42

Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

СОГЛАСОВАНО
Начальник I Управления
ФСТЭК России
_____ А.Г. Дротенко
"6" мая 2015 г.

УТВЕРЖДАЮ
Директор АНО ДПО
«Учебный центр «Информзащита»
_____ М.С. Савельев
"19" мая 2015 г.

СОГЛАСОВАНО
Первый заместитель начальника
Центра ФСБ России
_____ А.С. Кузьмин
"10" 04. 2015 г.

СОГЛАСОВАНО
Заместитель Председателя Совета УМО
по образованию в области
информационной безопасности
_____ Е.Б. Белов
"16" 04. 2015 г.

Срок действия согласования
1 июня 2017 г.
от ФСБ России 30.06.16 г. N149/3-144
от ФСТЭК России 12.07.16 г. N240/11/3121
Заместитель Председателя УМО ИБ
Белов

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ РУКОВОДИТЕЛЕЙ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ ПОДРАЗДЕЛЕНИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЗАЩИТЫ ИНФОРМАЦИИ) ПРЕДПРИЯТИЙ, ОРГАНИЗАЦИЙ И УЧРЕЖДЕНИЙ

по направлению «Информационная безопасность»

Виды профессиональной деятельности:
организационно-управленческая, эксплуатационная, контрольно-аналитическая

Трудоемкость обучения: 504 ч.
Срок действия согласования: до 01 июля **2016 г.**

Москва
2015

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Цель реализации программы

Целями реализации настоящей «Программы профессиональной переподготовки руководителей и инженерно-технических специалистов подразделений обеспечения информационной безопасности (защиты информации) предприятий, организаций и учреждений» (далее – «Программа») являются совершенствование имеющихся и/или формирование у обучающихся (слушателей) новых необходимых компетенций (знаний и умений), необходимых для последующего ведения нового вида профессиональной деятельности и выполнения трудовых функций в сфере информационной безопасности (по обеспечению информационной безопасности автоматизированных систем от вредоносных технических воздействий в рамках ОКВЭД 75.24 «Деятельности по обеспечению общественного порядка и безопасности. Обеспечение безопасности средств связи и информации»).

При разработке содержания Программы в части требований к результатам освоения образовательных программ учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего профессионального образования (ФГОС ВПО) по направлению подготовки "Информационная безопасность", а именно ФГОС ВПО 10.05.01 «Компьютерная безопасность» (квалификация (степень) "специалист")" по специализации "Информационная безопасность объектов информатизации на базе компьютерных систем".

Программа относится к дополнительным профессиональным программам в области информационной безопасности (далее - ИБ) и разработана на основании установленных квалификационных требований (видов профессиональной деятельности, трудовых функций и уровней квалификации) профессионального стандарта для «Специалиста по информационной безопасности» приказом Министерства труда и социальной защиты Российской Федерации, а также с учётом иных доступных квалификационных требований, указанных в квалификационных справочниках, утверждаемых в порядке, устанавливаемом Правительством Российской Федерации, по соответствующим должностям, профессиям, специальностям (в соответствии с Приказом Минтруда России №148н от 12 апреля 2013 г. «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»).

Кроме того, при разработке программы учитывались требования и положения:

- Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»;

- Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499), зарегистрированного в Минюсте РФ 20 августа 2013 г. Регистрационный № 29444;

- Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);

- ранее использовавшегося Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090301 «Компьютерная безопасность» (квалификация (степень) "специалист")" (утв. приказом Минобрнауки РФ от 17.01.2011 № 69, ред. от 31.05.2011, Зарегистрировано в Минюсте РФ 20.04.2011 Регистрационный № 20544).

Плановая (нормативная) продолжительность освоения Программы составляет 512 и более академических часов аудиторных занятий (в зависимости от набора выбранных программ, модулей, курсов вариативной части программы).

Программа разработана Учебным центром «Информзащита» в инициативном порядке (Приказ Директора УЦ от «16 » декабря 2014 г. № 01/11).

Обучение по данной дополнительной образовательной Программе направлено на решение следующих основных задач:

- получение и углубление профессиональных знаний и умений обучающихся по правовым основам защиты информации, организационным мерам и техническим средствам обеспечения безопасности при использовании современных информационных технологий на предприятиях;
- удовлетворение потребности специалистов в получении знаний об актуальных нормативных требованиях к защите и о новейших достижениях в области защиты конфиденциальной информации и систем её обработки (в комплексном обновлении их профессиональных компетенций, в рамках того же вида профессиональной деятельности);
- популяризация передовых технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации предприятий (объединений), организаций и учреждений, распространение передового опыта по успешному решению задач обеспечения информационной безопасности;
- оказание помощи предприятиям (объединениям), организациям и учреждениям в повышении квалификации и переподготовке руководителей и инженерно-технических работников (специалистов) служб безопасности и подразделений защиты информации по вопросам построения и эффективного применения комплексных систем защиты информации;
- профессиональная переподготовка руководителей и инженерно-технических работников (специалистов по защите информации) предприятий и организаций, в соответствии с квалификационными требованиями к персоналу в штате у соискателя лицензии (лицензиата) на осуществление лицензируемых видов деятельности по направлениям ФСБ России и ФСТЭК России.

