МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)
АВИАЦИОННЫЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Директор колледжа
_____ А.И. Азарова
личная подпись инициалы, фамилия
«___»_____2021г
Рег. № _____

Методические указания по выполнению практических занятий по дисциплине ОП.13 Информационная безопасность для обучающихся на специальности 09.02.07 Информационные системы и программирование

Ростов-на-Дону
2021

Практическое занятие №1
«Практическое использование законодательства в области лицензирования и сертификации»

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

1. Учебные вопросы

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №1 «Российское законодательство в области информационной безопасности», используя литературу [1, с.7-98; 2, с.3-7; 3-11], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация».
3. В чем заключается двуединство документированной информации с правовой точки зрения.
4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
10. Назовите основные цели государства в области обеспечения информационной безопасности.
11. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
12. Какой закон определяет понятие «официальный документ»?

13. Какой закон определяет понятие «электронный документ»?
14. В тексте какого закона приведена классификация средств защиты информации?
15. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
16. Назовите основные положения Доктрины информационной безопасности РФ.
17. Назовите составляющие правового института государственной тайны.
18. В каких случаях нельзя относить информацию к государственной тайне?
19. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
20. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.
21. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
22. Что в соответствии с законодательством РФ представляет собой засекречивание информации.
23. Перечислите основные принципы засекречивания информации.
24. Что понимается под профессиональной тайной?
25. Какие виды профессиональных тайн вам известны?
26. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?
27. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
28. Что представляет собой электронная цифровая подпись?
29. Каковы основные особенности правового режима электронного документа?
30. Назовите основные ограничения на использование электронных документов?

Практическое занятие №2
«Защита информации передаваемой по локальным сетям»

Цель занятия – закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации.

1. Учебные вопросы

1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.
3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №2 «Государственное лицензирование деятельности в области защиты информации», используя литературу [1, с.45-55; 2-8], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы государственного лицензирования в области защиты информации, порядка

лицензирования и контроля лицензиатов, изучения видов деятельности предприятий в области защиты информации, подлежащих лицензированию, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?
10. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
11. Какие средства относятся к шифровальным?
12. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
13. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
14. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
15. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.
16. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Практическое занятие №3
«Установка и настройка защищенных программ»

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств защиты информации по требованиям безопасности информации.

1. Учебные вопросы

1. Система сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Виды и схемы сертификации средств защиты информации.
4. Функции ФСТЭК в области сертификации средств защиты информации.
5. Функции органов сертификации средств защиты информации.
6. Функции испытательных лабораторий (центров).
7. Функции заявителей.
8. Порядок проведения сертификации и контроля.

9. Перечень средств защиты информации, подлежащих сертификации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №3 «Сертификация средств защиты информации по требованиям безопасности информации», используя литературу [1, с.56-80; 2,3], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации средств защиты информации, порядка сертификации и контроля, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Назовите виды и схемы сертификации средств защиты информации.
4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
5. Каковы функции органов сертификации средств защиты информации?
6. Каковы функции испытательных лабораторий (центров).
7. Каковы функции заявителей?
8. Общий порядок проведения сертификации средств защиты информации.
9. Виды контроля в области сертификации средств защиты информации.
10. Чем определяются сроки проведения сертификационных испытаний?
11. На какой срок выдается сертификат?
12. Назовите причины приостановления или аннулирования действия сертификата.

Практическое занятие №4
«Приемы работы с защищенными программами»

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств криптографической защиты информации.

1. Учебные вопросы

1. Система сертификации средств криптографической защиты информации.
2. Виды и схемы сертификации средств криптографической защиты информации.
3. Функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации.
4. Особенности подготовки и проведения сертификации криптографических средств защиты информации.
5. Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №3 «Сертификация средств защиты информации по требованиям безопасности информации», используя литературу [1, с.81-88; 2], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации средств криптографической защиты информации, особенностей подготовки, проведения сертификации средств криптографической защиты информации и контроля за сертифицированной продукцией, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации средств криптографической защиты информации.
2. Назовите виды и схемы сертификации средств криптографической защиты информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств криптографической защиты информации?
4. Особенности порядка подготовки и проведения сертификации средств криптографической защиты информации.
5. Виды контроля в области сертификации средств криптографической защиты информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Какие средства относятся к шифровальным?
9. Что относится к закрытым телекоммуникационным системам и комплексам?

