ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Сборник планов проведения семинарских и практических занятий

для курсантов по специальности 030501 – Юриспруденция

ОРЕЛ
ОрЮИ МВД России
2010

УДК 004+34С33.2
ББК 32.97+67.99(2)116
О-75

О-75 **Основы информационной безопасности в органах внутренних дел**: Сборник планов проведения семинарских и практических занятий для курсантов по специальности 030501 – Юриспруденция /Составитель: Д.С.Мишин – Орел: Орловский юридический институт МВД России, 2010. – 36 с.

В сборнике даны организационные и методические рекомендации проведения семинарских и практических занятий по курсу «Основы информационной безопасности в органах внутренних дел». Настоящие материалы ориентированы на преподавателей и курсантов ОрЮИ МВД РФ для самостоятельного изучения и использования в учебном процессе.

УДК 004+34С33.2
ББК 32.97+67.99(2)116

Содержание

КРАТКИЕ ОРГАНИЗАЦИОННЫЕ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Главной целью развития информационной инфраструктуры общества является приведение ее в состояние, позволяющее обеспечить надежную защиту личности, общества и государства от преступных посягательств.

Для решения целевой установки, необходимо обеспечить выполнение задач информационной безопасности:

- разработать единые правовые, методические, программно-технические и технологические подходы при организации защиты информации в органах внутренних дел;

- гарантировать информационную безопасность интегрированных банков данных коллективного пользования оперативно-розыскной и справочной информации организованных на базе современных средств вычислительной техники;

- обеспечить закрытие служебной и конфиденциальной информации в локальных вычислительных сетях в службах и подразделениях органов внутренних дел, объединенных в региональные информационно-вычислительные сети;

- завершить формирование единой методологии информационной безопасности оперативно-розыскного, справочного, криминалистического и статистического назначения, поэтапно внедрять новые средства и методы защиты информации с информацией.

В настоящее время происходит интенсивное внедрение современных информационных технологий. В этой связи необходимо дальнейшее развитие методологического и методического обоснования борьбы с преступлениями в информационной сфере. Для этого требуется построение и применение адекватных математических моделей формирования и представления знаний по проблеме защиты информации, которые должны базироваться на системном анализе всего комплекса взаимодействующих факторов, определяющих каждую конкретную ситуацию. Решения, базирующиеся на моделях такого типа, позволяют рационально обосновывать широкий спектр мероприятий, направленных на обеспечение информационной безопасности.

Цели курса:

- развитие у курсантов понятийный аппарат, знаний основных положений теории защиты информации, методологии защиты в целом;

- приобретение обучаемыми знаний об организации защиты информации и использования средств и методов закрытия информации для повышения эффективности борьбы с преступностью;

- привитие курсантам практических навыков и умений применения программных и технических средств обеспечения информационной безопасности на высоком профессиональном уровне.

Задачи курса:

- усвоение курсантами основных положений теории, методологии и практики защиты информации;
- выработка навыков анализа моделей процесса защиты информации и оценки угроз информации;
- выработка умений и практических навыков применения программно-аппаратных средств защиты информации.

Курсанты должны знать:

- современное состояние развития средств и методов информационной безопасности и возможности их применения в практической деятельности органов внутренних дел;
- принципы построения и функционирования средств защиты информации;
- основы постановки и решения задач защиты информации;
- принципы построения и функционирования систем защиты информации;
- организационно-правовые основы защиты информации в органах внутренних дел.

Курсанты должны уметь:

- работать с программно-техническими средствами, обеспечивающими закрытие информации служебного и конфиденциального характера на ПЭВМ и в локальных сетях;
- эффективно использовать программно-технические средства защиты информации в локальных сетях;
- моделировать системы защиты информации при решении конкретных задач по обеспечению информационной безопасности.

Изучение курса «Основы информационной безопасности в органах внутренних дел» базируется на Конституции РФ, законах РФ, Указах Президента РФ, Постановлениях Совета Министров и Федерального собрания по вопросам борьбы с преступностью, а так же на ведомственных приказах и инструкциях, регулирующих вопросы правового обеспечения борьбы с преступностью и профилактики правонарушений.

В данный сборник включены некоторые рекомендации по подготовке к занятиям, работе с нормативными документами и литературой, приведены вопросы для самоконтроля.

