МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Национальный исследовательский университет
«Московский физико-технический институт (государственный университет)»
(МФТИ)

СОГЛАСОВАНО
Председатель УМО по образованию в области информационной безопасности
доктор технических наук, профессор,
член-корреспондент Академии криптографии

_____ А.П.Коваленко

«__» _____ 20__ г.

УТВЕРЖДАЮ
Ректор МФТИ
доктор физико-математических наук,
профессор,
член-корреспондент РАН

_____ Н.Н. Кудрявцев

« ___ » _____ 20 ____ г.

Дополнительная образовательная программа повышения квалификации «Технологии и средства защиты компьютерных систем»

ОТ РАЗРАБОТЧИКА
Генеральный директор
ООО «Центр исследования безопасности информационных технологий»

_____ О.В.Иванов

« 11 » марта 20 13 г.

Москва 2013

Дополнительная профессиональная образовательная программа «Технологии и средства защиты компьютерных систем» повышения квалификации разработана с учетом основной профессиональной образовательной программы «Компьютерная безопасность» (090102) по направлению «Информационная безопасность» (090000).

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Категории слушателей, на обучение которых рассчитана программа повышения квалификации (далее – программа):

Системные администраторы
Специалисты по информационным технологиям
Специалисты по информационной безопасности
Специалисты технической поддержки
Офицеры информационной безопасности
Руководители ИТ- и ИБ-подразделений

1.2 Сфера применения слушателями полученных профессиональных компетенций, умений и знаний:

использование современных технологий и средств защиты компьютерных систем.

2 ХАРАКТЕРИСТИКА ПОДГОТОВКИ ПО ПРОГРАММЕ

2.1 Нормативный срок освоения программы – 102 аудиторных часа, включая самостоятельную работу слушателей в аудитории под общим руководством преподавателя, итоговую аттестацию, написание и защиту квалификационной работы.

2.2 Режим обучения – 30 часов в неделю.

2.3 Форма обучения – групповые лекционные и практические занятия или дистанционные занятия посредством сети Интернет с частичным отрывом от работы (ПП №362 от 06.05.08).

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ

Слушатель, освоивший программу, должен:

3.1 совершенствовать профессиональные компетенции, включающие в себя способности:

- способность использовать нормативные правовые документы в своей профессиональной деятельности;
- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности;
- способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем;
- способность производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем;
- способность проводить сбор и анализ исходных данных для проектирования систем защиты информации.

3.2 сформировать профессиональные компетенции, включающие в себя способности:

- способность организовать антивирусную защиту информации при работе с компьютерными системами;
- способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;
- способность проводить обоснование и выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований.

3.3 знать:

- нормативные требования по административно-правовому регулированию в области защиты информации;
- основные модели безопасности в компьютерных системах;
- стандарты по оценке защищенных систем;
- методы защиты информации в операционных системах и вычислительных сетях.
- государственные и международные стандарты в области криптографии.
- типовые шифры замены и перестановки;
- частотные характеристики языков и их использование при построении систем парольной защиты;
- требования к шифрам и их характеристики;
- принципы построения современных криптографических систем;
- типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы;
- методы криптозащиты компьютерных систем и сетей;
- способы и технологии применения криптографии в решении задач аутентификации, и построения юридически значимого документооборота;

3.4 уметь:

- использовать современные информационные технологии при решении задач защиты информации;
- производить анализ систем защиты информации;
- теоретически обосновывать соответствие системы защиты выбранной политике безопасности;
- разрабатывать модели и политику безопасности, используя известные подходы, методы и средства;

3.5. владеть:

- навыками использования критериев оценки систем защиты;
- криптографической терминологией;
- навыками использования основных типов криптографических алгоритмов.

