МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
АЛЕКСАНДРОВСК-САХАЛИНСКИЙ КОЛЛЕДЖ (ФИЛИАЛ)
ФГБОУ ВПО «САХАЛИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ЦК естественно-математических и технических дисциплин
(название ЦК)

Ф.И.О. автора Ищенко Е.Ю.

Учебно-методический комплекс по дисциплине

СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ ВИРУСАХ, ЗАЩИТА ИНФОРМАЦИИ
(название)

Специальность: 230104.51 «Техническое обслуживание средств вычислительной техники и компьютерных сетей»
(код по ОКСО) (наименование специальности)

Согласовано:
Учебно-методический отдел
«30» сентября 2014 г.
Протокол №1

Рекомендовано ЦК:
Протокол № 1
«18» 09 2014 г.
Председатель ЦК

Александровск-Сахалинский

Автор-составитель:

Ищенко Евгений Юрьевич
(фамилия, имя, отчество)

преподаватель
(ученая степень, ученое звание, должность)

Учебно-методический комплекс Сведения о компьютерных вирусах, защита информации
(название дисциплины)

Учебно-методический комплекс по дисциплине «Сведения о компьютерных вирусах, защита информации» составлен в соответствии с требованиями Государственного образовательного стандарта среднего профессионального образования по специальности:

230106.51« Техническое обслуживание средств вычислительной техники и компьютерных сетей»
(наименование специальности)

Дисциплина входит в федеральный компонент цикла общепрофессиональных дисциплин и является обязательной для изучения.

Заместитель директора О.Н. Салангин

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Программа учебной дисциплины «Сведения о компьютерных вирусах, защита информации» предназначена для реализации государственных требований к минимуму содержания и уровню подготовки выпускников по специальности 230106.51 «Техническое обслуживание средств вычислительной техники и компьютерных сетей» среднего профессионального образования базового уровня и является единой для всех форм обучения, а также для всех типов и видов образовательных учреждений, реализующих основные профессиональные образовательные программы среднего профессионального образования.

Учебная дисциплина «Сведения о компьютерных вирусах, защита информации» является общепрофессиональной дисциплиной, устанавливающей базовые знания для освоения специальных дисциплин.

Защита информационных процессов в компьютерных системах (КС) – это дисциплина, в которой на основе системного анализа процессов получения, передачи, обработки и хранения информации сформулирована проблема защиты информации в КС; определены пространство угроз, методы и средства защиты от этих угроз; особенности угроз и соответствующих методов и средств защиты для локального компьютера, локальных вычислительных сетей и распределенных систем. В дисциплине на основе анализа реализуемых информационных процессов, свойств обрабатываемой информации, архитектуры КС, возможных видов угроз и моделей нарушителя/злоумышленника анализируются разработка политики безопасности, применяемой в системе, ее эффективность и возможности оптимизации.

Дается представление о современных методах и способах защиты электронной информации и возможных направлениях их развития, рассматривается защита локального (одиночного) компьютера от несанкционированного доступа и способы безопасной работы по обеспечению конфиденциальности информации и защиты компьютера, работающего в локальной и глобальной сетях.

Изучение дисциплины «Защита информационных процессов в компьютерных системах» необходимо будущим специалистам для формирования правильного представления по вопросам организации и осуществлению мероприятий связанных с использованием современных методов защиты информации в КС для обеспечения информационной безопасности организации (предприятия, фирмы).

Предмет курса излагается по определенной системе, обеспечивающей последовательное и понятное изложение изучаемой специальной дисциплины, и включает следующие разделы:

- основные виды информационных процессов в современных КС;
- проблема защиты информации в КС;
- защита локального компьютера и локальной вычислительной сети;
- защита распределенных систем с коммутацией через глобальные соединения;
- защита от компьютерных вирусов;
- криптография и шифрование данных;
- защита программного обеспечения КС.

