|  |  |  |
| --- | --- | --- |
| Методические рекомендации и указания |  | Форма  Ф СО ПГУ 7.18.2/05 |

Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Кафедра информатики и информационных систем

**МЕТОДИЧЕСКИЕ рекомендации и УКАЗАНИЯ**

к курсовым работам

по дисциплине Информационная безопасность и защита информации

для студентов специальности 050703 «Информационные системы»

Павлодар

|  |  |  |
| --- | --- | --- |
| Лист утверждения к методическим рекомендациям указаниям |  | Форма  Ф СО ПГУ 7.18.1/05 |

**УТВЕРЖДАЮ**

Декан ФФМиИТ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.К. Тлеукенов

«\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_200\_ г.

Составитель: Старший преподаватель Дзангиева Лидия Идрисовна

(должность, уч. степень, звание, подпись)

Кафедра Информатика и информационные системы

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

к курсовым работам

по дисциплине Информационная безопасность и защита информации

для студентов специальности 050703 «Информационные системы»

**Рекомендовано**  на заседании кафедры

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_200\_\_г., протокол №\_\_

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Нурбекова Ж.К.

(подпись)

ОдобреноУМС ФФМиИТ

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_200\_\_г., протокол №\_\_\_\_

Председатель УМС\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кишубаева А.Т.

(подпись)

**Одобрено ОПиМО:**

Начальник ОПиМО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ф.И.О. «**\_\_\_\_**»**\_\_\_\_\_\_\_\_\_\_\_\_\_**200\_г.

(подпись) (дата)

Одобрена учебно-методическим советом университета

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_200\_г. Протокол №\_\_\_\_

**Цель:** курсовая работа предназначена для закрепления теоретических и практических знаний, полученных при изучении материала рассматриваемой дисциплины.

**Рекомендуемые темы:**

***Темы 1-5. Программная реализация криптографической системы ГОСТ 28147-89***:

1. Основной шаг криптографического преобразования.
2. Шифрование и расшифрование в режиме простой замены.
3. Шифрование и расшифрование в режиме гаммирования.
4. Шифрование и расшифрование в режиме гаммирования с обратной связью.
5. Генерация и проверка имитовставки (совместно с любым из трех основных режимов).

Примечание: проекты по данным темам должны выполняться и защищаться совместно.

***Темы 6-12. Программная реализация криптографических систем DES, 3-DES и DESX***:

1. Основная функция шифрования.
2. Шифрование и расшифрование в режиме электронной кодовой книги (ECB).
3. Шифрование и расшифрование в режиме сцепления блоков шифра (CBC).
4. Шифрование и расшифрование в режиме обратной связи по шифротексту (CFB).
5. Шифрование и расшифрование в режиме обратной связи по выходу (OFB).
6. Шифрование и расшифрование по алгоритму 3-DES в одном из режимов.
7. Шифрование и расшифрование по алгоритму DESX в одном из режимов.

Примечание: проекты по данным темам должны выполняться и защищаться совместно.

***Темы 13-17. Разработка программы, защищенной от несанкционированного доступа и использующей различные способы аутентификации пользователей***:

1. Парольная аутентификация (аналогично лабораторной работе №1) с дополнительными средствами администрирования (задание максимального и минимального сроков действия пароля, ведение списка уже использованных паролей задаваемой максимальной длины).
2. Аутентификация пользователей на основе модели «рукопожатия».
3. Аутентификация пользователей по их «росписи» мышью.
4. Аутентификация пользователей по их клавиатурному почерку.
5. Аутентификация пользователей на основе их способности к запоминанию отображаемой на короткое время на экране информации.