4 ТРЕБОВАНИЯ К СТРУКТУРЕ ПРОГРАММЫ

Программа предусматривает изучение следующих модулей:

1 Правовые аспекты информационной безопасности;

2 Модели безопасности компьютерных систем;

3 Методы и стандарты оценки защищенности компьютерных систем;

4 Криптографические средства и методы защиты компьютерных систем;

5 Криптографические протоколы;

6 Защита информации в операционных системах;

7 Построение защищенных компьютерных сетей;

8 Защита программ и данных.

По окончании теоретического обучения предусматриваются итоговая аттестация (тест) и написание квалификационной работы.

Структура программы представлена в таблице 1.

Таблица 1 - Структура программы

№ п/п	Наименование модулей и форм контроля	Всего аудиторных часов	В том числе:		
			Лекции	Практические занятия (семинары),	Самост. работа под рук. препод.
1	2	3	4	5	6
1	Правовые аспекты информационной безопасности	6	4	—	2
2	Модели безопасности компьютерных систем	8	4	—	4
3	Методы и стандарты оценки защищенности компьютерных систем	10	4	—	6
4	Криптографические средства и методы защиты компьютерных систем	14	8	2	4
5	Криптографические протоколы	6	4	—	2
6	Защита информации в операционных системах	10	4	2	4
7	Построение защищенных компьютерных сетей	10	4	2	4

№ п/п	Наименование модулей и форм контроля	Всего аудиторных часов	В том числе:		
			Лекции	Практические занятия (семинары),	Самост. работа под рук. препод.
1	2	3	4	5	6
8	Защита программ и данных	10	4	2	4
9	Квалификационная работа	24 (включая 4 часа на защиту)	—	—	20
10	Итоговая аттестация (тест)	4	—	—	—
Итого		102 (включая 4 часа на защиту и 4 часа на итоговую аттестацию)	36	8	50

Самостоятельная работа слушателей вне аудитории планируется из расчета:

- на 1 час лекции – 1 час самостоятельной работы;
- на 1 час практических занятий – 0,5 часа самостоятельной работы

5 ТРЕБОВАНИЯ К МИНИМУМУ СОДЕРЖАНИЯ ПРОГРАММЫ

5.1 Учебно-тематический план программы представлен в таблице 2.

Таблица 2 -Учебно-тематический план программы

№ п/п	Наименование модулей и форм контроля	Всего аудиторных часов	В том числе:		
			Лекции	Практические занятия (семинары),	Самост. работа под рук. препод.
1	2	3	4	5	6
1	Правовые аспекты информационной безопасности	6	4	—	2
2	Модели безопасности компьютерных систем	8	4	—	4
3	Методы и стандарты оценки защищенности компьютерных систем	10	4	—	6
4	Криптографические средства и методы защиты компьютерных систем				
4.1.	Введение в криптографию.	4	2	—	—
4.2.	Основные классы шифров и их свойства. Надежность шифров.	6	4		2
4.3.	Криптографические алгоритмы симметричного и асимметричного шифрования, алгоритмы электронных подписей.	4	2	2	2
5	Криптографические протоколы				
5.1.	Криптографические протоколы.	2	2	—	—
5.2.	Реализация криптосистем.	4	2	—	2
6	Защита информации в операционных системах	10	4	2	4
7	Построение защищенных компьютерных сетей	10	4	2	4
8	Защита программ и данных	10	4	2	4
9	Квалификационная работа	24 (включая 4 часа на защиту)	—	—	20

№ п/п	Наименование модулей и форм контроля	Всего аудиторных часов	В том числе:		
			Лекции	Практические занятия (семинары),	Самост. работа под рук. препод.
1	2	3	4	5	6
10	Итоговая аттестация (тест)	4	—	—	—
Итого		102 (включая 4 часа на защиту и 4 часа на итоговую аттестацию)	36	8	50

5.2 Учебная программа по курсу представлена в таблице 3.