2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Студент, изучающий дисциплину должен:

Иметь представление:

- о возможных уязвимостях информационных (компьютерных) систем и их ресурсов;
- общие представления о криптографии, шифровании и стеганографии для защиты электронной цифровой информации;
- о симметричной и асимметричной системах шифрования;
- о системе подтверждения подлинности информации, электронной цифровой подписи и электронных «водяных знаках»;

Знать:

- суть и содержание понятий «безопасность информации», «угрозы безопасности информации», «уязвимость информации», «защищённость информации», «утечка информации», «модификация информации», «несанкционированный доступ», «разрушающее программное воздействие» (РПВ), «компьютерный вирус», «криптография», «стеганография», «шифр», «ключ», «аппаратный ключ», «шифрование», «зашифрование», «расшифрование», «дешифрование», «криптостойкость», «электронная цифровая подпись»;
- классификацию угроз безопасности информации. Источники угроз. Методы защиты.
- программно-аппаратные методы и их место в комплексной системе защиты ИС;
- способы противодействия попыткам хищения информации или нарушения ее целостности;
- способы защиты программного обеспечения компьютерных систем от несанкционированного (контрафактного) использования;
- защиту сетевого компьютера и его ресурсов от проникновения из внешней сети;
- защиту от проникновения вирусов и троянских коней через сеть и различных носителей;
- классификацию компьютерных вирусов с позиции программно-аппаратных методов и алгоритмы работы известных типов компьютерных вирусов, а также соответствующие алгоритмы их нейтрализации.
- признаки заражения вирусами и основные правила защиты от компьютерных вирусах.

Уметь:

- находить основные уязвимости информационных систем;
- определять необходимые пути их устранения;
- настраивать систему безопасности локального и сетевого компьютеров;
- предотвращать потери информации на локальном компьютере;
- осуществлять защиту от несанкционированного доступа при загрузке файлов, папок, работе с логическими дисками и применять парольную защиту;
- обнаруживать сетевые атаки и защищаться от них;
- применять аппаратные ключи, методы биометрической идентификации;
- определять опасность вирусного заражения ресурсов ИС;
- владеть методикой эффективного использования антивирусных программ.

3. ОБЪЕМ ДИСЦИПЛИНЫ

3.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	***Количество часов по формам обучения***	
	очная	
№ семестра	***8***	
Аудиторные занятия	36	
Лекции	24	
Практические и семинарские занятия	12	
Самостоятельная работа	10	
ВСЕГО ЧАСОВ НА ДИСЦИПЛИНУ	46	
Текущий контроль (количество и вид текущего контроля)		
Виды промежуточного контроля (экзамен, зачет)	контрольная работа	

3.2. РАСПРЕДЕЛЕНИЕ ЧАСОВ ПО ТЕМАМ И ВИДАМ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Наименование разделов и тем	Всего	Виды учебных занятий			Самостоятельная работа
		Лекции	Практические\ Семинарские	Лабораторные работы	
Раздел 1. Проблема защиты информационных процессов в КС. Пространство угроз.		**8**	**4**		**2**
1. Проблема защиты электронной информации.	2	2			
2. Программные методы восстановления данных и активного профилактического обслуживания компьютера.	2	2			2
3. Место программно-математических	2	2			

методов в комплексной системе защиты информации.					
4. Обслуживание компьютера стандартными диагностическими программами, входящими в состав утилит операционных систем.	2		2		
5. Действия пользователей и безопасность данных.			2		
6. Работа с утилитами восстановления диска и данных	2	2			
Раздел 2. Защита локального и сетевого компьютеров		**6**	**4**		**4**
7. Предотвращение потери информации на локальном компьютере.	2	2			
8. Предотвращение потери информации при работе компьютера в сети.	2	2			
9. Программные установки и настройки систем защиты компьютера.	2	2			2
10. Защита локального компьютера с помощью паролей и с использованием программ-архиваторов.	2		2		
11. Настройка	2		2		2