***Темы 18-22. Разработка программных средств администрирования ОС Windows***:

1. Протоколирование в специальном файле событий, связанных с доступом других приложений к выбираемым информационным ресурсам (папкам, принтерам, разделам реестра).
2. Получение списка пользователей, имеющих право доступа к выбираемому информационному ресурсу (файлу, папке, принтеру, разделу реестра), с указанием имеющихся у них прав доступа.
3. Получение списка информационных ресурсов (файлов, папок, разделов реестра) к которым имеет доступ на чтение (запись) задаваемый пользователь.
4. Получение списка папок, к которым имеют право на чтение все пользователи системы.
5. Выявление легко подбираемых паролей пользователей (совпадающих с паролями из специального словаря или не удовлетворяющих задаваемым требованиям сложности).

Примечание: проекты по темам 19-22 выполняются для ОС Windows NT/2000/XP (по темам 19-21 – с файловой системой NTFS).

***Темы 23-24. Разработка программных средств защиты от несанкционированного копирования***:

1. Сбор, хеширование, вычисление ЭЦП и сохранение ее в реестре, вывод информации о структуре жесткого диска и параметрах BIOS компьютера.
2. Запись (чтение) не копируемой стандартными средствами метки на дискете.

***Темы 25-28. Разработка программных средств, выполняющих взаимную аутентификацию (создающих защищенный сеанс связи) двух хостов в сети на основе одного из криптографических протоколов***:

1. Трехфазный протокол Microsoft.
2. Протокол CHAP.
3. Протокол S/Key.
4. Протокол SSL.

***Темы 29-32. Разработка программных средств компьютерной стеганографии***:

1. Скрытие и извлечение информации в графических файлах.
2. Скрытие и извлечение информации в звуковых файлах.
3. Скрытие и извлечение информации в видеофайлах.
4. Скрытие и извлечение информации в текстовых файлах.

***Темы 33-35. Разработка защищенной почтовой клиентской программы***:

1. С автоматическим шифрованием (расшифрованием) сообщений и (или) присоединенных к ним файлов.
2. С автоматическим получением ЭЦП под сообщением и (или) присоединенных к нему файлов (при отправке сообщения) и проверкой ЭЦП (при получении сообщения).
3. С автоматической проверкой на вредоносные вложения с помощью одной из программ-сканеров.

***Темы 37-38. Разработка программ раскрытия паролей пользователей***:

1. Расшифрование паролей пользователей ОС Windows 9x/ME, хранящихся в pwl-файлах.
2. Получение паролей на загрузку ОС, установленных программой BIOS Setup и хранящихся в энергонезависимой (CMOS) памяти компьютера.

***Тема 39. Вирусы в макросах документов: способы внедрения, распространения и защиты***

* создание вирусов в макросах и их внедрение в различные типы файлов документов (.doc, .xls, .mdb, .htt и др.) с собственными иллюстративными примерами;
* обзор наиболее известных вирусов в макросах документов;
* распространение вирусов в макросах документов (с примерами);
* способы защиты от вирусов в макросах документов (организационные, «ручные», программные).

***Тема 40. Программные закладки: типы, способы внедрения и защиты***

* определение и классификация программных закладок;
* способы внедрения программных закладок с известными примерами;
* способы взаимодействия между программной закладкой и нарушителем;
* примеры известных программных закладок (BackOrifice, NetBus, DIRT, Paparazzi и

др.);

* способы защиты от программных закладок.

***Тема 41. Безопасность компьютерных систем на основе инфраструктуры открытых ключей***

* назначение и основные понятия инфраструктуры открытых ключей (Public Key Infrastructure);
* компоненты инфраструктуры открытых ключей;
* возможные применения инфраструктуры открытых ключей;
* реализация инфраструктуры открытых ключей в ОС Windows 2000/XP;
* другие реализации инфраструктуры открытых ключей;
* демонстрационные примеры использования инфраструктуры открытых ключей.

***Тема 42. Программно-аппаратные средства защиты информации фирмы АНКАД***

* общая характеристика средств защиты информации фирмы АНКАД;
* устройства криптографической защиты информации серии КРИПТОН;
* модификации платы КРИПТОН;
* программные эмуляторы платы КРИПТОН;
* средство защиты информации Crypton Office;
* другие программно-аппаратные средства защиты информации;
* примеры использования демонстрационных версий программных средств.