Таблица 3 -Учебная программа по модулю

№ п/п	Наименование модуля, разделов и тем	Содержание обучения, основные дидактические единицы
1	2	3
1.	Правовые аспекты информационной безопасности	Государственная система защиты информации, обрабатываемой техническими средствами. Правовое обеспечение защиты информации в России и за рубежом. Лицензирование, стандартизация и сертификация деятельности по защите информации. Правовые аспекты обработки и защиты информации, применения информационных технологий (ФЗ № 149 «Об информации, информационных технологиях и о защите информации»). Правовые аспекты применения средств криптографической защиты информации (№ 63-ФЗ «Об электронной подписи»). Техническая и организационная защита персональных данных (ФЗ № 152 «О персональных данных»).
2.	Модели безопасности компьютерных систем	Основные понятия теории компьютерной безопасности. Модели ценности информации. Угрозы безопасности информации и их классификация. Основные виды защищаемой информации. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Классическая и расширенная модели распространения прав доступа Take-Grant. Алгоритм построения замыкания графа доступов и информационных потоков. Анализ безопасности компьютерных систем с дискреционным управлением доступом. Модели компьютерных систем с мандатным управлением доступом. Классическая модель Белла-ЛаПадулы. Интерпретации модели Белла-ЛаПадулы. Субъектно-ориентированная модель изолированной программной среды. Модели компьютерных систем с ролевым управлением доступом. Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом.
3.	Методы и стандарты	Современные стандарты оценки безопасности

	оценки защищенности компьютерных систем	компьютерных систем. Критерии TCSEC ("Оранжевая книга"). Руководящие документы ФСТЭК. Основные положения руководящих документов ГТК. Определение НСД. Модель нарушителя. Требования классов защищенности СВТ и АС. Требования классов защищенности межсетевых экранов. Классы отсутствия недекларированных возможностей программного обеспечение средств защиты информации. Общие критерии оценки безопасности информационных технологий ИСО/МЭК 15408. Функциональные требования и требования доверия. Разработка профилей защиты и политики безопасности. Технологии анализа рисков. Методики и инструментальные средства оценки рисков CCRAM, FRAP, RiskWatch. Стандарты оценки рисков информационной безопасности. Практические правила управления и требования к системам управления информационной безопасности ИСО/МЭК 17799 и ИСО/МЭК 27001. Зарубежные стандарты в области управления рисками серии ISO 27000.
4.	Криптографические средства и методы защиты компьютерных систем	**4.1. Введение в криптографию** Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Сцитала, решетка Кардано, книжный шифр и др. Основные этапы становления криптографии как науки. Частотные характеристики открытых сообщений. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений. Ключевая система шифра. Основные требования к шифрам. Понятие криптосистемы. Симметричные и асимметричные криптосистемы. Ключевые пары. Вопросы распределения ключей в сети шифрованной связи. **4.2. Основные классы шифров и их свойства. Надежность шифров** Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Одноалфавитные и многоалфавитные замены. Поточные и блочные шифры замены. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Теоретико-информационный подход к оценке стойкости шифров. Ненадежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры.

		4.3. Криптографические алгоритмы симметричного и асимметричного шифрования, алгоритмы электронных подписей Криптографические алгоритмы симметричного шифрования. Сети Фейстеля и алгоритмы, основанные на них (DES, 3DES, ГОСТ 28147-89). Стандарт AES. Режимы использования блочных шифров замены. Понятие односторонней функции и односторонней функции с "лазейкой". Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Преимущества и недостатки асимметричных систем шифрования. Понятие хэш-функции и ее использование в криптографии. Взаимосвязь между свойствами однонаправленности и сложностью нахождения коллизий. Хеш-функции, построенные на основе схем блочного шифрования и их анализ. Алгоритмы выработки хэш-функций MD4, MD5, стандарты SHA и серии P34.
5.	Криптографические протоколы	**5.1. Криптографические протоколы** Понятие протокола как распределенного алгоритма. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Понятие схемы электронной подписи (ЭП). Протоколы электронных подписей RSA, Эль-Гамаля, с посредником. Протоколы взаимной аутентификации. Протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и цифровой подписи. Ключевые структуры с полной матрицей. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Протокол с самосертифицируемыми ключами. Протокол "Керберос". Инфраструктура открытых ключей X.509 и PGP. **5.2. Реализация криптосистем** Проектирование приложений с использованием CryptoAPI и PKCS#11. Архитектура CSP. Проблемы реализации криптографических подсистем и систем управления ключами. Система PGP. Программно-аппаратные средства криптографической защиты информации (СКЗИ). Применение токенов в системах электронных платежей. Особенности использования криптографических методов защиты информации в системах Банк-Клиент. Особенности построения защищенного юридически значимого документооборота с использованием СКЗИ. Криптографические средства и протоколы защиты компьютерных сетей.