системы защиты браузеров и почтовых клиентов.					
Раздел 3. Защита от компьютерных вирусов. Криптография и шифрование данных		**10**	**4**		**4**
12. Защита информации от компьютерных вирусов	2	2			
13. Криптография и шифрование данных	2	2			
14. Разновидности компьютерных вирусов и действия, выполняемые вирусами.	2	2			
15. Антивирусные программы.	2	2			2
16. Настройка и работа с антивирусной программой.		2			2
17. Ознакомление с программой шифрования PGP	2		2		
18. Контрольная работа.	2		2		
ИТОГО:	**36**	**24**	**12**		**10**

4. СОДЕРЖАНИЕ КУРСА

Раздел 1. Проблема защиты информационных процессов в КС. Пространство угроз

Тема 1. Проблема защиты электронной информации.

Суть и содержание понятий «безопасность информации», «угрозы безопасности информации», «уязвимость информации», «защищённость информации», «утрам информации», «утечка информации», «модификация информации».

Тема 2. Программные методы восстановления данных и активного профилактического обслуживания компьютера.

Классификация угроз безопасности информации. Источники угроз. Методы защиты. Программно-математические методы и их место в комплексной системе защиты информации.

Тема 3. Место программно-математических методов в комплексной системе защиты информации.

Способ представления данных в компьютере. Современные носители информации. Способ хранения информации на магнитных носителях. Структура магнитного диска. Процесс записи информации на магнитный диск. Файловая система FAT.

Тема 4. Обслуживание компьютера стандартными диагностическими программами, входящими в состав утилит операционных систем.

Ошибки файловой системы: суть, причины, способы исправление ситуации Дефрагментирование файлов. Алгоритмы удаления данных. Возможность восстановления потерянных и удалённых данных. Программы, обеспечивающие безопасность данных.

Тема 5. Действия пользователей и безопасность данных.

Действия пользователя и безопасность данных. Наиболее часто встречающиеся сообщения об ошибках и способы решения проблем с файловой системой. Сообщения об ошибках загрузки операционных систем и способы преодоления ситуации. Эффективные меры, повышающие шансы восстановления данных.

Тема 6. Работа с утилитами восстановления диска и данных.

Утилиты восстановления диска и данных. Утилиты восстановления данных на носителях. Создания загрузочных восстановительных дисков.

Раздел 2. Защита локального и сетевого компьютеров

Тема 7. Предотвращение потери информации на локальном компьютере.

Предотвращение потери информации на локальном компьютере. Защита от несанкционированного доступа при загрузке. Защита файлов, папок и логических дисков. Применение паролей. Временные файлы. Удаление временных файлов. Доступ к файлам.

Тема 8. Предотвращение потери информации при работе компьютера в сети.

Предотвращение потери информации при работе компьютера в сети. Сетевая защита паролями дисков, папок, файлов. Защита компьютера от проникновения из внешней сети. Защита электронной почты. Защита от проникновения вирусов и троянских коней через сеть.

Тема 9. Программные установки и настройки систем защиты компьютера. Настройка безопасности системы. Особенности файлов текстовых процессоров. Уничтожение удалённого и исправленного текста.

Тема 10. Защита локального компьютера с помощью паролей и с использованием программ-архиваторов.

Использование паролей для входа в систему и безопасности файлов и папок. Программы-архиваторы. Защита архивов.

Тема 11. Настройка системы защиты браузеров и почтовых клиентов.
Опасность программ-апплетов и защита от них. Файлы «cookie» и чем они опасны. Безопасные узлы Интернет. Поиск и удаление с компьютера информации о Вашей работе в сети.

Раздел 3. Защита от компьютерных вирусов. Криптография и шифрование данных

Тема 12. Защита информации от компьютерных вирусов

Суть и содержание понятий «компьютерный вирус», «криптография», «стеганография», «шифр», «ключ», «шифрование», «зашифрование», «расшифрование», «дешифрование», «криптостойкость».