Практическое занятие №5
«Защита информации от копирования: задание некопируемых меток»

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств вычислительной техники и связи.

1. Учебные вопросы

1. Система сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Виды и схемы сертификации средств вычислительной техники и связи.
3. Особенности подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №3 «Сертификация средств защиты информации по требованиям безопасности информации», используя литературу [1, с.89-98; 2], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации, особенностей подготовки, проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Назовите показатели защищенности.
9. Сколько классов защищенности существует?

Практическое занятие №6
«Защита программ от дисассемблирования»

Цель занятия – закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации объектов информатизации по требованиям безопасности информации.
3. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
4. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
5. Порядок проведения аттестации и контроля.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №4 «Аттестация объектов информатизации по требованиям безопасности ин-

формации», используя литературу [1, с.129-139; 2,3], а также конспект лекций.
При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.
2.2. Порядок проведения занятия
Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.
Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации объектов информатизации по требованиям безопасности информации и контроля, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.
По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Организационная структура системы объектов информатизации по требованиям безопасности информации.
3. Виды аттестации объектов информатизации по требованиям безопасности информации.
4. Какие объекты информатизации подлежат обязательной аттестации?
5. Каковы функции ФСТЭК в области аттестации объектов информатизации по требованиям безопасности информации?
6. Каковы функции органов по аттестации?
7. Каковы функции заявителей в области аттестации объектов информатизации по требованиям безопасности информации?
8. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
9. На основе каких сведений разрабатывается программа аттестационных испытаний?
10. Порядок проведения аттестационных испытаний.
11. Какая документация представляется органу по аттестации?

Практическое занятие №7
«Идентификация и аутентификация в программных продуктах»

Цель занятия – закрепление теоретических знаний по вопросам аттестации помещений по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Особенности проведения аттестации помещений по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию
В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №4 «Аттестация объектов информатизации по требованиям безопасности информации», используя литературу [1, с.129-139; 2,3], а также конспект лекций.
При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации помещений по требованиям безопасности информации и контроля, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Какие помещения подлежат обязательной аттестации?
4. Порядок проведения аттестации помещений по требованиям безопасности информации.
5. Какая документация представляется органу по аттестации?
6. Содержание заключения аттестационной проверки помещения.
7. Содержание протокола аттестационных испытаний помещения.
8. Содержание аттестата соответствия на объект информатизации.

Практическое занятие №8
«Установка резидентных программ»

Цель занятия – закрепление теоретических знаний по вопросам аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации.

1. Учебные вопросы

1. Понятие аккредитации предприятий в качестве органов по сертификации средств защиты информации.
2. Порядок аккредитации предприятия.
3. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов сертификации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №5 «Аккредитации органов сертификации (испытательных лабораторий) средств защиты информации по требованиям безопасности информации», используя литературу [1, с.99-102; 2-4], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся порядка аккредитации предприятий, контроля и надзора за деятельностью аккредитованных предприятий, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аккредитации предприятия в качестве органа по сертификации средств защиты информации.
2. Дайте определение аккредитации предприятия в качестве испытательной лаборатории.
3. Порядок аккредитации предприятия в качестве органа по сертификации (испытательной лаборатории) средств защиты информации.
4. На какой срок выдается аттестат аккредитации?
5. Виды контроля за деятельностью аккредитованных предприятий.
6. Перечислите случаи, в которых аккредитация может быть досрочно аннулирована.

Практическое занятие №9
«Защита программ в оперативной памяти»

Цель занятия – закрепление теоретических знаний о функциях, правах, обязанностях, ответственности и других аспектах деятельности испытательной лаборатории при проведении сертификационных испытаний.

1. Учебные вопросы

1. Испытательная лаборатория, как составная часть организационной структуры системы сертификации продукции по требованиям безопасности информации.
2. Основные задачи испытательной лаборатории.
3. Основные функции испытательной лаборатории.
4. Права, обязанности и ответственность испытательной лаборатории.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №6 «Испытательная лаборатория (центр)», используя литературу [1, с.103-108; 2-4], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся функций, прав, обязанностей, ответственности и других аспектах деятельности испытательной лаборатории при проведении сертификационных испытаний, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Кто осуществляет руководство деятельностью испытательной лаборатории?
2. Чем должна располагать испытательная лаборатория для проведения сертификационных испытаний?
3. Перечислите задачи испытательной лаборатории.
4. Перечислите функции испытательной лаборатории.
5. Какие документы готовит испытательная лаборатория по окончании сертификационных испытаний?

