Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ**» **(ТУСУР)**

Кафедра автоматизированных систем управления (АСУ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания к лабораторным работам, практическим занятиям и организации самостоятельной работы для студентов направления «Прикладная информатика» (уровень бакалавриата) заочной формы обучения

Томск-2018

Горитов А.Н.
Информационная безопасность: методические указания к лабораторным работам, практическим занятиям и организации самостоятельной работы для студентов направления «Прикладная информатика» (уровень бакалавриата) заочной формы обучения / А.Н. Горитов. – Томск: ТУСУР, 2018. – 15 с.

СОДЕРЖАНИЕ

1 Введение

Цель дисциплины - ознакомить студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании информационных систем (ИС).

Задачи изучения дисциплины состоят в том, что в результате ее изучения студенты должны:

– иметь представление об использовании основных положений теории информационной безопасности в различных областях ИС и иметь представление о направлении развития и перспективах защиты информации;

– знать правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;

– уметь применять методы защиты компьютерной информации при проектировании ИС в различных предметных областях.

Для успешного освоения дисциплины применяются различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме.

Для контроля освоения компетенций используются следующие формы контроля: защита лабораторных работ, тесты.

Дисциплина «Информационная безопасность» относится к числу дисциплин вариативной части профессионального цикла. «Информационная безопасность» как учебная дисциплина в системе подготовки бакалавров по

направлению «Прикладная информатика» связана с дисциплинами учебного плана: «Математика», «Дискретная математика», «Информатика и программирование», «Основы алгоритмизации и языки программирования», «Вычислительные системы, сети и телекоммуникации».

Знания и навыки, полученные при изучении этой дисциплины, используются в дисциплине профессионального цикла: «Проектирование информационных систем» и выпускной квалификационной работе.

2 Методические указания к проведению лабораторных работ

2.1 Общие положения

Целью проведения лабораторных работ является формирование компетенций в области «Информационная безопасность».

Основной формой проведения лабораторных работ является разработка алгоритма решения индивидуальной задачи и его программная реализация на одном из языков программирования. Процесс программной реализации включает в себя написание программы, отладку программы и тестирование программы.

К основным способам контроля формирования компетенций при выполнении лабораторных работ относятся индивидуальная защита выполненной работы, организация входного контроля уровня подготовки студентов по теоретическому материалу дисциплины, практическое применение которого осуществляется в ходе выполнения лабораторной работы.

Для получения максимальной оценки за лабораторную работу необходимо выполнить и защитить работу во время, отведенное для ее выполнения, согласно расписанию занятий. Допускается досрочное выполнение лабораторной работы по предварительной договоренности с преподавателем.

Выполнение всех лабораторных работ, предусмотренных рабочей программой дисциплины, является условием допуска к итоговому контролю изучения дисциплины.

2.1 Порядок выполнения лабораторных работ

1) изучить теоретический материал по теме лабораторной работы;

2) составить программу на одном из алгоритмических языков программирования для заданного варианта задания;

3) выполнить отладку составленной программы и показать преподавателю;

4) составить отчет по лабораторной работе.

5) защитить выполненную лабораторную работу.

2.2 Лабораторные работы

1. Методы донаучной криптографии.

2. Электронная цифровая подпись.

3. Практическое применение криптографии с открытым ключом.

2.3 Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.

2. Основные положения закона об информации, информационных технологиях и защите информации.

3. Основные положения закона о государственной тайне.

4. Основные положения закона о защите персональных данных.

5. Основные положения закона об электронной цифровой подписи.

6. Что такое «политика безопасности»?

7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?

8. Основные модели политик безопасности?

9. Приведите схему и объясните принцип работы блочного шифра.

10. Дайте характеристику шифра DES.

11. Дайте характеристику шифра ГОСТ 28147-89.

12. Чем отличается криптография с открытым ключом от симметричных шифров?

13. Опишите алгоритм RSA.

14. Что такое электронная цифровая подпись?