Тема 13. Криптография и шифрование данных
Общие представления о криптографии, шифровании и стеганографии для защиты электронной цифровой информации. Симметричные и асимметричные системы шифрования. Системы шифрования с открытым ключом. Электронная цифровая подпись. Электронные «водяные знаки».

Тема 14. Разновидности компьютерных вирусов и действия, выполняемые вирусами.

Классификация компьютерных вирусов с позиции программно-математических методов. Алгоритмы работы известных типов компьютерных вирусов, соответствующие алгоритмы их нейтрализации.

Тема 15. Антивирусные программы.
Признаки заражения вирусами. Анивирусные программы.

Тема 16. . Настройка и работа с антивирусной программой.
Методика использования антивирусных программ.

Тема 17. Ознакомление с программой шифрования PGP

Системы блочного шифрования. DES и ГОСТ 28147-89.

Тема 18. Итоговая контрольная работа.

5. ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Раздел 1. Проблема защиты информационных процессов в КС. Пространство угроз

Тема 1.4. Обслуживание компьютера стандартными диагностическими программами, входящими в состав утилит операционных систем.

Цель: Изучить алгоритмы работы со стандартными диагностическими программами.

Задание 1. Создание резервной копии данных. Восстановление информации с резервной копни

Задание 2. Работа со стандартными программам обслуживания дисков ОС Windows

Литература:

1. Защита информации в персональных ЭВМ. Спесивцев A.EL, Вегнер В..А.. Крутяков А.Ю и др. - М: Радио и связь, МП «Веста», 1993.
2. Малюк А. Д.. Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. - М.: Горячая линия-Телеком. 2001

Тема 1.5**.** Действия пользователей и безопасность данных.

Цель: сформировать представления о формах и методах обеспечения безопасности и защиты электронной информации.

Вопросы:

1. Почему на современном этапе развитая общества обострилась проблема защиты электронной информации?
2. Дайте классификацию угроз безопасности информации.
3. Каковы возможные методы защиты от известных угроз безопасности информации?
4. Что такое резервное копирование системы? Почему оно необходимо ?
5. Место программно-математических методов в комплексной системе защиты информации.
6. Кратко охарактеризуйте современные носители информации персонального компьютера.
7. Каков способ хранения информации на магнитных носителях?
8. Как рассчитать объём магнитного диска?
9. Какие структуры на магнитных носителях создаются программами FDISK и FORMAT?
10. Изложите алгоритм записи информации на магнитный даек.
11. Почему существует возможность восстановления удалённых файлов.
12. Чем различаются алгоритмы удаления информации в Корзину и MI MO Корзины в *ОС* Windows? Каковы алгоритмы восстановления данных в каждом из случаев?
13. Каковы возможные ошибки файловой системы FAT? Их суть, причины появления и способы исправления ситуации в каждом из случаев.
14. Что такое фрагментирование файлов? Его суть и причины возникновения. Программы для дефрагментации.
15. Дайте общий обзор программного обеспечения для профилактического обслуживания носителей информации и восстановления данных.
16. Каковы эффективные меры, повышающие шансы восстановления информации на магнитных носителях?
17. Основные приёмы работы и команды операционной системы MS-DOS.

18. Алгоритмы работы в программной оболочке Norton Commander.
19. Основные приёмы и алгоритмы работы в графической оболочке Windows.

Литература:

1. А. Миллер. DOS для пользователя ПК: Пер. с англ. - М.: Мир, 1993
2. А. А. Тюрникова, Н. А. Боровикова. Надёжная аутентификация - гарант безопасности информационной системы // Защита информации. Конфидент.- № 6.-2001 - с. 80-82.

Раздел 2. Защита локального и сетевого компьютеров

Тема: 2.5. Защита локального компьютера с помощью паролей и с использованием программ-архиваторов.

Цель: Научиться устанавливать комплексную защиту компьютера, препятствующую несанкционированной загрузке, получению доступа к электронной информации, попыткам изучения деятельности пользователя и доступа на компьютер извне по сети.