6. Какие права имеет испытательная лаборатория?
7. Перечислите обязанности испытательной лаборатории.
8. Какие требования предъявляются к сотрудникам испытательной лаборатории?
9. Какой документацией должна располагать испытательная лаборатория?
10. Какими помещениями должна располагать испытательная лаборатория?
11. Ответственность испытательной лаборатории.

Практическое занятие №10
«Пакеты антивирусных программ»

Цель занятия – закрепление теоретических знаний о условиях, порядке и объеме проведения испытаний объектов.

1. Учебные вопросы

1. Объекты испытаний.
2. Цели и задачи проверок и испытаний.
3. Условия и порядок проведения испытаний.
4. Методы испытаний.
5. Испытания объектов на соответствие организационно-техническим требованиям по защите информации.
6. Испытания объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.
7. Испытания объектов на соответствие требованиям по защите информации от несанкционированного доступа (НСД).
8. Проверка правильности применения криптографических средств защиты информации.
9. Испытания объекта на соответствие требованиям по защите информации от утечки по акустическим каналам.
10. Проверка выполнения требований по защите информации от утечки за счет строенных технических средств.
11. Оценка результатов испытаний и оформление отчетных материалов.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №6 «Испытательная лаборатория (центр)», используя литературу [1, с.109-128; 2, с. 129-246; 3,4],а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся условий, порядка и объема проведения испытаний объектов, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Перечислите объекты испытаний.
2. Назовите цели и задачи испытаний и проверок.
3. Каковы условия проведения испытаний?

4. Порядок проведения испытаний.
5. Перечислите общие методы испытаний.
6. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
7. Методы испытаний объектов на соответствие организационно-техническим требованиям по защите информации.
8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
9. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН средств вычислительной техники (СВТ).
10. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН СВТ.
11. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.
12. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.
13. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.
14. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.
15. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.
16. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.
17. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД.
18. Виды испытаний объектов на соответствие требованиям по защите информации от НСД.
19. Методы испытаний объектов на соответствие требованиям по защите информации от НСД.
20. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам.
21. В чем состоит суть проверки выполнения требований по защите информации от течки за счет встроенных технических средств.
22. В чем состоит суть проверки правильности применения криптографических средств защиты информации.
23. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

Практическое занятие 11
«Инсталляция и настройка антивирусных программ»

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

1. Учебные вопросы

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №1 «Российское законодательство в области информационной безопасности», используя литературу [1, с.7-98; 2, с.3-7; 3-11], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

31. Охарактеризуйте информацию и ее основные показатели.
32. Какие существуют подходы к определению понятия «информация».
33. В чем заключается двуединство документированной информации с правовой точки зрения.
34. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
35. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
36. Назовите основные виды конфиденциальной информации.
37. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
38. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
39. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
40. Назовите основные цели государства в области обеспечения информационной безопасности.
41. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
42. Какой закон определяет понятие «официальный документ»?
43. Какой закон определяет понятие «электронный документ»?
44. В тексте какого закона приведена классификация средств защиты информации?
45. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
46. Назовите основные положения Доктрины информационной безопасности РФ.
47. Назовите составляющие правового института государственной тайны.
48. В каких случаях нельзя относить информацию к государственной тайне?
49. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
50. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.
51. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
52. Что в соответствии с законодательством РФ представляет собой засекречивание информа-

ции.
53. Перечислите основные принципы засекречивания информации.
54. Что понимается под профессиональной тайной?
55. Какие виды профессиональных тайн вам известны?
56. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?
57. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
58. Что представляет собой электронная цифровая подпись?
59. Каковы основные особенности правового режима электронного документа?
60. Назовите основные ограничения на использование электронных документов?

Практическое занятие 12
«Сравнительный анализ работы антивирусных программ»

Цель занятия – закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации.

1. Учебные вопросы

1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.
3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №2 «Государственное лицензирование деятельности в области защиты информации», используя литературу [1, с.45-55; 2-8], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы государственного лицензирования в области защиты информации, порядка лицензирования и контроля лицензиатов, изучения видов деятельности предприятий в области защиты информации, подлежащих лицензированию, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.

6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?
10. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
11. Какие средства относятся к шифровальным?
12. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
13. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
14. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
15. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.
16. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Практическое занятие 13
«Обнаружение современных вредоносных программ»

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств криптографической защиты информации.