Изучение программного материала обеспечивается проведением лекций, дающим научные знания по предмету, раскрывающих наиболее важные вопросы изучаемых тем; указывающих основные направления самостоятельного изучения материала и содержащих методические рекомендации для углубленной

самостоятельной работы слушателей, а также семинарских и практических занятий.

Семинарские занятия по курсу проводятся с целью углубления и закрепления знаний, полученных на лекциях, а также выработки устойчивых навыков самостоятельного активного получения дополнительных новых знаний по темам, предусмотренным программой и тематическим планом. Проведение семинарских занятий предусмотрено в двух основных формах:

- обсуждение вопросов, содержащихся в планах, решение ситуационных задач;
- обсуждение докладов и рефератов, подготовленных слушателями.

Успешное проведение семинарских занятий и достижение поставленных целей требует тщательной самостоятельной подготовки слушателей к каждому семинару, который включает в себя:

- ознакомление с планом семинарского занятия;
- повторение материала учебной лекции по данной тематике;
- изучение рекомендованных нормативных материалов и литературных источников;
- подготовка ответов на теоретические вопросы, написание докладов и рефератов.

Особое внимание при изучении учебной дисциплины уделяется **практическим занятиям**, предназначенным выработать у слушателей навыки использования программно-технических средств обеспечения информационной безопасности.

Практические занятия по курсу проводятся с целью закрепления теоретических знаний и приобретения умений и навыков по непосредственному решению задач по организации защиты информации в служебной деятельности. При проведении практических занятий группы делятся на подгруппы.

При подготовке к практическому занятию слушателям необходимо:

- рассмотреть теоретические вопросы темы;
- ознакомиться с содержанием основных практических занятий по теме;
-выработать примерные варианты их решения.

Контроль за качеством усвоения учебного материала и оценка знаний, умений и навыков слушателей проводится с целью определения степени достижения поставленных курсом целей обучения. **Итоговый контроль** по дисциплине проводится в форме **зачета**. Контроль за работой слушателей по изучению курса осуществляется путем опроса по пропущенным темам, проверке тетрадей с конспектами лекций и выполненных заданий практических занятий. Слушатели, получившие на семинарских, практических занятиях неудовлетворительную оценку, обязаны в установленные сроки отработать тему у преподавателя.

По всем возникающим вопросам по изучению курса, слушателям рекомендуется обращаться за консультацией к преподавателям кафедры.

ТЕМА N 1 «Проблемы обеспечения информационной безопасности органов внутренних дел»

Семинар: «Проблемы обеспечения информационной безопасности органов внутренних дел»

Цель:

- рассмотреть структуру организационно-правового обеспечения информационной безопасности;
- проанализировать современные тенденции организационно-правового обеспечения информационной безопасности;
- рассмотреть общие принципы организационно-правовых основ защиты информации;
- способствовать развитию научно-технического кругозора слушателей по вопросу использования нормативных документов в сфере информационной безопасности.

Время: 2 часа.
Место проведения: Учебная аудитория.
Уровни усвоения учебного материала:
Получить представление:

- о назначении организационно-правового обеспечения информационной безопасности;
- о современных тенденциях развития нормативной базы в сфере информационной безопасности

Усвоить:

- общее содержание организационно-правового обеспечения информационной безопасности.

Методические рекомендации.

При подготовке к семинару необходимо внимательно ознакомиться с его целями, уровнями усвоения учебного материала, вопросами, выносимыми на обсуждение.

При подготовке первого вопроса следует изучить структуризацию нормативно-правовой и организационной основы защиты информации. Особое внимание обратить на состав организационно-правового обеспечения и его составляющие.

По второму вопросу требуется уяснить тенденции развития нормативной базы в международной сфере информационной безопасности информации. Необходимо показать динамику развития информационной базы по данной проблематики.

При рассмотрении третьего вопроса особое внимание следует обратить на аспекты применения нормативной базы.

РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ.

1. Вступительная часть - 5 мин.
2. Основная часть - 80 мин.

Вопросы для обсуждения на семинаре:

1. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.
1.1. Состав организационно-правового обеспечения.
1.2. Основные Законы Российской Федерации по обеспечению информационной безопасности.
2. Основные составляющие национальных интересов в информационной сфере.
2.1. Виды и источники угроз информационной безопасности страны.
2.2. Принципы государственной политики обеспечения информационной безопасности Российской Федерации.
3. Актуальность обеспечения информационной безопасности органов внутренних дел.
3.1. Нормативные документы, регламентирующие организационные мероприятий по обеспечению информационной безопасности.
3.2. Обеспечение информационной безопасности как составляющая информационного противоборства организованной преступности.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить план ответов на теоретические вопросы, выносимые на семинар.