15. Что такое сертификат открытого ключа?

16. Опишите алгоритм цифровой подписи DSA (DSS).

17. Опишите алгоритм цифровой подписи ГОСТ Р3410-94.

18. Чем отличается аутентификация от идентификации?

19. Что такое авторизация?

20. Принципы использования многоразовых паролей?

3 Методические указания к проведению практических занятий

3.1 Общие положения

Практические занятия по дисциплине формируют навыки практического применения теоретических знаний, полученных во время изучения дисциплины.

Для каждого практического занятия определяется тема, вопросы для проведения фронтального опроса, порядок проведения занятия. Первая часть занятия, как правило, проводится в виде семинара, в ходе которого проводится обсуждение темы занятия и опрос студентов. Во второй части занятия студенты решают практические задания по индивидуальным вариантам.

3.2 Практические занятия

1. Федеральные законы в области информационной безопасности
2. Политики безопасности. Основные модели политики безопасности
3. Симметричные криптографические методы
4. Криптография с открытым ключом
5. Электронная цифровая подпись
6. Методы идентификации и проверки подлинности пользователей

3.2.1 Федеральные законы в области информационной безопасности

Основы российского законодательства в сфере защиты информации: закон об информации, информационных технологиях и защите информации; закон о государственной тайне; закон о защите персональных данных; закон об электронной цифровой подписи. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации.

Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных тех-

нологиях и защите информации.

3. Основные положения закона о государственной тайне.

4. Основные положения закона о защите персональных данных.

5. Основные положения закона об электронной цифровой подписи.

3.2.2 Политики безопасности. Основные модели политики безопасности

Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.

Контрольные вопросы

1. Что такое «политика безопасности»?

2. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?

3. В каких случаях применяются модели безопасности?

4. Основные модели политик безопасности?

3.2.3 Симметричные криптографические методы

Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

Контрольные вопросы

1. Принципы, используемые для повышения стойкости шифра?

2. Приведите схему и объясните принцип работы блочного шифра.

3. Дайте характеристику шифра DES.

4. Дайте характеристику шифра ГОСТ 28147-89.

5. Перечислите основные различия между DES и ГОСТ 28147-89.

6. Что такое – режим применения блочного шифра?

3.2.4 Криптография с открытым ключом

Основные способы использования алгоритмов с открытым ключом. Шифр Шамира. Шифр Эль-Гамаля. Алгоритм RSA. Вопросы стойкости. Задача распределения ключей. Метод Диффи-Хеллмана

Контрольные вопросы

1. Чем отличается криптография с открытым ключом от симметричных шифров?

2. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?

3. Опишите алгоритм Шамира.

4. Опишите алгоритм Эль-Гамаля.

5. Опишите алгоритм RSA.

3.2.5 Электронная цифровая подпись

Общие сведения об электронной цифровой подписи (ЭЦП). Основные способы использования ЭЦП. Алгоритмы ЭЦП с открытыми ключами – RSA, DSA, ГОСТ Р34.10–94.

Контрольные вопросы

1. Опишите алгоритм цифровой подписи RSA.

2. Опишите алгоритм цифровой подписи Эль-Гамаля.

3. Опишите алгоритм цифровой подписи DSA (DSS).

4. Опишите алгоритм цифровой подписи ГОСТ Р3410-94.

5. Что такое сертификат открытого ключа?

3.2.6 Методы идентификации и проверки подлинности пользователей

Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации, использующие пароли и PIN-коды: на основе многоразовых паролей, на основе одноразовых паролей, на основе сертификатов. Строгая аутентификация, основанная: на симметричных алгоритмах, на асимметричных алгоритмах, на однонаправленных хеш-функциях. Биометрическая аутентификация пользователя.

Контрольные вопросы

1. Чем отличается аутентификация от идентификации?
2. Что такое авторизация?
3. Принципы использования многоразовых паролей?
4. Как получают одноразовые пароли?
5. Как используются сертификаты при аутентификации пользователей?

