Автономная некоммерческая организация
«ИНСТИТУТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ и УПРАВЛЕНИЯ РИСКАМИ»

УТВЕРЖДАЮ:

РЕКТОР АНО «ИНБУР»

_____Г.Г.Блохин

« ___ » _____2012 год

ПРОГРАММА

Повышения квалификации

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Барнаул 2011

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.

Программа курсов повышения квалификации «Обеспечение информационной безопасности и защита персональных данных» адресована специалистам государственных учреждений и организаций, сотрудникам правоохранительных органов, специалистам финансовых организаций, а также работникам предприятий и организаций различных форм собственности, профессиональные интересы которых связаны с использованием современной вычислительной техники, применением информационных сетей, привлечением телекоммуникационных технологий, электроники, вычислительной техники.

Актуальность программы. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также систему регулирования возникающих при этом отношений. Развитие информационной сферы, обеспечение ее безопасности становится одним из приоритетов национальной политики нашего государства. В «Доктрине информационной безопасности Российской Федерации» в качестве одной из основных задач указывается необходимость защиты интересов личности, общества, государства в информационной сфере. Особую актуальность этой проблеме придает реализация закона №152-ФЗ «О персональных данных», существенно повышающая требования к государственным организациям, которые хранят, собирают, передают или обрабатывают персональные данные с применением информационных технологий.

Цель программы – рассмотреть основные представления, касающиеся защиты информации и персональных данных в условиях широкого использования компьютерной техники и информационных сетей, получить представление о современных программно-аппаратных и технических методах защиты информации, практически ознакомиться со средствами, устройствами и приборами такой защиты. Реализация данной цели позволит слушателям изучить защиту информации в автоматизированных системах, овладеть методиками ее организации.

Задачи программы:

- формирование у слушателей представлений о современном состоянии защиты информации в автоматизированных системах;
- ознакомление с возможностями по обеспечению информационной безопасности, предоставляемыми современными средствами и методами;
- формирование целостных представлений о проблемах и перспективах комплексного обеспечения защиты информации;
- ознакомление с радиоэлектронными устройствами и прибора, используемыми для защиты информации;
- формирование практических навыков по работе с программно-аппаратным обеспечением защиты информации в информационных сетях;
- формирование умений применять современные методы защиты информации.

В целом программа имеет **практико-ориентированный характер**. В числе организационных форм обучения преобладают практические и лабораторные занятия, на которых слушатели приобретают практические навыки защиты информации.

Основные направления работы по программе. Программа предусматривает лекционные занятия и выполнение индивидуальных работ лабораторного практикума в специализированных лабораториях защиты информации. Слушатели обеспечиваются комплектом методических материалов. Учебным планом программы предусматривается самостоятельная работа слушателей, в ходе которой будут задействованы вычислительная техника и программное обеспечение лабораторий. Индивидуальная траектория обучения подбирается таким образом, чтобы участники программы смогли использовать имеющийся у них профессиональный опыт. На заключительном этапе курсов проводится круглый стол, на котором слушатели смогут обменяться мнениями по актуальным для них конкретным вопросам защиты информации в компьютерных системах.

Ресурсное обеспечение программы.

Программа будет реализовываться на базе НОУ АОЦСТ и Объединения обучающих организаций. В реализации программы задействованы специалисты АНО «ИНСТИТУТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ и УПРАВЛЕНИЯ РИСКАМИ».

Все лаборатории полностью оснащены необходимой компьютерной техникой и лицензионным программным обеспечением, образуют защищенную локальную вычислительную сеть и имеют выход в сеть Интернет. Для выхода в глобальную сеть Интернет и сеть RUNNet используются оптоволоконный (8Мбит/с) канал. Имеется специализированный компьютерный класс (11 компьютеров с выходом в сеть Интернет) и аудитория с мультимедийным обеспечением для проведения лекционных занятий.