Вопросы:

1. Как защитить компьютер паролем включения?
2. Как защитить загрузку компьютера при помощи специальной дискеты (смарт-карты, электронного ключа)?
3. Приведите пример простой программы для защиты загрузки компьютера.
4. Как защитить загрузку компьютера паролем заставки экрана?
5. Что такое «скрытый файл»? Как скрывать файлы (папки) с использованием встроенных возможностей операционной системы Windows?
6. Как создать виртуальный логический диск с использованием системы Strong Disk?
7. Как скрывать программы, папки, файлы изменением имени и расширения?
8. Приведите способы удаления информации о файлах (документах), с которыми Вы работали.
9. Почему опасно использовать рабочие папки, предлагаемые ОС Windows и приложениями «по умолчанию»?
10. Каковы способы защиты файлов и документов в MS Office?
11. Как защитить файлы (папки) с помощью программ-архиваторов?

Задание 1. Защитить загрузку компьютера паролем заставки экрана
Задание 2. Защитить рабочие файлы установкой атрибутов
Задание 3. Защитить рабочие файлы изменением имени файла
Задание 4. Защитить документ MS Word от редактирования
Задание 5. Защитить документ MS Word паролем открытия
Задание 6. Защитить файл архивированием с паролем

Литература:

1. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных.: Учебное пособие для вузов./ Белкин П.Ю., Михальский О.О., Першаков А.С. и др. - М.: Радио и связь, 1999. - 168 с.

2. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах.: Учеб.пособие для вузов./ Проскурин В.Г., Крутов С.В., Мацкевич И.В. - М.: Радио и связь, 2000. - 168 с.

Тема 2.6. Настройка системы защиты браузеров и почтовых клиентов.

Цель: Научиться устанавливать комплексную защиту компьютера, препятствующую несанкционированной загрузке, получению доступа к электронной информации, попыткам изучения деятельности пользователя и доступа на компьютер извне по сети.

Вопросы:

1. Назначение и задачи программы-брандмауэра.
2. Возможен ли перехват электронной почты?
3. Каковы способы защиты электронной почты от перехвата, модификации, несанкционированного доступа?
4. Как отправить анонимное сообщение по электронной почте?
5. В чём состоит опасность вложении в почтовые сообщения? Каковы меры обеспечения безопасности?
6. Что такое «троянский конь»? Как не стать жертвой троянского коня?
7. Что такое файлы-апплеты и чем они опасны? Как настроить браузер на безопасную работу с апплетами?
8. Что такое файлы «cookie» и чем они опасны? Как настроить браузер на безопасную работу с cookie?
9. Что такое прокси-сервер? Алгоритм работы прокси-сервера.
10. Как удалить с компьютера информацию о Вашей работе в сети?

Литература:

1. Мельников В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электрониинформ, 1997.
2. Атака на Internet./ Медведовский И.Д., Семьянов П.В. и др. - М.: ДМК, 1999.
3. Безопасность глобальных сетевых технологий. - СПб.: Изд-во СПбГУ, 1999.
4. Защита информации в компьютерных системах и сетях./ Романец Ю.В., Тимофеев И.А., Шаньгин В.Ф. - М.: Радио и связь, 1999. - 328 с.

Раздел 3. Защита от компьютерных вирусов. Криптография и шифрование данных

Тема 3.6. Ознакомление с программой шифрования PGP

Цель: Используя современное программное обеспечение, научиться работать с антивирусной программой и защищать информацию при помощи стеганографических методов и путём создания шифрованных логических дисков.

Вопросы:

1. Дайте определение шифра и сформулируйте основные требования к нему
2. Зашифруйте шифром Цезаря слово «ЦЕЗАРЬ»
3. Расшифруйте слово «ЖВЖВ», зашифрованное шифром Цезаря
4. Что такое стеганография?
5. Поясните, что вы понимаете под совершенным шифром. Приведите пример совершенного шифра.