1. Учебные вопросы

1. Система сертификации средств криптографической защиты информации.
2. Виды и схемы сертификации средств криптографической защиты информации.
3. Функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации.
4. Особенности подготовки и проведения сертификации криптографических средств защиты информации.
5. Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №3 «Сертификация средств защиты информации по требованиям безопасности информации», используя литературу [1, с.81-88; 2], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации средств криптографической защиты информации, особенностей подготовки, проведения сертификации средств криптографической защиты информации и контроля за сертифицированной продукцией, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руко-

водством преподавателя.
По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации средств криптографической защиты информации.
2. Назовите виды и схемы сертификации средств криптографической защиты информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств криптографической защиты информации?
4. Особенности порядка подготовки и проведения сертификации средств криптографической защиты информации.
5. Виды контроля в области сертификации средств криптографической защиты информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Какие средства относятся к шифровальным?
9. Что относится к закрытым телекоммуникационным системам и комплексам?

Практическое занятие 14
«Методы предотвращения заражения вредоносными программами»

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств вычислительной техники и связи.

1. Учебные вопросы

1. Система сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Виды и схемы сертификации средств вычислительной техники и связи.
3. Особенности подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №3 «Сертификация средств защиты информации по требованиям безопасности информации», используя литературу [1, с.89-98; 2], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации, особенностей подготовки, проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Назовите показатели защищенности.

Практическое занятие 15
Удаление вредоносного программного обеспечения»

Цель занятия – закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации объектов информатизации по требованиям безопасности информации.
3. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
4. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
5. Порядок проведения аттестации и контроля.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №4 «Аттестация объектов информатизации по требованиям безопасности информации», используя литературу [1, с.129-139; 2,3], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации объектов информатизации по требованиям безопасности информации и контроля, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности

информации.
2. Организационная структура системы объектов информатизации по требованиям безопасности информации.
3. Виды аттестации объектов информатизации по требованиям безопасности информации.
4. Какие объекты информатизации подлежат обязательной аттестации?
5. Каковы функции ФСТЭК в области аттестации объектов информатизации по требованиям безопасности информации?
6. Каковы функции органов по аттестации?
7. Каковы функции заявителей в области аттестации объектов информатизации по требованиям безопасности информации?
8. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
9. На основе каких сведений разрабатывается программа аттестационных испытаний?
10. Порядок проведения аттестационных испытаний.
11. Какая документация представляется органу по аттестации?
12. Что такое технический паспорт объекта информатизации и какие сведения о объекте он включает в себя?
13. В чем состоит содержание специального исследования аттестуемого объекта информатизации?
14. Цель и содержание специальных обследований и проверок.
15. Проведение измерения и оценка уровней защищенности.
16. Какие измерения дополнительно проводятся при использовании на объекте информатизации систем активной защиты?
17. Содержание заключения аттестационной проверки объекта информатизации.
18. Содержание протокола аттестационных испытаний объекта информатизации.
19. Содержание аттестата соответствия на объект информатизации.
20. Ответственность за выполнение установленных условий функционирования аттестованного объекта информатизации.

Практическое занятие 16
«Методы обнаружение каналов утечки информации»

Цель занятия – закрепление теоретических знаний по вопросам аттестации помещений по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Особенности проведения аттестации помещений по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №4 «Аттестация объектов информатизации по требованиям безопасности информации», используя литературу [1, с.129-139; 2,3], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации помещений по требованиям безопасности информации и контроля, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Какие помещения подлежат обязательной аттестации?
4. Порядок проведения аттестации помещений по требованиям безопасности информации.
5. Какая документация представляется органу по аттестации?
6. Содержание заключения аттестационной проверки помещения.
7. Содержание протокола аттестационных испытаний помещения.
8. Содержание аттестата соответствия на объект информатизации.

Практическая работа № 17
«Защита информации в каналах утечки информации»

1. Цель работы

Ознакомиться с алгоритмами оценки риска информационной безопасности.