6.	Защита информации в операционных системах	Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах. Защита информации в UNIX-системах. Протоколы локальной и сетевой аутентификации, избирательное разграничение доступа на основе векторов, децентрализованный аудит. Защита информации в Windows 2000/XP/Vista/7. Протоколы локальной и сетевой аутентификации, избирательное разграничение доступа на основе списков, централизованный аудит в пределах компьютера. Механизм олицетворения и проблемы его безопасности. Интеграция защищенных операционных систем в защищенную сеть, централизованное управление защитой сети. Плоская доменная модель Windows. Хранение аутентификационной информации пользователей ОС с использованием токенов и СКЗИ. Средства сквозной и двухфакторной аутентификации. Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Реализация аудита в UNIX и Windows.
7.	Построение защищенных компьютерных сетей	Классификация сетевых атак. Атаки, направленные на отказ в обслуживании: floods и nukes. Несанкционированный перехват и навязывание сетевого трафика, создание ложных объектов, несанкционированное изменение путей маршрутизации. Особенности применения шифрования и электронной цифровой подписи в криптографических протоколах IPSec и SSL. Туннелирование сетевого трафика и виртуальные частные сети. Межсетевые экраны, их достоинства и недостатки, пути обхода межсетевых экранов. Криптомаршрутизаторы и особенности их применения. Сетевые сканеры безопасности. Системы автоматизированного обнаружения вторжений. Утечка конфиденциальной информации через Интернет. Защита от спама. Контроль и предотвращение утечки данных в корпоративных сетях. Защита информации в беспроводных сетях.
8.	Защита программ и данных	Особенности защиты программ в многозадачной и многопользовательской среде. Статический и

		динамический анализ кода. Защита кода от изучения, средства и методы защиты от статического и динамического анализа. Защита от несанкционированного копирования. Электронные ключи защиты. Классификация компьютерных вирусов. Методы и средства защиты от компьютерных вирусов. Технологии применения программно-аппаратных комплексов средств защиты информации от несанкционированного доступа. Средства доверенной загрузки. Анализ остаточной информации в компьютерных системах. Проблема утечки криптографических ключей в ОС Windows через программные закладки и информационные потоки. Проведение расследований компьютерных инцидентов (ГОСТ Р ИСО/МЭК ТО 18044-2007).

ТЕМАТИКА И ФОРМЫ ИНДИВИДУАЛЬНОЙ РАБОТЫ. ПРИМЕРНАЯ ТЕМАТИКА КВАЛИФИКАЦИОННЫХ РАБОТ.

Обзор литературы, составление рефератов на темы:

- современные методологии оценки рисков;
- дискреционные и мандатные модели разграничения доступа;
- модель изолированной программной среды;
- протоколы сквозной аутентификации в АИС;
- стандарт шифрования AES, оценка его криптостойкости.
- методы построения виртуальных частных сетей с использованием отечественных криптографических стандартов;
- разработка профилей защиты продукта ИТ-технологий;
- построение системы защиты информации в системах Банк-Клиент;
- методы защиты приложений от анализа алгоритма функционирования;
- анализ остаточной информации в компьютерных системах.