***Тема 43. Программные средства защиты информации серии «Верба»***

* общая характеристика и назначение программных продуктов серии «Верба»;
* средства криптографической защиты информации «Верба-OW» и «Верба-W»;
* библиотеки функций WSIGN, WSIGN(O), WBOTH, WBOTH(O);
* управление ключами с помощью средств криптографической защиты информации серии «Верба»;
* применение средств криптографической защиты информации серии «Верба» (с примерами);
* примеры использования демонстрационных версий программных средств.

***Тема 44. Программные средства защиты информации фирмы Инфотекс***

* общая характеристика и назначение программных продуктов фирмы Инфотекс;
* программное средство ViPNet[Клиент];
* программное средство ViPNet[Координатор];
* программное средство ViPNet[Персональный сетевой экран];
* программное средство ViPNet Office Firewall;
* программное средство Контроль приложений;
* программные средства для защиты электронной почты;
* примеры использования демонстрационных версий программных средств.

***Темы 45-49. Программная реализация асимметричных криптографических алгоритмов:***

1. Шифрование и расшифрование по алгоритму RSA.
2. Генерация сеансового ключа по методу Диффи-Хеллмана.
3. Получение и проверка ЭЦП по алгоритму Эль-Гамаля (ГОСТ Р 34.10-94).
4. Получение и проверка ЭЦП в криптосистеме на основе эллиптических кривых (ГОСТ Р. 34.10-2001).
5. Вычисление функции хеширования по алгоритму ГОСТ Р 34.11-94.

Примечание: проекты по темам 47, 49 и 48, 49 выполняются и защищаются совместно. Выполнение проекта по теме 49 предполагает использование результатов выполнения проектов по темам 1 и 2.

***Тема 50. Программные средства защиты информации на магнитных дисках:***

* система защиты конфиденциальной информации Strong Disk Pro;
* система защиты конфиденциальной информации Strong Disk Server и программное средство Strong Disk Remote Administrator;
* система защиты конфиденциальной информации Secret Disk;
* система защиты корпоративных серверов Secure NT;
* другие программные средства защиты информации на магнитных дисках;
* примеры использования демонстрационных версий программных средств.

***Тема 51. Разработка программных средств администрирования ОС Linux:***

Одна из тем 19-22, но применительно к ОС Linux.

***Тема 52. Программные средства защиты информации для ОС Linux:***

* оболочки (командные процессоры) с ограничением прав пользователя;
* ограниченная файловая система;
* системные средства шифрования файлов и каталогов;
* дополнительные программные средства шифрования файлов и каталогов;
* программные средства разграничения доступа к объектам на уровне отдельных пользователей;
* защищенные информационные системы («Утес-К» и другие);
* примеры практического использования рассмотренных программных средств.

***Тема 53. Программно-аппаратные средства защиты информационных ресурсов от несанкционированного использования и копирования:***

* средства защиты программ от статического анализа;
* средства защиты программ от динамического анализа;
* защита программ от исследования с помощью электронных ключей;
* электронные ключи Guardant и другие;
* сравнительный анализ эффективности рассмотренных средств защиты;
* критерии выбора средств защиты информационных ресурсов от несанкционированного использования и копирования.

***Тема 54. Средства аудита в операционных системах класса Unix:***

* аудит в Unix-системах: определение политики аудита, файлы аудита, реакция на события аудита;
* аудит событий безопасности, связанных с доступом к объектам (на примере файлового сервера Samba);
* аудит событий безопасности в коммерческих версиях Unix (Solaris, Unix System V Release 4 и др.);
* сравнительный анализ средств аудита в ОС Windows и Unix.

***Тема 55. Программные средства компьютерной стеганографии:***

* сущность, применение, методы компьютерной стеганографии, ее отличие от криптографии;
* обзор существующих программных средств компьютерной стеганографии, их достоинств и недостатков (contraband, steganos и др.);
* методы стегоанализа (обнаружения наличия скрытых сообщений в контейнерах);
* тенденции развития и возможные новые методы компьютерной стеганографии.