6. Перечислите основные режимы работы, предусмотренные в российском стандарте на шифрование данных.
7. Проведите сравнительный анализ параметров алгоритмов шифрования DES и Российского стандарта (в режиме простой замены).
8. Изложите принципиальную схему- организации секретной связи с использованием системы шифрования с открытым ключом.
9. Изложите принципиальную схему организации обмена документами, заверенными цифровой подписью.
10. Перечислите основные требования, предъявляемые к хеш-функции, пригодной для использования при вычислении цифровой подписи документа.

Задание 1. Презентация и доклад-обзор современных антивирусных программ.
Задание 2. Установить и настроить антивирусную программу.
Литература:

1. Козлов Д. А.. Парандовский А. Д.. Парандовский Д. К. Энциклопедия компьютерных вирусов. М.: Солон-Р, 2001.
2. С. Ф. Быков. О репликации компьютерных вирусов Защита информации. Конфидент. -ЛЬ 6.-2001.-с. 62-65.
3. К. Касперский. Техника сетевых атак: Том 1. -М.: Солон-Р, 2001.

Тема 3.7. Контрольная работа.

Цель: Проверить знания студентов по изученным разделам.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Литература

Основная:

1. Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2002.
2. Анисимова И.Н. Защита информации. Методические указания по выполнению лаб. работ для студентов всех специальностей. - 2001.
3. Анисимова И.Н. Защита информации. Метод. указания по изучению дисциплины и контрольные задания для студентов заочной формы обучения. Специальность 521400. - 2001.
4. Анин Б.Ю. Защита компьютерной информации. - СПб.: БХВ-Санкт-Петербург, 2000. - 384 с.
5. Теоретические основы компьютерной безопасности. : Учеб. пособие для вузов./ Девянин Н.Н., Михальский О.О. и др. - М.: Радио и связь, 2000. - 192 с.
6. Нечаев В.И. Элементы криптографии. Основы теории защиты информации.: Учеб.пособие для ун-тов и пед.вузов. - М.: Высшая школа, 1999. - 109 с.
7. Уваров О. Государственная и коммерческая тайна и инсайдерская информация.//Рынок ценных бумаг. - № 7(166). - М., 2000. - С.66-69.
8. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.:Издательство «ДиаСофт», 1999.

9. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2000. - 496 с.
10. Как построить защищенную информационную систему./ Под науч. ред. Зегжды Д.П. и Платонова В.В. - СПб.: Мир и семья, 1997.
11. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных.: Учебное пособие для вузов./ Белкин П.Ю., Михальский О.О., Першаков А.С. и др. - М.: Радио и связь, 1999. - 168 с.
12. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах.: Учеб.пособие для вузов./ Проскурин В.Г., Крутов С.В., Мацке-вич И.В. - М.: Радио и связь, 2000. - 168 с.
13. Мельников В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электрониинформ, 1997.
14. Атака на Internet./ Медведовский И.Д., Семьянов П.В. и др. - М.: ДМК, 1999.
15. Безопасность глобальных сетевых технологий. - СПб.: Изд-во СПбГУ, 1999.
16. Защита информации в компьютерных системах и сетях./ Романец Ю.В., Тимофеев И.А., Шаньгин В.Ф. - М.: Радио и связь, 1999. - 328 с.
17. Николаев Ю.И. Проектирование защищенных информационных технологий. - СПб.: Изд-во СПбГТУ, 1997.
18. Быков В.А. Электронный бизнес и безопасность. - М.: Радио и связь, 2000. - 200 с.
19. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2000. - 448 с.
20. Липаев В.В. Надежность программных средств. - М.: СИН-ТЕГ, 1998. - 232 с.
21. Богумильский Б. Энциклопедия Windows 98. - СПб.: Питер-Ком, 1999. - 816 с.
22. Терентьев А.М. Противовирусная защита ПК в Windows 95/98/NT. - М.: ЦЭМИ, 1999. - 81 с.