2. ХАРАКТЕРИСТИКА ПОДГОТОВКИ ПО ПРОГРАММЕ

Программа соответствует Приоритетным направлениям развития науки, технологий и техники в Российской Федерации (утвержденным Президентом РФ 21.05.2006 г., Пр-843) «Информационно - телекоммуникационные системы» и «Безопасность и противодействие терроризму».

Учебная программа составлена в соответствии со следующими документами:

- «Требования к содержанию дополнительных профессиональных образовательных программ», утвержденные приказом Минобразования РФ от 18 июня 1997 г. № 1221;
- «Методические рекомендации по разработке образовательных программ дополнительного профессионального образования по направлению подготовки «Информационная безопасность», утвержденные заместителем директора ФСТЭК РФ 01 августа 2009 г.

Нормативный срок освоения программы – 72 часа.

Режим обучения – 36 часов в неделю.

По окончанию курсов слушателям выдается **Удостоверение о краткосрочном повышении квалификации** установленного образца.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ

Слушатель, освоивший программу, должен:

3.1. Обладать профессиональными компетенциями, включающими в себя следующие способности:

- Способность понимать социальную значимость защиты информации;
- Способность логически верно, аргументировано и ясно представлять результаты в области защиты информации, вести дискуссии;
- Способность к свободному чтению текстов и литературы по тематике программы;
- Способность использовать нормативные правовые документы в области информационной безопасности в своей деятельности;
- Способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- Способность определять виды и формы информации, подверженной угрозам на основе анализа структуры и содержания информационных процессов в конкретной автоматизированной системе;
- Способность определять комплекс мер по защите информации с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.
- Способность применять программные средства защиты информации системного, прикладного и специального назначения;
- Способность использовать инженерно-технические средства и методы защиты информации;
- Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- Способность изучать и обобщать опыт работы других учреждений и организаций и предприятий в области повышения эффективности защиты информации.

3.2. *владеть*:

- навыками критического восприятия информации;
- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
- навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов);
- навыками выявления и уничтожения компьютерных вирусов;
- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности автоматизированным системам;

- методами организации и управления деятельностью служб защиты информации;
- методиками проверки защищенности объектов информатизации;
- профессиональной терминологией;
- навыками безопасного использования технических средств в профессиональной деятельности.

3.3. *уметь*:

- использовать программные и аппаратные средства персонального компьютера;
- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

3.4. *знать*:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- принципы и методы организационной защиты информации;
- технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам;
- принципы и методы противодействия несанкционированному информационному воздействию на автоматизированные системы и системы передачи информации.

4. СОДЕРЖАНИЕ ПРОГРАММЫ

4.1. Учебный план программы

№ п/п	Наименование разделов и тем	Всего, час.	Лекции, час.	Практические занятия, лабораторные работы, час.
1.	Современное состояние защиты информации и персональных данных	**18**	**6**	**12**
1.1	Раздел 1. Проблемы обеспечения информационной безопасности	2	2	
1.1.1.	Тема 1. Основы информационной безопасности человека и общества	1	1	
1.1.2.	Тема 2. Виды угроз информационной безопасности Российской Федерации	1	1	
1.2.	Раздел 2. Теоретические основы защиты компьютерной информации	6	2	4
1.2.1.	Тема 1. Основные понятия теории компьютерной безопасности	1	1	
1.2.2.	Тема 2. Основные уровни защиты информации	1	1	
1.2.3.	Тема 3. Основные виды атак на автоматизированные системы обработки информации	4		4
12.2.4.	Тема 4. Понятие политики безопасности	2	2	
1.3.	Раздел 3. Обеспечение безопасности информационных сетей	6	2	4
12.3.1.	Тема 1. Типовые угрозы сетевой безопасности	2	2	
1.3.2.	Тема 2. Безопасность сети Интернет	8		8
2.	Современные методы и средства защиты информации и персональных данных в автоматизированных системах	**36**	**12**	**24**