4 Методические указания для организации самостоятельной работы

4.1 Общие положения

Самостоятельная работа является важной составляющей в изучении дисциплины и состоит из следующих видов деятельности: проработка лекционного материала для подготовки к тестированию и контрольным работам, подготовка к лабораторным работам и практическим заданиям, выполнение контрольных работ, самостоятельное изучение тем курса.

Самостоятельная работа над теоретическим материалом направлена систематизацию и закрепление знаний, полученных на лекционных занятиях и на получение новых знаний по дисциплине, путем самостоятельного изучения тем.

Самостоятельная работа по подготовке к лабораторным работам и практическим занятиям направлена на изучение методического и теоретического материала по теме лабораторной работы или практического занятия.

Выполнение контрольных работ — полностью самостоятельная работа, направленная на получение навыков самостоятельного составления алгоритмов, реализацию программ, их дальнейшей отладки и тестирования.

4.2 Проработка лекционного материала, подготовка к лабораторным работам и практическим занятиям

Проработка лекционного курса является одной из важных активных форм самостоятельной работы. Этот вид самостоятельной работы может быть организован следующим образом:

1) прочитайте конспект лекции, согласуя Ваши записи с информацией на слайдах лекции;

2) попробуйте выполнить самостоятельно примеры программ, разобранных на лекции;

3) если в лекции рассматривался какой-либо алгоритм, попытайтесь выполнить этот алгоритм на тестовых данных без использования компьютерной программы; такой способ проработки материалов лекции покажет, правильно

ли Вы поняли идею алгоритма;

4) изучите дополнительные учебные материалы, рекомендованные преподавателем;

5) попытайтесь ответить на контрольные вопросы, которыми, как правило, заканчиваются разделы учебных пособий или учебников;

6) если после выполненной работы Вы считаете, что материал освоен не полностью, сформулируйте вопросы и задайте их преподавателю.

Методические указания к ведению конспектов лекций. Лекции по дисциплине проводятся с использованием слайдов. Но это не означает, что лекцию можно просто слушать. Ведение конспектов значительно повышает качество последующей проработки лекционного материала. В силу специфики дисциплины на слайдах лекций очень много алгоритмов, кодов программ, примеров демонстрации работы изучаемых алгоритмов. Но этот материал может быть бесполезен, если Вы не делаете записи в течение лекции, потому что большинстве случаев, комментарии по представленным на слайдах примерам, лектор выполняет в устной форме.

Можно рекомендовать распечатывать слайды перед лекцией и вести конспект непосредственно на бумажном варианте слайд-презентации.

Одной из форм текущего мониторинга уровня знаний по дисциплине являются контрольные работы.

Самостоятельная работа по подготовке к лабораторным работам и практическим занятиям по дисциплине состоит в изучении методических материалов по темам соответствующих видов аудиторных занятий.

Рекомендуется перед выполнением лабораторной работы изучить лекционный и методический материал по теме занятия, ознакомиться с алгоритмами, реализацию которых необходимо выполнить во время проведения занятия. Обратите особое внимание на порядок выполнения работы. Поскольку конечным результатом всех лабораторных работ является компьютерная программа, самостоятельно разработайте структурную схему будущей програм-

мы, выполните заготовку проекта, подготовьте самостоятельно тестовые данные.

Перед проведением практического занятия подготовьте ответы на вопросы, вынесенные для проведения входного контроля уровня знаний по теме занятия. Если при подготовке к занятию остались нерешенные вопросы, обратитесь за консультацией к преподавателю.

5 Рекомендуемые источники

1. Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578.

2. Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111016.

3. Информационная безопасность : учебное пособие / составители Е. Р. Кирколуп [и др.]. — Барнаул : АлтГПУ, 2017. — 316 с. — ISBN 978-5-88210-898-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112164.

4. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; под редакцией В. Н. Ясенева. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2017. — 198 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153011.