Дополнительная:

1. А. Миллер. DOS для пользователя ПК: Пер. с англ. - М.: Мир, 1993.
2. А. Галичев. Шифр - лучшее средство от бессоницы // Хакер.-№ 4.-2002.-с. 26-27.
3. А. Левин. Самоучитель работы на компьютере. М.: «Нолидж», 2003.
4. А. Каролик. Установи виртуальный сейф: программы для хранения паролей // Хакер.-№ 5.-2003.-с. 38-40.
5. А. Левин. Самоучитель работы в Windows. - М. «Нолидж», 2000.
6. А. Савельев. Прячем свой IP адрес // Хакер.-№ 9.-1999.- с. 24.
7. А. А. Тюрникова, Н. А. Боровикова. Надёжная аутентификация - гарант безопасности информационной системы // Защита информации. Конфидент.-№ 6.-2001 - с. 80-82.
8. Е. В. Касперский. Компьютерные вирусы: что это такое и как с ними бороться. - М. СК Пресс, 1998.
9. Козлов Д. А.. Парандовский А. Д.. Парандовский Д. К. Энциклопедия компьютерных вирусов. М.: Солон-Р, 2001.
10. К. Касперски. Техника сетевых атак: Том 1. -М.: Солон-Р, 2001.
11. Т. Оглтри. Firewalls. - М.: ДМК Пресс, 2001.
12. Оборонный комплекс PGP Хакер.-№ 3.-2001.-с. 62-64.
13. С. Ф. Быков. О репликации компьютерных вирусов Защита информации. Конфидент. № 11.-2001.-с. 62-65.

14. С. Мюллер. Модернизация и ремонт ПК. 2-е издание: Пер с англ. М..: Издательский дом «Вильямс», 2002.
15. CD под защитой Хакер.-№ 6.-2003.-е. 30-34.

6.2. Материально-техническое и информационное обеспечение дисциплины

В учебном процессе для освоения дисциплины применяют:
- компьютерное и мультимедийное оборудование;
- ссылки на Интернет ресурсы.

6.3. Методические указания студентам

(очная формы обучения)

Самостоятельная работа студентов, предусмотренная учебным планом, должна соответствовать более глубокому усвоению изучаемого курса, формировать навыки исследовательской работы, умения пользоваться научной и справочной литературой, ориентировать студентов на умение применять теоретические знания на практике. Самостоятельная работа должна носить систематический характер. Задания для самостоятельной работы составляются по разделам и темам, по которым не предусмотрены аудиторные занятия.

Разделы и темы для самостоятельного изучения	**Вид и содержание самостоятельной работы**
Раздел 1. Проблема защиты информационных процессов в КС. Пространство угроз Тема 1.2. Программные методы восстановления данных и активного профилактического обслуживания компьютера.	Подготовка сообщений по теме "Современные программные методы восстановления данных"
Раздел 2. Защита локального и сетевого компьютеров Тема 2.3. Программные установки и настройки систем защиты компьютера. Тема 2.5. Настройка системы защиты браузеров и почтовых клиентов.	Подготовка сообщений по темам: "Настройка системы защиты компьютера", "Защиты электронной почты", "Обзор современных браузеров и настройка защиты" Разработка памятки для пользователя электронной почтой.
Раздел 3. Защита от компьютерных вирусов. Криптография и шифрование данных Тема 3.4. Антивирусные программы Тема 3.5. Настройка и работа с антивирусной программой.	Подготовка сообщений по темам: "Современные антивирусные программы", "Настройка антивирусных программ", "Классификация вирусов", "Обзор стеганографических программ"

Результаты самостоятельной работы контролируются и учитываются при аттестации студента. При этом проводятся контрольные работы и семинары.

6.4. Материалы, устанавливающие содержание и порядок проведения промежуточных и итоговых аттестаций

Итоговой аттестацией изучения является контрольная работа.