2.1.	Раздел 1. Приборы и устройства защиты информации	14	4	10
2.1.1.	Тема 1. Структура, классификация и основные характеристики технических каналов утечки информации	2	2	
2.1.2.	Тема 2. Побочные электромагнитные излучения и наводки	2	2	
2.1.3.	Тема 3. Утечка информации по акустическим каналам	4		4
2.1.4.	Тема 4. Защита от утечки информации по радиоканалу	4		4
2.1.5.	Тема 5. Оптические системы защиты информации	2		2
2.2.	Раздел 2. Программно-аппаратные средства защиты информации	14	6	8
2.2.1	Тема 1. Идентификация и аутентификация пользователей	1	1	
2.2.2.	Тема 2. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничение доступа	2	2	
2.2.3.	Тема 3. Понятие аппаратных и программно-аппаратных средства криптозащиты данных	1	1	
2.2.4.	Тема 4. Защита компонентов ПЭВМ	4		4
2.2.5.	Тема 5. Средства защиты в компьютерной сети. Межсетевые экраны	4		4
2.3.	Раздел 3. Биометрические системы защиты информации	8	2	6
2.3.1.	Тема 1. Понятие биометрии. Биометрическая идентификация и верификация	1	1	
2.3.2.	Тема 2. Биометрические технологии	3	1	2
2.3.3.	Тема 3. Использование при защите информации полиграфа	4		4
3.	Предотвращение преступлений и правонарушений в сфере защиты информации	**18**	**14**	**4**

3.1.	Раздел 1. Особенности преступлений в сфере компьютерной информации	2	2	
3.1.1.	Тема 1. Признаки и элементы компьютерных преступлений	2	2	
3.1.2.	Тема 2. Особенности расследования компьютерных преступлений	8	8	
3.2.	Раздел 2. Правовое обеспечение информационной безопасности	6	4	2
3.2.1.	Тема 1. Правовой режим защиты конфиденциальной информации	4	2	2
3.2.2.	Тема 2. Судебное преследование за преступления в сфере компьютерной информации	2	2	
Итого		**72**	**32**	**40**

4.2. Тематический план программы

№ п/п	Наименование разделов и тем	Содержание обучения по темам
1.	**Современное состояние защиты информации и персональных данных**	
1.1	Раздел 1. Проблемы обеспечения информационной безопасности	
1.1.1	Тема 1. Основы информационной безопасности человека и общества	Основные принципы, обеспечивающие высокую информационную безопасность человека и общества в современных условиях. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере.
1.1.2	Тема 2. Виды угроз информационной безопасности Российской Федерации	Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации. Угрозы безопасности информационных и телекоммуникационных средств и систем. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Проблемы региональной информационной безопасности. Направления обеспечения информационной безопасности государства.

1.2	Раздел 2. Теоретические основы защиты компьютерной информации	
1.2.1	Тема 1. Основные понятия теории компьютерной безопасности	Язык, объекты, субъекты, доступ. Ценность информации. Решетка ценности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности.
1.2.2	Тема 2. Основные уровни защиты информации	Уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации.
1.2.3	Тема 3. Основные виды атак на автоматизированные системы обработки информации	Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак. Классификация вредоносного программного обеспечения.
1.2.4	Тема 4. Понятие политики безопасности	Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа. Политика изолированной программной среды. Разработка и реализация политики безопасности.
1.3	Раздел 3. Обеспечение безопасности информационных сетей	
1.3.1	Тема 1. Типовые угрозы сетевой безопасности	Основы классификации сетевых угроз и атак. Примеры типовых атак. Рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность. Маршрутизаторы. Межсетевые экраны. Основные схемы применения межсетевых экранов.
1.3.2	Тема 2. Безопасность сети Интернет	Стандарты и протоколы Интернет. Виды используемых в Интернет каналов связи. Особенности их защиты. Защита персональных данных. Защита от вирусов.

