. Асимметрические криптосхемы.

Понятие вычислительной сложности алгоритма. Структурная схема криптосхемы с открытым ключом. Однонаправленная функция Диффи-Хеллмана, вычислительная неразрешимость задач логарифмирования и факторизации. Криптосистема шифрования RSA: общие сведения, структурная схема, выбор параметров, процедуры зашифрования-расшифрования. Сравнительный анализ симметричных и асимметричных систем. Комбинированный метод шифрования.

5. Электронная цифровая подпись. Хэш-функция.

Три основные задачи современной криптографии. Проблема аутентифика-

ции и электронная цифровая подпись (ЭЦП). Процедуры ЭЦП на основе схемы RSA. Российский стандарт цифровой подписи ГОСТ Р 34.10-94: общие сведения, используемые преобразования. Понятие о хэш-функции. Отечественный стандарт функции хэширования ГОСТ Р 34.11-94. Основные положения Закона РФ «Об электронной цифровой подписи».

6. Генерация, хранение, распределение ключей.

Ключевая информация криптографической системы. Генерация ключей: основные требования к псевдослучайным числовым последовательностям (ПСП), линейный конгруэнтный генератор ПСП, рекуррентные двоичные последовательности, роль неприводимых многочленов над полем 2^n, последовательности максимальной длины. Тесты качества ПСП. Хранение ключей: носители ключевой информации, реализация концепции иерархии ключей. Способы распределения ключей.

7. Обеспечение безопасности локальных сетей.

Организация защиты информации на различных уровнях компьютерных систем. Защита локальной рабочей станции. Защита в локальных сетях. Защита технологии «клиент-сервер». Применение межсетевых экранов. Защита электронной почты. Характеристика отечественных сертифицированных аппаратно-программных средств защиты информации в компьютерных системах и сетях.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБРАЗОВАНИЯ ПО ДИСЦИПЛИНЕ

Промежуточная аттестация по итогам освоения дисциплины: 7 семестр – дифференцированный зачет.

Вопросы для самоконтроля и проведения зачета

1. Составные части информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Понятие политики безопасности, реализация политики безопасности.
4. Основные модели безопасности.
5. Критерии защищенности компьютерных систем.
6. Три уровня защиты информации.
7. Роль и место криптографических методов в обеспечении информационной безопасности, типы криптографических систем, принцип Керкхоффа.
8. Симметричные криптосхемы: основные понятия, структурная схема.
9. Шифры перестановки, простой замены, сложной замены.
10. Современные симметричные криптосхемы.
11. Американский стандарт шифрования данных: общие сведения, структурная схема, используемые преобразования, основные режимы работы.
12. Понятия о блочных и поточных шифрах.
13. Понятие вычислительной сложности алгоритма.
14. Структурная схема криптосхемы с открытым ключом.
15. Однонаправленная функция Диффи-Хеллмана, вычислительная неразрешимость задач логарифмирования и факторизации.
16. Криптосистема шифрования RSA: общие сведения, структурная схема, выбор параметров, процедуры зашифрования-расшифрования.
17. Сравнительный анализ симметричных и асимметричных систем.
18. Комбинированный метод шифрования.
19. Три основные задачи современной криптографии.
20. Проблема аутентификации и электронная цифровая подпись (ЭЦП).

Критерии оценки за освоение дисциплины определены в Инструктивном письме И-23 от 14 мая 2012 г.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература:

1. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учебное пособие для вузов.– М.: Академия, 2006.

2. Расторгуев С. П. Основы информационной безопасности: учебное пособие для вузов.– М.: Академия, 2009.

3. Смарт Н. Криптография: пер. с англ.– М.: Техносфера, 2005.

4. Мельников В. П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: учебное пособие.– М.: АКАДЕМИЯ, 2008.

5. Хорев П. Б. Защита информационных систем: учебное пособие. – М.: Издательский дом МЭИ, 2010.

6. Черемушкин А. В. Криптографические протоколы. Основные свойства и уязвимости : учебное пособие для вузов.– М.: АКАДЕМИЯ, 2010.

Дополнительная литература:

7. Девянин П. Н. Модели безопасности компьютерных систем: учебное пособие для вузов.– М.: Академия, 2005.

8. Хохлов Г. И. Основы теории информации: учебное пособие для вузов.– М.: АКАДЕМИЯ, 2008.

9. Проскурин В. Г. Защита программ и данных: учебное пособие для вузов.– М.: Академия, 2012.

10. Грибунин В. Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учебное пособие.– М.: АКАДЕМИЯ, 2009.

11. Ниссенбаум О. В. Криптографические протоколы: учебное пособие.– Тюмень: ТюмГУ, 2007.

12. Шумский А. А., Шелупанов А.А. Системный анализ в защите информации: учебное пособие для вузов.– М. : Гелиос АРВ, 2005.