Квалификационная работа выполняется в период обучения на основании методических рекомендаций, подготовленных специалистами компании ЦИБИТ и утвержденные ВНИИПВТИ.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ.
Нормативные акты и стандарты

1. Конституция Российской Федерации.
2. Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. Федеральных законов от 27.07.2010 N 227-ФЗ, от 06.04.2011 N 65-ФЗ, от 21.07.2011 N 252-ФЗ, от 28.07.2012 N 139-ФЗ).
3. Федеральный закон Российской Федерации от 27.12.2002 года N 184-ФЗ "О техническом регулировании" (В редакции ФЗ №160 от 23.07.2008)
4. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
5. Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон Российской Федерации от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».
7. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».
8. Гражданский кодекс Российской Федерации, часть четвертая от 18 декабря 2006 г. № 230-ФЗ.
9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
11. Указ Президента Российской Федерации от 23.09.2005 № 1111 «Об утверждении перечня сведений конфиденциального характера».
12. Указ Президента Российской Федерации от 12.05.2009 № 537 «Стратегия национальной безопасности Российской Федерации до 2020 года».
13. Постановление Правительства РФ от 06.07.2008 г. №512 (В редакции Постановления Правительства от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационной системы персональных данных».
14. Постановление Правительства РФ от 15.09.2008 г. №687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
15. Постановление Правительства РФ от 31.08.06 № 532 (В редакциях Постановлений Правительства РФ от 21.04.2010 N 268, от 24.09.2010 N

749**)** «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

16. «Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» (утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532).
17. Постановление Правительства Российской Федерации от 26 июня 1995 г. N 608. В редакции Постановления Правительства от 23.04.1996 №509 «Положение о сертификации средств защиты информации».
18. Постановление от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
19. Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утверждено Постановлением от 01.11.2012 г. №1119).
20. Постановление Правительства РФ от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» (с изменениями и дополнениями).
21. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
22. «Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем,

защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» (утверждено постановлением Правительства РФ от 16.04.2012 № 313).

23. Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
24. «Положение о лицензировании деятельности по технической защите конфиденциальной информации» (утверждено постановлением Правительства Российской Федерации от 15.08.2006 № 504).
25. Государственный стандарт Российской Федерации ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
26. Государственный стандарт Российской Федерации ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
27. Государственный Стандарт Российской Федерации ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
28. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
29. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».
30. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».
31. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».

32. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».
33. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».
34. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».
35. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
36. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
37. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799 «Информационные технологии. Практические правила управления информационной безопасностью».
38. Государственный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001 «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».
39. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)».
40. Приказ ФСБ РФ от 12 апреля 2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (с изменениями и дополнениями от 30 августа, 28 декабря 2012 г., 10 января 2013 г.)
41. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
42. «Порядок проведения классификации информационных систем персональных данных» (утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20).
43. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21. «Об утверждении Состава и

содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Зарегистрирован в Минюсте РФ 14.05.2013 (рег. № 28375).
44. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года.
45. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года.
46. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года.
47. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года.
48. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года.
49. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25 июля 1997 года.
50. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утвержден решением председателя Гостехкомиссии России от 25 июля 1997 года.
51. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 года № 114.

52. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1- 2, ЗВведен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187.
53. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003.
54. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003.
55. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003.
56. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением заместителя директора ФСТЭК России от 14 февраля 2008 г.
57. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением заместителя директора ФСТЭК России от 15 февраля 2008 г.
58. Стандарт ЦБ РФ СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».
59. Система сертификации средств криптографической защиты информации № РОСС RU.0001.030001.
60. Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00.
61. Стандарт ISO/IEC 27001:2005 «Information technology - Security techniques - Information security management systems - Requirements»
62. ISO/IEC 27002:2005 «Information technology - Security techniques - Code of practice for information security management».
63. Стандарт BS 7799-3:2005 «Information Security Management Systems - Guidelines for Information Security Risk Management».

Учебные пособия

1. *Алферов А.П. , Зубов А.Ю. , Кузьмин А.С. , Черемушкин А.В.* «Основы криптографии». — М.: Гелиос АРВ, 2005.
2. *Черемушкин А.В.* Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009.
3. *Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.* Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011.