Вопросы для самоконтроля:

- назначение и структура организационно-правового обеспечения;
- общие тенденции развития нормативно-правовой базы информационной безопасности;
- правоприменительная практика защиты информации.

Темы рефератов :

1. Правовые аспекты регулирования отношений в сфере информационной безопасности.
2. Обзор Руководящих документов ФСТЭК по защите информации в АС и СВТ.
3. Перспективы использования средств идентификации и аутентификации в вычислительных сетях.
4. Зарубежный опыт организационного обеспечения защиты информации.

Заключительная часть .

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за ответы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.

2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).

3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).

4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».

5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному

доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

ТЕМА N 2 «Организационно-правовые основы зашиты информации в органах внутренних дел»

Семинар: «Назначение и общее содержание организационно-правового обеспечения информационной безопасности»

Цель:

- рассмотреть структуру организационно-правового обеспечения информационной безопасности;
- проанализировать современные тенденции организационно-правового обеспечения информационной безопасности;
- рассмотреть общие принципы организационно-правовых основ защиты информации;
- способствовать развитию научно-технического кругозора слушателей по вопросу использования нормативных документов в сфере информационной безопасности.

Время: 2 часа.
Место проведения: Учебная аудитория.
Уровни усвоения учебного материала:
Получить представление:

- о назначении организационно-правового обеспечения информационной безопасности;
- о современных тенденциях развития нормативной базы в сфере информационной безопасности

Усвоить:

- общее содержание организационно-правового обеспечения информационной безопасности.

Методические рекомендации.

При подготовке к семинару необходимо внимательно ознакомиться с его целями, уровнями усвоения учебного материала, вопросами, выносимыми на обсуждение.

При подготовке первого вопроса следует изучить структуризацию нормативно-правовой и организационной основы защиты информации. Особое внимание обратить на состав организационно-правового обеспечения и его составляющие.

По второму вопросу требуется уяснить тенденции развития нормативной базы в международной сфере информационной безопасности информации. Необходимо показать динамику развития информационной базы по данной проблематики.

При рассмотрении третьего вопроса особое внимание следует обратить на аспекты применения нормативной базы.

РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ.

1. Вступительная часть - 5 мин.
2. Основная часть - 80 мин.

Вопросы для обсуждения на семинаре:

1. Правовые основы деятельности органов внутренних дел в сфере выявления, пресечения и раскрытия преступлений.

1.1. Федеральные законы «Об информации, информационных технологиях и о защите информации», «Об оперативно-розыскной деятельности».

1.2. Нормативные документы МВД России, регламентирующие организационные мероприятий по обеспечению информационной безопасности

2. Основные угрозы информационной безопасности, возникающие в процессе деятельности органов внутренних дел.

2.1. Правовые основы реализации функций по добыванию, обработке и использованию оперативно-розыскной информации.

2.2. Сведения об оперативно-розыскной деятельности, подлежащие засекречиванию в системе органов внутренних дел.
2.3. Правовая защита сотрудников оперативных подразделений органов внутренних дел от негативных информационно-психологических воздействии.

Задания на самоподготовку:
1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить план ответов на теоретические вопросы, выносимые на семинар.

Вопросы для самоконтроля:
- назначение и структура организационно-правового обеспечения;
- общие тенденции развития нормативно-правовой базы информационной безопасности;
- правоприменительная практика защиты информации.

Темы рефератов :
1. Методы и средства защиты информации при работе с удаленными базами данных.
2. Возможные каналы утечки, искажения и порчи информации, циркулирующей в сети.
3. Защитные преобразования, шифрование и дешифрование для обеспечения достоверности и целостности информации передаваемой по каналам связи.
4. Обеспечение информационной безопасности в телекоммуникационных системах.

Заключительная часть .

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за ответы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России.

Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

ТЕМА N 3 «Защита информации от утечки на объектах информатизации органов внутренних дел»

Семинар: «Основы противодействия неправомерному доступу в сфере информационных технологий»**.**

Цель:

- рассмотреть принципы и методы защиты компьютерной информации;
- проанализировать современные тенденции требований защиты информации;
- рассмотреть общие принципы структуирования норм защищенности;
- способствовать развитию научно-технического кругозора слушателей по вопросу применения требований и норм защищенности в сфере информационной безопасности.

Время: 2 часа.
Место проведения: Учебная аудитория.
Уровни усвоения учебного материала:
Получить представление:

- о назначении требований к защите информации и нормам защищенности;
- о современных тенденциях развития методологии формирования требований защищенности СВТ.

Усвоить:

- общее содержание требований и норм защищенности.

Методические рекомендации.

При подготовке к семинару необходимо внимательно ознакомится с его целями, уровнями усвоения учебного материала, вопросами, выносимыми на обсуждение.

При подготовке первого вопроса следует изучить обоснование требований к защите информации. Обратить внимание на спецификацию функций безопасности и анализ слабых мест защиты.

По второму вопросу требуется уяснить тенденции развития требований и показателей защищенности автоматизированных систем обработки информации. Подчеркнуть значимость и роль с 7-го по 4-й классов защищенности.

РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ.

1. Вступительная часть - 5 мин.
2. Основная часть - 80 мин.

Вопросы для обсуждения на семинаре:

1. Понятие и виды каналов утечки информации.
1.1. Классификация каналов утечки информации.
1.2. Условия и факторы, способствующие утечке информации
1.3. Основные каналы утечки информации объектов информатизации ОВД
2. Основные угрозы безопасности информации.
2.1. Каналы утечки информации.
2.2. Характеристика средств несанкционированного получения информации.
2.3. Технологии применения средств несанкционированного получения информации.
3. Основные направления инженерно-технической защиты информации.
3.1. Способы блокирования каналов утечки информации.
3.2. Основные этапы проведения специальных проверок объектов информатизации.
5. **Заключительная часть** - 5 мин.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить план ответов на теоретические вопросы, выносимые на семинар.

Вопросы для самоконтроля:

- Средства обнаружения и лечения компьютера от вирусов;
- Типовые методы и средства защиты от перехвата компьютерной информации через ПЭМИН;
- Принцип действия, технические характеристики устройств защиты и правила эксплуатации;

Темы рефератов:

1. Модель угроз и принципы обеспечения безопасности программного обеспечения.
2. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок.
3. Методы идентификации программ и их характеристик.

4. Обеспечение эксплуатационной безопасности программного обеспечения.
5. Способы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок.

Заключительная часть .

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за ответы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».
8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».
9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».
10. Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).
11. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).
12. Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.
3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для

высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

ТЕМА N 4 «Защита информационных процессов и информации в компьютерных системах»

Практическое занятие: «Программные средства защиты компьютерной информации от НСД»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;

- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Восстановление зараженных файлов
2. Профилактика проникновения «троянских программ»
3. Настройка безопасности почтового клиента Outlook Express
4. Настройка параметров аутентификации Windows 2000 (XP)
5. Шифрующая файловая система EFS и управление сертификатами в Windows 2000 (XP)

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.

2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).

3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).

4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».

5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Практическое занятие: «Каналы утечки, искажения и порчи компьютерной информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Назначение прав пользователей произвольном управлении доступом в Windows 2000 (XP)
2. Настройка параметров регистрации и аудита в Windows 2000 [XP]
3. Управление шаблонами безопасности в Windows 2000 (XP)
4. Настройка и использование межсетевого экрана в Windows 2000 (XP)
5. Создание VPN-подключения средствами Windows 2000 (XP)

Задания на самоподготовку:
1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:
Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун,

СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Практическое занятие: «Каналы утечки, искажения и порчи компьютерной информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Работа с программами: Acronis Privacy Expert Suite, Steganos Crypt; Kerio WinRoute Firewall.
2. Работа с программами защиты информации от несанкционированного доступа Tiny Firewall Pro; McAfee Personal; CrypKey SDK.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.

6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».
8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».
9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».
10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).
11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).
12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-

2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

5. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

6. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

2. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

3. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Практическое занятие: «Каналы утечки, искажения и порчи компьютерной информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;

- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Работа с программами: S-tools, Burmies Password; Password Organizer; Paragon Encrypted.
2. Работа с программами защиты информации от несанкционированного доступа F-Secure Antivirus for Firewall; Mercury Interactive SiteScore.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.