2. Краткие теоретические сведения

Риск ИБ – потенциальная возможность использования определенной ***угрозой уязвимостей актива*** или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

3. Задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Практическая работа № 18.
«Обнаружение каналов утечки информации»

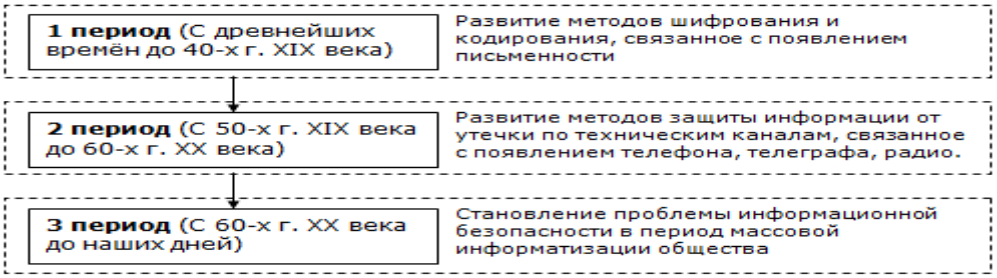
1. Цель работы

Ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах.

2. Краткие теоретические сведения

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории РФ средств и методов обеспечения ИБ основаны на импортных методиках и строятся из импортных компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим прежде чем приступить к изучению непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

3. Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. ″Системы защиты информации в ведущих зарубежных странах" и другие доступные источники информации.
2. Заполнить таблицу " Системы обеспечения ИБ в ведущих зарубежных странах "(см. вариант) на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

Практическая работа № 18
«Программные средства защиты от несанкционированного доступа к защищаемой информации»

1. Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом

особенностей его информационной инфраструктуры.

2. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – **Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Практическая работа № 19

«Восстановление работоспособности защиты каналов от утечки информации»

1. Цель работы

Изучение технологии аутентификации пользователя на основе пароля.

2. Краткие теоретические сведения

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

3. Задание

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:

1. В качестве информационного ресурса использовать любой файл или приложение.

Для справки: работа с текстовым файлом в среде Delphi:

```
  var
  myFile : TextFile;
  text   : string;
egin
  // Попытка открыть файл Test.txt для записи
  AssignFile(myFile, 'Test.txt');
  ReWrite(myFile);
  // Запись нескольких известных слов в этот файл
  WriteLn(myFile, 'Hello');
  WriteLn(myFile, 'World');
  // Закрытие файла
  CloseFile(myFile);
  // Открытие файла в режиме только для чтения
  FileMode := fmOpenRead;
  Reset(myFile);
  // Показ содержимого файла
  while not Eof(myFile) do
  begin
    ReadLn(myFile, text);
    ShowMessage(text);
  end;
  // Закрытие файла в последний раз
  CloseFile(myFile);
end;
```

2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.

Для справки: Пример поиска элемента в массиве (Delphi):

```
// ввод массива for i:=l to SIZE do
a[i] := StrToInt(StringGridl.Cells[i - 1, 0]);
// ввод образца для поиска
obr := StrToInt(edit2.text);
// поиск
found := FALSE; // пусть нужного элемента в массиве нет
i := 1;
repeat
  if a[i] = obr then
    found := TRUE
  else
    i := i + 1;
until (i > SIZE) or (found = TRUE);
```

3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.

4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

Практическая работа № 20

«Методы шифрование конфиденциальных данных»

1. Цель работы

Знакомство с основными методами криптографической зашиты информации.

2. Краткие теоретические сведения

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т

Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О

З	Т	О	Г	О		З	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.
2. Получатель выбирает целое число e ($1<e<\varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

3. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1(\text{mod } \varphi(n))$.

Пара чисел **(d,n)** является **секретным ключом**.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod(n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod (n)}$.

3. Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).
2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

Практическая работа №21
«Программное обеспечение для шифрования и дешифрования конфиденциальной информации»

1. Цель работы

Изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

2. Теоретические сведения

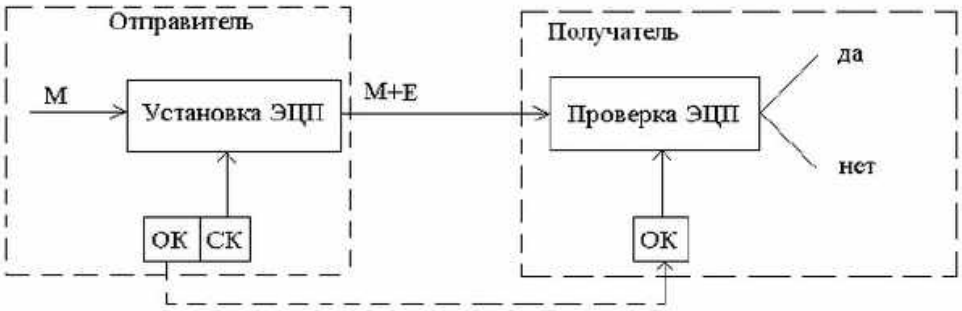
В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумыш-

ленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭЦП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭЦП использует секретный ключ отправителя сообщения, а процедура проверки ЭЦП – открытый ключ отправителя сообщения (рис. 1). Здесь



M – электронный документ, E – электронно-цифровая подпись.