***Тема 56. Построение аппаратных компонент криптозащиты данных:***

* защита алгоритма шифрования;
* принцип чувствительной области и принцип главного ключа;
* необходимые и достаточные функции аппаратного средства криптозащиты;
* примеры аппаратных средств криптозащиты и их характеристики.

***Темы 57-61. Программная реализация функций хеширования:***

1. SHA.
2. MD2.
3. MD4.
4. MD5.
5. RIPEMD.

**Темы 62-65 Криптографические средства защиты**

1. Проектирование датчика случайных чисел с последующим исследованием его характеристик.
2. Написание программы блочного шифрования.
3. Создание программ - закладок.
4. Исследования статистических свойств зашифрованного текста (сравнительный анализ для различных методов шифрования).

**Темы 66-79 Принципы и методы оценки эффективности средств защиты информации.**

1. Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
2. Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
3. Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
4. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
5. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
6. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
7. Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями «Оранжевой книги».
8. Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
9. Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
10. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями «Оранжевой книги».
11. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
12. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
13. Оценка защищенности ОС Windows XP Professional (NT, 2000) в соответствии со стандартами ISO.
14. Оценка защищенности ОС Linux в соответствии со стандартами ISO.

**Тема 80-97 Анализ методов и средств систем защиты информации.**

1. Сравнительный анализ антивирусных пакетов.
2. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.
3. Сравнительный анализ систем обнаружения атак.
4. Сравнительный анализ межсетевых экранов.
5. Оценка защищенности межсетевых экранов компании «Инфотекс» в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
6. Сравнение анализаторов безопасности компьютерных систем.
7. Сравнительный анализ средств защиты электронной почты.
8. Анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им.
9. Анализ методов нарушения безопасности сетевых ОС и методов противодействия им.
10. Анализ методов организации антивирусной защиты компьютерных систем.
11. Сравнительный анализ персональных брандмауэров.
12. Анализ средств безопасности в пакете Microsoft Office.
13. Анализ средств защиты от спама.
14. Анализ методов повышения надежности хранения информации на жестких магнитных дисках.
15. Анализ методов обеспечения безопасности электронного магазина.
16. Анализ методов обеспечения безопасности домашней сети.
17. Анализ средств защиты компакт-дисков от несанкционированного копирования.
18. Анализ методов гарантированного удаления конфиденциальной информации на электронных носителях.

**Тема 97-101 Разработка по и средств для защиты информаци**

1. Разработка лабораторного практикума по изучению подсистемы безопасности ОС Linux.
2. Использование языка сценариев ОС Windows для разграничения прав пользователей компьютерных систем.
3. Разработка макета персонального брандмауэра.
4. Разработка дополнительных средств администрирования ОС Windows XP Professional (NT, 2000).

**Методические рекомендации по выполнению задания, в том числе по использованию ЭВМ или других технических средств:**

**Материально-техническое обеспечение дисциплины**

Класс ПЭВМ не ниже Intel Pentium 166, 64 Mb RAM, 2 Gb HDD с

установленным программным обеспечением: Microsoft Windows NT 4.0, Microsoft Windows 2000 Professional, Microsoft Visual C++, Linux. Из расчета одна ПЭВМ на человека.

**Содержание задания, объём и условия выполнения работы**

**бюджет времени**

По темам, не связанным с проектированием и (или) разработкой программных средств (темы 39-44, 50, 52-56), необходимо при выполнении курсовой работы:

* отразить все пункты, конкретизирующие тему курсовой работы;
* при возможности установить и изучить демонстрационные версии анализируемых программных средств, отразить эти результаты в записке к курсовой работе;
* при невозможности установить анализируемые программные средства отразить в отчете сведения об их характеристиках и применении, полученные из различных источников (не только от производителей этих средств);
* подготовить пояснительную записку к курсовой работе;
* подготовить текст выступления (на 7-8 минут) на защите курсовой работы;
* подготовить 2-3 комплекта слайдов (формата А4) с иллюстративным материалом для защиты.