Перечень вопросов к итоговой контрольной работе:

1. Проблема защиты электронной информации.
2. Место программно-математических методов в комплексной системе защиты информации.
3. Классификация угроз безопасности информации и возможные методы зашиты.
4. Резервное копирование данных: суть, устройства для хранения копии, рекомендации по резервному копированию.
5. Способ хранения информации на мандатных носителях.
6. Структура магнитного диска.
7. Алгоритм записи информации на магнитный диск и возможность восстановления удалённых файлов.
8. Операционная система Windows: алгоритмы удаления информации в Корзину и мимо Корзины.
9. Ошибки файловой системы FAT: супь, причины, способы исправления ситуации.
10. Фрагментирование файлов: суть, причины, программы для дефрагментации.
11. Общий обзор программного обеспечения для профилактического обслуживания носителей информации и восстановления данных.
12. Эффектные меры, повышающие шансы восстановления информации на магнитных носителях.
13. Защита локального компьютера паролем включения: суть, алгоритм настройки, способы преодоления защиты.
14. Загрузка локального компьютера с использованием оригинальной дискеты: суть, программный пример, способы преодоления защиты.
15. Защита локального компьютера паролем заставки экрана, суть, алгоритм настройки, способы преодоления защиты.
16. Защита информации скрытием файлов и папок, изменением имени и расширения, атрибутом «только для чтения»: алгоритмы настройки, способы преодоления защиты.
17. MS Office: алгоритмы защиты документов от несанкционированного доступа и использования. Правила задания пароля. Способы преодоления защиты.
18. Особенности строения файлов текстовых процессоров. Алгоритмы уничтожения удалённого и исправленного текста в теле файла текстового процессора.
19. Применение программ-архиваторов для скрытия и защиты файлов. Правила задания пароля. Способы преодоления защиты.
20. Генератор паролей, алгоритмы генерации. Оценка стойкости пароля.
21. Временные файлы, причинны появления временных файлов. Удаление временных файлов программными методами и вкруговую.
22. Программное обеспечение для полного уничтожения удалённых файлов. Алгоритмы работы программ.
23. Алгоритмы настройки защиты дисков, папок, файлов в локальной сети. ПО для защиты компьютера от проникновения из внешней среды. Суть работы программ....

24. Электронная почта: алгоритм отправки сообщении, возможность перехвата, способы защиты. Отправка анонимных сообщении.
25. Опасность программ-апплетов Java, JavaScript. ActiveX. Алгоритмы настроим защиты браузеров.
26. Опасность файлов «cookie». Методы контроле записи файлов «cookie» на жесткий диск.
27. Принцип работы прокси-сервера. Безопасные узлы. алгоритмы проверки безопасности.
28. Классификация компьютерных вирусов с позиции программно-математических методов, краткая характеристика каждого вида. Общие признаки заражения. Файловые вирусы: краткая характеристика перезаписывающего и паразитного вирусов
29. Файловые вирусы: характеристика компаньон-, link-вирусов и файловых червей.
30. Файловые вирусы: наиболее общий алгоритм работы, алгоритм обнаружения вирусов, возможность восстановления файлов.
31. Загрузочный вирус, алгоритм получения управления вирусом. Алгоритмы предотвращения заражения, обнаружения заражения, удаления вируса.
32. Макровирусы, принципы устройства и функционирования. Алгоритмы обнаружения вирусов и обезвреживания файлов.
33. Вирусы, передающиеся по сети (сетевые, HTML-вирусы, вирусы-апплеты, троянские кони) и способы защиты от них.
34. Резидентные вирусы: краткая характеристика алгоритмов работы.
35. Резидентные вирусы, обнаружение и обезвреживание, возможность восстановления файлов.
36. Последовательность действий при обнаружении заражения вирусом. Правила предотвращения заражения вирусом.
37. Общие представления о криптографии и шифровании Симметричные и асимметричные системы шифрования.
38. Системы шифрования с открытым ключом.
39. Электронная цифровая подпись
40. Общие представления о стеганографии и её использовании для защиты электронной цифровой информации.
41. Система шифрования RSA.
42. Системы блочного шифрования. DES и ГОСТ 28147-89.