Рис. 1 – Схема использования ЭЦП

В технологии ЭЦП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

Схема установки ЭЦП (рис. 2):

1. Для документа M формируется дайджест H с помощью заданного алгоритма хэширования.

2. Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭЦП.

3. Сообщение M и его ЭЦП передаются получателю сообщения.

Рис. 2 – Схема установки ЭЦП.

Схема проверки ЭЦП (рис. 3):

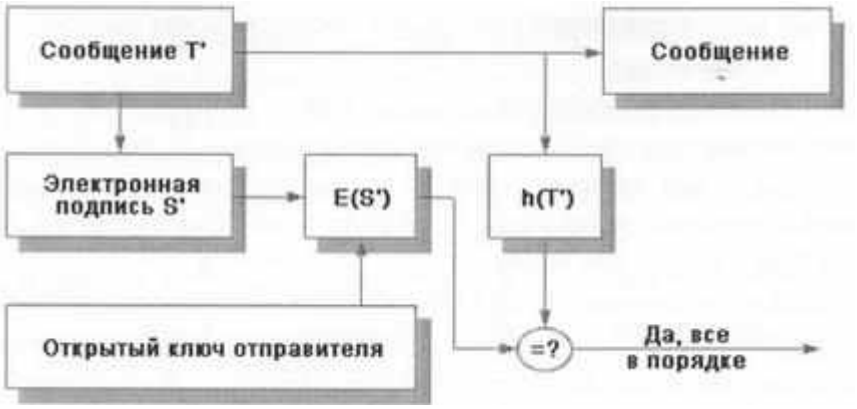
1. Получатель для проверки ЭЦП должен иметь доступ к самому сообщению М и его ЭЦП.

2. Зная алгоритм хэширования, который был использован при установке ЭЦП, получатель получает дайджест Н1 присланного сообщения М.

3. Зная открытый ключ отправителя, получатель дешифрует ЭЦП, в результате чего получает дайджест Н2, сформированный на этапе установки ЭЦП.

4. Критерием целостности присланного сообщения М и подтверждения его автора является совпадение дайджестов Н1 и Н2. Если это равенство не выполнено, то принимается решение о некорректности ЭЦП.

Рис. 3 – Схема проверки ЭЦП.



3. Задание

Сформировать ЭЦП к сообщению М' (см. вариант) и произвести проверку целостности принятого сообщения.

Порядок выполнения работы:

1. Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.

2. На стороне отправителя выполнить следующие действия:

2.1. Записать сообщение М (см. вариант).

2.2. Сформировать профиль сообщения М’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.

2.3. Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).

3. На стороне получателя выполнить следующие действия:

3.1. Записать сообщение М (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).

3.2. Сформировать профиль принятого сообщения, М’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).

3.3. Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (e, n) см. в таблице с вариантами задания).

3.4 Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.

Практическая работа № 22
«Программное обеспечение для шифрования и дешифрования конфиденциальной информации»

1. Цель работы

Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.

2. Краткие теоретические сведения

Исторически первое определение компьютерного вируса было дано в 1984 г. Фредом Коэном: «Компьютерный вирус — это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются *способность вируса к саморазмножению* и *способность к модификации вычислительного процесса*.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

• способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);

• наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Указанные свойства следует дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация по *среде обитания*, или по *типам объектов* компьютерной системы, в которые внедряются вирусы. В соответствии с этой классификацией вирусы делятся на файловые, загрузочные, сетевые (черви) и макровирусы.

Существует также много комбинированных типов компьютерных вирусов.

Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это троянские программы, логические бомбы, хакерские утилиты скрытого администрирования удаленных компьютеров, программы, ворующие пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т. д.

3. Задание

Разработать программу имитирующую некоторые (см. вариант) действия вируса или другой вредоносной программы и подготовить отчет о проделанной работе.