Оценка за курсовую работу, выполненный по темам, которые не связаны с проектированием и (или) разработкой программных средств, будет выставлена по итогам публичной защиты работы с представлением пояснительной записки к работе.

По темам, связанным с проектированием и (или) разработкой программных средств, необходимо при выполнении курсовой работы:

* спроектировать (изучить, если задан) алгоритм решения поставленной задачи и записать его в виде псевдокода или структурной схемы (блок-схемы);
* разработать проект пользовательского интерфейса для программной реализации алгоритма (структуры главного меню и диалоговых форм);
* реализовать алгоритм на языке программирования C++;
* создать макет программы в системе C++ Builder для реализации разработанного пользовательского интерфейса;
* выполнить тестирование и отладку программы;
* подготовить пояснительную записку к курсовому проекту.

Оценка за курсовую работу, выполненный по темам, которые связаны с проектированием и (или) разработкой программных средств, будет выставлена по итогам демонстрации их работы и просмотра текстов разработанных программ с представлением пояснительной записки к проекту. Возможна защита курсовой работы без выполнения полного тестирования и отладки разработанной программы.

**Требования к содержанию и оформлению:**

Структура пояснительной записки к курсовой работе:

* титульный лист с указанием названий университета, факультета, кафедры, учебной дисциплины, вида задания (курсовая работа), темы курсовой работы, студенческой группы, фамилий и инициалов студента и преподавателя, города и года выполнения работы;
* содержание с указанием номеров страниц;
* введение с развернутой постановкой задачи и кратким содержанием пояснительной записки;
* основная часть, разделенная на имеющие нумерацию главы (разделы) и (при необходимости) подразделы;
* заключение с выводами и основными результатами выполненной работы;
* список использованных источников;
* приложение (тексты разработанных программ, инструкции по их применению и т.п.).

**Список рекомендуемой литературы.**

***Основная***

1. Домашев А.В., Попов В.О., Правиков Д.И., Прокофьев И.В., Щербаков А.Ю. Программированием алгоритмов защиты информации. Учебное пособие -М.: «Нолидж», 2000,-288с.

2.Зегджа Д.П., Ивашко A.M. Основы безопасности информационных систем. - М: Горячая линия-Телеком.2000.-452с,

3. Милославская Н.Г. Толстой А.И, Интрасети: доступ в Internet, защита: Учебное пособие для вузов. - М.: ЮНИТИ-ДАНА, 2000.-527 с.

4. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие, Алматы: КазНТУ, 2000-125с. ISB 9965-487-36-7

***Дополнительная***

5. Алин Б. Защита компьютерной информации. - СПб.: БХВ-Санк-Петербург, 2000.- 384с.

6. Герасименко В. А. Защита информации в автоматизированныхсистемах обработки данных. Книга 1,2 М.; Энергоатомиздат, 1994 .-176 с.

7. Гостехкомиссия РФ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. — М.: Воениздат, 1992.

8. Грушо А. А., ТимонинаЕ.Е. Теоретические основы защиты информации.- Издательство агентства «Яхтсмен » М.- 1996 -71с.

9. Гульев И.А. Компьютерные вирусы взгляд изнутри - М.: ДМКД 1998-304 с.

10. Мафтик С. Механизмы защиты в сетях ЭВМ. — М.: Мир, 1993.-216с.

11. Мельников В. В. Защита информации в компьютерных системах Москва «Финансы и статистика» «Электроинформ» 1997. -368с.

12. Расторгуев СП. Программные методы защиты информации в компьютерах и сетях Издательство агентства «Яхтсмен » М.-, 1991. -368с

3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях /Под ред. В.Ф. Шаньгина,- М.; Радио и связь, 1999.-328 с.

14. Салома А. Криптография с открытым ключом. Пер. с англ. — М: Мир, 1996.~304с.

15. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. — М.: Сов. радио, 198О.-2б4с.