2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).

3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).

4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».

5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко,

Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

ТЕМА N 5 «Защита информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД)»

Практическое занятие: «Порядок проведения работ по обеспечению информационной безопасности вычислительных сетей»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Работа с программами: Acronis Privacy Expert Suite, Paragon Encrypted; Password Organizer; Burmies Password.

2. Работа с программами защиты информации от несанкционированного доступа Mercury Interactive SiteScore; F-Secure Antivirus for Firewall.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».

5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

4. И.И.Журавленка, В.Е.Кадулин, К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России.

Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Практическое занятие: «Каналы утечки, искажения и порчи информации, циркулирующей в сети»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Работа с программами использующими стеганографические методы в процессе передачи информации (S-tools).
2. Аутентификация электронных документов с использованием электронной цифровой подписи.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 165 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Ознакомиться с учебно-методическими материалами.
2. Ознакомиться с характеристикой и изучить порядок шифрования и дешифрования файлов.
3. Ознакомиться с характеристиками программ и изучить порядок работы с ними на конкретных примерах.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».
8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».
9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».
10. Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).
11. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).
12. Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «По-

ложение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.
3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

5. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

6. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

2. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

3. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Практическое занятие: «Методы и средства дистанционного съема информации посредством каналов связи»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 2 часа.
2. **Цель занятия**:

- ознакомить слушателей с основными понятиями и принципами организации защиты информации в вычислительных сетях;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования современных средств обеспечения информационной безопасности.

3. **Учебные вопросы**:

1. Изучение технических характеристик и параметров устройств обеспечивающих блокирования каналов утечки информации через ПЭМИН.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. **Рекомендуемый план распределения времени**:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 75 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 10 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет «Вычислительной техники».
7. **Исходные материалы**: УММ, рекомендуемая литература,
конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II.ПРАКТИЧЕСКАЯ РАБОТА.

1. Изучение технических характеристик программно-аппаратных средств обеспечения информационной безопасности в каналах связи.
2. Назначение и тактико-технические характеристики средств защиты информации.
3. Безопасность компьютерной сети.

III. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Рассмотреть рекомендуемые учебно-методические материалы;
2. Ознакомиться с основными характеристиками программно-аппаратных средств, обеспечивающих информационную безопасность в каналах связи.

IV. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

ЛИТЕРАТУРА ПО ТЕМЕ

Основная:

Нормативно-правовые акты:

1. Конституция Российской Федерации. - 1993 г.

2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).

3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).

4. Закон РФ or 5 мая 1992 года№ 2446-1 «О безопасности».

5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Закон РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».

8. Закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9. Федеральный закон РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

10.Перечень сведений, отнесенных к государственной тайне (Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

11.Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

12.Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Нормативные источники:

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

2. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Основная литература:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.С.Хохлов. - М.: Маросейка, 2008.-368с.

2. Белоглазов Е.Г. и др. Основы информационной безопасности органов

внутренних дел: Учебное пособие. - М.: МосУ МВД России. 2008.

3. И.И.Журавленка, В.Е.Кадулин,К.К.Борзунов. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2007.

4. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов ОВД / А.Н. Ильяшенко, Д.С. Мишин – Краснодар: КрУ МВД России, 2009 г.

5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2007.

6. Э. Бот, К. Зихерт. Безопасность Windows. - СПб.: Питер, 2007.

7. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007.

Дополнительная литература:

1. Информатика: учебник для высших учебных заведений МВД России. Том I. Информатика: Концептуальные основы / В.А.Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов - М.: Маросейка, 2008.-464с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / В.А. Минаев, А.П.Фисун, СВ.Скрыль, СВ.Дворянкин, М.М.Никитин, Н.СХохлов. - М: Маросейка, 2008. - 544с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006.

4. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2008.

Сборник планов проведения семинарских и практических занятий
для курсантов по специальности 030501 – Юриспруденция

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Составитель:
Мишин Дмитрий Станиславович, к.ю.н.

Свидетельство о государственной аккредитации
Рег. № 0051 от 02.11.09 г.
Подписано в печать _____ г. Формат 60x90$^{1}/_{16}$.
Усл.печ.л. - _____. Тираж _____. Заказ № _____.

Орловский юридический институт МВД РФ.
302027, Орел, Игнатова, 2.