Практическая работа № 23
«Права и обязанности сотрудников службы безопасности»

1. Цель работы

Знакомство с некоторыми алгоритмами предупреждения и обнаружения вирусных угроз.

2. Краткие теоретические сведения

Для зашиты от компьютерных вирусов и других вредоносных программ могут использоваться:

• общие методы и средства защиты информации;

• специализированные программы для защиты от вирусов;

• профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Существуют две основные разновидности общих методов и средств защиты информации, также эффективных при борьбе вирусными угрозами:

•средства копирования информации;

• средства разграничения доступа.

При заражении компьютера вирусом важно его обнаружить. К внешним признакам

проявления деятельности вирусов можно отнести следующие:

• вывод на экран непредусмотренных сообщений или изображений;

• подача непредусмотренных звуковых сигналов;

• изменение даты и времени модификации файлов;

• исчезновение файлов и каталогов или искажение их содержимого;

• частые зависания и сбои в работе компьютера;

• медленная работа компьютера;

• невозможность загрузки ОС;

• существенное уменьшение размера свободной оперативной памяти;

• прекращение работы или неправильная работа ранее успешно функционировавших программ;

• изменение размеров файлов;

• неожиданное значительное увеличение количества файлов на диске.

Но мало заметить, что компьютерная система подверглась воздействию вредоносного ПО, необходимо обнаружить источник угрозы. К основным методам обнаружения компьютерных вирусов можно отнести следующие:

• метод сравнения с эталоном;

• эвристический анализ;

• антивирусный мониторинг;

• метод обнаружения изменений;

• встраивание антивирусов и др.

Различают следующие виды антивирусных программ:

• программы-фаги (сканеры);

• программы-ревизоры (CRC-сканеры);

• программы-блокировщики;

• программы-иммунизаторы.

Однако, абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение информации на дисках, необходимо выполнять следующие меры профилактики:

• применять только лицензионное ПО;

• оснастить компьютер современными антивирусными программами и постоянно возобновлять их версии;

• всегда проверять съемные носители информации на наличие вирусов (запуская антивирусные программы своего компьютера) перед считыванием с них информации, записанной на других компьютерах;

• при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

• периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков;

• всегда защищать съемные носители информации от записи при работе на других компьютерах, если на них не будет производиться запись информации;

• обязательно делать на съемных дисках архивные копии ценной для пользователя информации;

• использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

3. Задание

Разработать программу имитирующую некоторые (см. вариант) действия по предупреждению вирусных угроз, обнаружению и удалению вирусных и других вредоносных программ и подготовить отчет о проделанной работе.

Практическая работа № 24
«Правовое обеспечение информационной безопасности»

1. Цель работы

Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

2. Краткие теоретические сведения

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

3. Задание

4. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

   Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.
5. Заполнить таблицу " Пакеты антивирусных программ " на основе подготовленного материала, а также докладов других студентов.
6. Провести анализ собранной информации и сделать выводы.

Практическая работа № 25
«Основные виды компьютерных преступлений»

1. Цель работы

Ознакомиться с основными видами компьютерных преступлений.

2. Краткие теоретические сведения

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернет).

Виртуальная частная сеть базируется на трех методах реализации:

Туннелирование;

Шифрование;

Аутентификация.

Hamachi— это программа, позволяющая создать виртуальную частную сеть (VPN) через Интернет и объединить в ней несколько компьютеров. После создания такой сети пользователи могут устанавливать VPN-сессии между собой и работать в этой сети точно так же, как в обычной локальной (LAN) сети с возможностью обмена файлами, удаленного администрирования компьютеров и т.д. Преимущество VPN-сети заключается в том, что она полностью защищена от несанкционированного вмешательства и невидима из Интернета, хотя и существует в нем.

Программа Hamachi должна быть установлена на всех компьютерах, которые предполагается объединить в виртуальную частную сеть.

Виртуальная сеть создается с помощью специализированного сервера Hamachi в Интернете.

После того как с помощью сервера Hamachi создается виртуальная сеть между выбранными компьютерами, обмен информацией между клиентами VPN-сети происходит уже напрямую, то есть без участия сервера Hamachi. Для обмена данными между клиентами VPN-сети используется протокол UDP.

3. Задание

Задание рассчитано на работу в паре.

Порядок выполнения задания:

1. Загрузить программу "LogMeIn Hamachi" с сайта http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.
2. Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html
3. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).
4. Подготовить отчет.