	Лабораторные работы	1. Атаки на автоматизированные системы обработки информации 2. Безопасность глобальной сети Интернет
	Самостоятельная работа	1. Антивирусная защита информации при наличии. 2. Контроль и сопровождение компьютерной безопасности в офисе. 3. Использование защищенных сетевых протоколов для передачи конфиденциальной информации. 4. Особенности обмена электронными почтовыми сообщениями, содержащими конфиденциальную информацию. 5. Особенности стандартов и протоколов сети Интернет. 6. Современные межсетевые экраны.
2.	**Современные методы и средства защиты информации и персональных данных в автоматизированных системах**	
2.1	Раздел 1. Приборы и устройства защиты информации	
2.1.1	Тема 1. Структура, классификация и основные характеристики технических каналов утечки информации	Понятие инженерно-технической защиты информации как области информационной безопасности. Проблемы инженерно-технической защиты информации. Представление средств и методов защиты информации в виде системы. Понятие об опасном сигнале. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.
2.1.2	Тема 2. Побочные электромагнитны	Понятие побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Сосредоточенные и распределенные источники

	е излучения и наводки	побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Паразитная генерация радиоэлектронных сигналов. Явления, вызывающие утеку информации по цепям электропитания, заземления и токопроводящим конструкциям.
2.1.3	Тема 3. Утечка информации по акустическим каналам	Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Защита речевой информации от утечки.
2.1.4	Тема 4. Защита от утечки информации по радиоканалу	Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Утечка информации по телефонным каналам связи. Подавление опасных сигналов помехами.
2.1.5	Тема 5. Оптические системы защиты информации	Распространение оптических сигналов в атмосфере и светопроводах. Основные показатели, влияющие на дальность каналов утечки и качество информации на выходе. Средства видеоконтроля и видеоохраны.
2.2	Раздел 2. Программно-аппаратные средства защиты информации	
2.2.1	Тема 1. Идентификация и аутентификация пользователей	Понятие идентификации пользователя. Задача идентификации пользователя. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие несанкционированного доступа. Понятие аутентификации.
2.2.2	Тема 2. Основные подходы к защите данных от несанкционированного доступа. Шифрование, контроль доступа, разграничение доступа	Шифрование. Контроль доступа. Разграничение доступа. Организация доступа к файлам. Журналы доступа. Выявление следов несанкционированного доступа к файлам. Понятие доступа к данным со стороны процесса и со стороны пользователя. Надежность систем ограничения доступа.

2.2.3	Тема 3. Понятие аппаратных и программно-аппаратных средства защиты информации	Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных. Необходимые и достаточные функции аппаратного средства криптозащит. Преимущества и недостатки программных и аппаратных средств.
2.2.4	Тема 4. Защита компонентов ПЭВМ	Классификация защищаемых компонент ПЭВМ. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Проблема защиты отчуждаемых компонентов ПЭВМ. Способы защиты информации на съемных дисках. Надежность средств защиты компонент.
2.2.5	Тема 5. Средства защиты в компьютерной сети. Межсетевые экраны	Протоколы аутентификации в локальной сети. Механизмы аутентификации при осуществлении подключений. Аутентификация в защищенных соединениях. Типы межсетевых экранов. Виртуальные частные сети (Virtual Private Network). Примеры реализации виртуальных частных сетей.
2.3	Раздел 3. Биометрические системы защиты информации	
2.3.1	Тема 1. Понятие биометрии. Биометрическая идентификация и верификация	Понятие биометрии. Биометрическая идентификация. Биометрическая верификация. Принципы работы биометрических систем. Области применения биометрии. Биометрические технологии. Идентификация по лицу. Идентификация по голосу. Идентификация по радужной оболочке глаза. Геометрическое строение руки и пальцев. Идентификация по подписи.
2.3.2	Тема 2. Биометрические технологии	Понятие биометрических технологий. Идентификация по лицу. Идентификация по голосу. Идентификация по радужной оболочке глаза. Идентификация по геометрическому строению руки и пальцев. Идентификация по подписи.
2.3.3	Тема 3. Использование при защите информации полиграфа	Психофизиологические принципы использования полиграфа. Правовые аспекты применения полиграфов при защите информации.
	Лабораторные работы	1. Оценка защищенности речевой информации на базе аппаратно-программного комплекса VNK-012GL.