4. *Белов Е.Б, Лось В.П., Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2006.
5. *Белкин П.Ю.* Защита программ и данных. Учебное пособие для вузов. / Белкин П.Ю., Михальский О.О., Першаков А.С., Правиков Д.И., Проскурин В.Г., Фоменков Г.В., Щербаков А.Ю.. М.: Радио и связь, 1999.
6. *Грушо А.А., Применко Э.А., Тимонина Е.Е.* Теоретические основы компьютерной безопасности. – М.: Академия, 2009.
7. *Девянин П.Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр Академия , 2005. 144 с.
8. *Иванов О.В., Чугринов А.В., Захаров Л.Н., Зырянов А.В., Калинин С.В., Солтанов А.Г.* «Построение юридически значимого электронного документооборота на основе инфраструктуры открытых ключей». — М.: РФК-Имидж Лаб, 2008. — 224 с.: ил.
9. *Касперски К.* Восстановление данных. Практическое руководство. СПб.: «БХВ-ПЕТЕРБУРГ», 2007.
10. *Конявский В.А. , Иванов О.В. , Чугринов А.В. , Захаров Л.Н* . «Технологии применения программно-аппаратных комплексов средств защиты информации от несанкционированного доступа семейств АККОРД и ШИПКА». — М.: РФК-Имидж Лаб, 2009. — 308 с.
11. *Кэрриэ Б.* Криминалистический анализ файловых систем.- М.: Питер, 2007.
12. *Проскурин, В.Г.* Защита в операционных системах / В.Г. Проскурин, С.В. Крутов, И. В. Мацкевич. – М. : Радио и связь, 2000.
13. *Щербаков А.Ю., Домашев А.В.* Прикладная криптография. Издательство: Русская Редакция, 2002 г.
14. *Россинская Е.Р., Усов А.И.* Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001.
15. *Руссинович М., Соломон Д.* Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс / Пер. с англ. – 4-е изд. — М.: Издательство «Русская Редакция»; Спб.: Питер, 2006.
16. *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганографии. – М.: Горячая линия–Телеком, 2010.
17. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995.
18. *Синадский Н.И.* Анализ и восстановление данных на носителях с файловой системой NTFS – Екатеринбург; ГОУ ВПО УГТУ-УПИ, 2007.
19. *Скиба В.Ю., Курбатов В.А.* Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008.
20. *Смарт Н.* Криптография. Издательство: Техносфера, 2006.
21. *Федотов Н.Н.* Форензика - компьютерная криминалистика. М.: Юридический мир, 2007.
22. *Шнаер Б.* «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002.
23. Фундаментальное руководство по расследованию компьютерных происшествий для Windows. –

<http://www.microsoft.com/rus/technet/security/guidance/disasterrecovery/computer_investigation/>

6 ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММ

Формы и методы контроля и оценки результатов освоения модулей представлены в таблице 4.

Таблица 4 -Формы и методы контроля и оценки результатов освоения модулей

Наименование модулей	Основные показатели оценки	Формы и методы контроля и оценки
Правовые аспекты информационной безопасности		дифференцированный зачет
Модели безопасности компьютерных систем		зачет
Методы и стандарты оценки защищенности компьютерных систем		дифференцированный зачет
Криптографические средства и методы защиты компьютерных систем		дифференцированный зачет
Криптографические протоколы		зачет
Защита информации в операционных системах		дифференцированный зачет
Построение защищенных компьютерных сетей		зачет
Защита программ и данных		зачет
Квалификационная работа		дифференцированный зачет
Итоговая аттестация		тестирование

Тестирование проводится в последний день занятий.

Прошедшим тестирование считается слушатель, ответивший верно не менее, чем на 60% вопросов.

Ответы на вопросы для тестирования заносятся в таблицу (форма таблицы выдается слушателям вместе с вопросами для тестирования).

Время, отводимое на тестирование – 2 (два) часа.