		2. Многоканальный комплекс радиоконтроля «Квадрат». 3. Оптические системы защиты информации. Системы видеонаблюдения. 4. Использование программно-аппаратных комплексов защиты информации от несанкционированного доступа «SECRET NET 2000», «АККОРД-NT/2000», «Соболь». 5. Средства защиты в компьютерной сети. Использование системы «ViPNet Personal Firewall». 6. Использование при защите информации компьютерного полиграфа «ЭПОС-2.
	Самостоятельная работа	1. Анализ акустической речевой информации. 2. Электронная цифровая подпись. 3. Компьютерная обработка изображений отпечатков пальцев. 4. Идентификация личности по голосовым сигналам. 5. Контроль защищенности от утечки речевой информации по акустическому каналу. 6. Особенности каналов утечки информации в проводных линиях. 7. Использование современных комплексов видеонаблюдения.
3.	**Предотвращение преступлений и правонарушений в сфере защиты информации**	
3.1	Раздел 1. Особенности преступлений в сфере компьютерной информации	
3.1.1	Тема 1. Признаки и элементы компьютерных преступлений	Понятие преступлений в сфере компьютерной информации. Признаки и элементы состава преступления. Характеристика компьютерных преступлений. Условия, способствующие и препятствующие компьютерным преступлениям.
3.1.2	Тема 2. Особенности расследования компьютерных преступлений	Расследование компьютерного преступления. Особенности основных следственных действий. Особенности сбора доказательств. Экспертиза преступлений в области компьютерной информации.

3.2	Раздел 2. Правовое обеспечение информационной безопасности	
3.2.1	Тема 1. Правовой режим защиты конфиденциальной информации	Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы конфиденциальной информации. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
3.2.2	Тема 2. Судебное преследование за преступления в сфере компьютерной информации	Проблемы судебного преследования за преступления в сфере компьютерной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации: уголовная, административная, гражданско-правовая, дисциплинарная.
	Практические занятия (семинары)	1. Особенности преступлений в сфере компьютерной информации. 2. Правовой режим защиты конфиденциальной информации.
	Самостоятельная работа	1. Анализ статей УК РФ, относящихся к преступлениям в информационной сфере. 2. Проблемы в расследовании компьютерных преступлений. 3. Факторы, способствующие совершению компьютерных преступлений. 4. Профилактика преступлений в информационной сфере. 5. Международное сотрудничество при обеспечении информационной безопасности.

5. ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММ

В качестве форм и методов контроля и оценки результатов освоения программы слушателями будут использоваться:
- критериально-ориентированный тестовый контроль усвоения знаний;
- анкетирование;
- проблемные дискуссии;
- анализ решения слушателями учебно-профессиональных задач и ситуаций;
- анализ выполнения лабораторных работ;
- контрольные задания.

По завершению обучения предусмотрена сдача зачета.

6. СПИСОК ЛИТЕРАТУРЫ

6.1. Основная литература

1. Конституция Российской Федерации / ст.ст. 23, 24, 29/2
2. Уголовный кодекс Российской Федерации / ст.ст. 137, 138, 155, 183, 272, 273, 274, 275, 276, 283, 284, 310, 311/
3. Трудовой кодекс Российской Федерации /Глава 14, ст.ст.85-90/
4. Кодекс Российской Федерации об административных правонарушениях /ст.13.11; 13.12/
5. Закон Российской Федерации «О безопасности» от 5 марта 1992г.
6. Закон Российской Федерации «О государственной тайне» от 21 июля 1993г.
7. Федеральный закон Российской Федерации «О системе государственной службы Российской Федерации» от 27.05.2003. № 58-ФЗ (с дополнениями и изменениями) /ст. 14/8.
8. Федеральный закон Российской Федерации «О государственной гражданской службе в Российской Федерации» от 27.07.2004. № 79-ФЗ (в ред. От 28.12.2010) /глава 7/9.
9. Федеральный закон «О муниципальной службе в Российской Федерации» от 02.03.2007. № 25-ФЗ (в ред. От 17.07.2009) /ст. 29/ 10.
10. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006г.11.
11. Федеральный закон Российской Федерации «Об оперативно-розыскной деятельности» от 12 августа 1995г.12.
12. Федеральный закон Российской Федерации «О связи» от 7 июля 2003г.13.
13. Федеральный закон Российской Федерации «О коммерческой тайне» от 29 июля 2004 14. Федеральный закон Российской Федерации «О персональных данных» от 27 июля 2006г.
14. Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02. 2009. № 8-ФЗ16.

15. Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела. Утверждено Указом Президента Российской Федерации от 30 мая 2005г. № 60917.
16. Положение о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах. Утверждено Постановлением Правительства Российской Федерации от 22 октября 2007г.18.
17. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено Постановлением Правительства Российской Федерации от 17 ноября 2007г.19.
18. Порядок проведения классификации информационных систем пе5рсональных данных. Утвержден приказом ФСТЭК, ФСБ, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008г. № 55/86/2020.
19. Положение о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 05.02 2010 № 58 .21.
20. Положение о ведении реестра операторов, осуществляющих обработку персональных данных. Утверждено приказом Федеральной службы по надзору в сфере массовых коммуникаций связи и охраны культурного наследия от 28.03. 2008 № 154.22.
21. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации от 09.09.2000. № Пр-1895
22. Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом Российской от 07.02. 2008.

6.2. Дополнительная литература

1. Виноградова С.М., Войтович Н.А., Вус М.А. Информационная безопасность: Учеб. пособие. - СПб.: Изд-во СПбГУ, 1999.
2. .Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. – М.: Логос, 2001.
4. Запечников С.В., Милославская Н.Г. , Толстой А.И. Основы построения виртуальных частных сетей. – М.: Горячая линия–Телеком, 2003. – 249 с.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных

систем. – М.: Горячая линия. – Телеком, 2000. – 452 с.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие / – М.: Горячая линия-Телеком, 2004.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999.
8. Ярочкин В.И. Информационная безопасность. Учеб. пособие. – М.: Академический проект; Гаудеамус, 2004.
9. Аутетификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие / Под ред. А.А. Шелупанова, С.Л. Груздева. – М.: Горячая линия. – Телеком, 2009. – 552 с.
10. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия. – Телеком, 2005. – 416 с.
11. Грибунин В.К., Чудовский В.В. Комплексная система защиты информации на предприятии: Учебное пособие. – М.: Издательский центр «Академия», 2009. – 416 с.
12. Зайцев А.П., Шелупанов А.А. Практикум по техническим средствам и методам защиты информации: Учебное пособие. – Томск: Изд-во ТУСУР, 2005. – 129 с.
13. Защита информации в системах мобильной связи: Учебное пособие / под ред. А.А. Заряева и С.В. Скрыля. – М.: Горячая линия. – Телеком, 2005. – 171 с.
14. Касперский К. Техника сетевых атак. Приемы противодействия. – М.: СОЛОН-Р, 2001.
15. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие. – М.: Горячая линия. – Телеком, 2007. – 180 с.
16. Технические средства обеспечения информационной безопасности: Учебное пособие / Сост. А.П. Зайцев. – Томск: Томский центр дистанционного образования, 2004. – 199 с.
17. Айков, Д. Компьютерные преступления. / Д. Айков, К. Сейгер, У. Фонсторх. – М.: Мир, 1999. – 351 с.
18. Волеводз А.Г. Противодействие компьютернымпреступлениям: правовые основы. – М.: ООО «Издательство «Юрлитинформ», 2002.
19. Мазуров В.А. Компьютерные преступления. Учебное пособие. – Барнаул: Изд-во АлтГУ, 2002.
20. Мазуров В.А., Головин А.В., Поляков В.В. Информационная безопасность: основы правовой и технической защиты информации. – Барнаул: Изд-во Алт. ун-та, 2006. – 196с.