Программа ориентирована на следующие категории обучающихся (специалистов, слушателей):

- начальников служб безопасности, руководителей подразделений обеспечения информационной безопасности (90ОИБ), технической защиты конфиденциальной информации (ТЗКИ), ответственных за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий. Возможное наименование должностей:
  - Начальник службы/отдела/департамента/лаборатории/сектора ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ (защите информации)
  - Руководитель службы/отдела/департамента ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Заместитель руководителя по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Заместитель руководителя службы/отдела/департамента корпоративной безопасности по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Главный специалист по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Главный инженер по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
- аналитиков подразделений ОИБ (ТЗКИ), отвечающих за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем ИС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации. Возможное наименование должностей:
  - Специалист/эксперт/инженер в области ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Специалист/эксперт/инженер по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Специалист/эксперт/инженер по безопасности компьютерных систем
  - Специалист/эксперт/инженер по анализу защищенности компьютерных систем
  - Специалист/эксперт/инженер по безопасности распределенных компьютерных систем
  - Специалист/эксперт/инженер по безопасности информационных ресурсов и информационных систем
  - Специалист/эксперт по обеспечению безопасности информации
  - Консультант по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
- администраторов средств защиты и специалистов подразделений ОИБ (ТЗКИ), ответственных за защиту конфиденциальной информации техническими средствами. Возможное наименование должностей:
  - Техник/администратор по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
  - Администратор безопасности операционных систем и систем управления базами данных

1.2 Характеристика нового вида профессиональной деятельности, новой квалификации

Слушатель, успешно завершивший обучение по данной Программе, должен решать профессиональные задачи по обеспечению защищенности компьютерных систем от

вредоносных технических воздействий в рамках «Деятельности по обеспечению общественного порядка и безопасности. Обеспечение безопасности средств связи и информации» (Код ОКВЭД75.24).

а. **Область профессиональной деятельности** слушателей, прошедших обучение по Программе для выполнения нового вида профессиональной деятельности по обеспечению защищенности компьютерных систем от вредоносных технических воздействий включает сферы техники и технологии, охватывающие совокупность проблем, связанных с:

- анализом и оценки уровня защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий в условиях существования угроз в информационной сфере
- эксплуатацией и администрированием средств и систем защиты информации компьютерных систем.

б. Объектами профессиональной деятельности являются:

- автоматизированные системы, входящие в них средства обработки, хранения и передачи информации и информационно-технологические ресурсы, подлежащие защите и функционирующие в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем;
- методы и реализующие их средства защиты информации в компьютерных системах;
- процессы, возникающие при защите информации, обрабатываемой в компьютерных системах;
- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах.

в. Виды профессиональной деятельности и решаемые задачи

Программа ориентирована на подготовку к следующим подвидам профессиональной деятельности:

- организационно-управленческая;
- эксплуатационная;
- контрольно-аналитическая.

Слушатели, успешно завершившие обучение по данной Программе, должны решать следующие профессиональные задачи в соответствии с подвидами профессиональной деятельности:

- **организационно-управленческая деятельность:**
  - управление информационной безопасностью объекта;
  - организация работ по выполнению требований режима защиты информации, в

том числе информации ограниченного доступа;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- контроль эффективности реализации политики информационной безопасности объекта;
- разработка проектов нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- участие в определении потребности в средствах защиты информации, контроль их поставки и эксплуатации;
- поиск рациональных решений при выборе средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.

– **эксплуатационная деятельность:**
- выполнение работ по защите информации;
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- проверка технического состояния и остаточного ресурса оборудования защиты информации, организация профилактических проверок и текущего ремонта;
- приемка и освоение программно-аппаратных средств защиты информации;
- составление инструкций по эксплуатации аппаратно-программных средств защиты информации;
- обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;
- проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

– **контрольно-аналитическая деятельность:**
- контроль эффективности реализации политики информационной безопасности объекта;
- проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- участие в обследовании объектов информатизации, их категорировании и аттестации по требованиям безопасности информации;
- проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы;
- проведение инструментального мониторинга защищенности компьютерных систем;
- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей;
- сбор и анализ исходных данных для проектирования систем защиты информации.

г. Уровень квалификации в соответствии с профессиональным стандартом

Профессиональная переподготовка по настоящей Программе осуществляется на базе высшего и среднего профессионального образования.

К освоению данной дополнительной профессиональной Программы переподготовки допускаются лица:

- имеющие среднее профессиональное и (или) высшее образование;
- получающие среднее профессиональное и (или) высшее образование.

1.3 Планируемые результаты обучения

1.3.1 Приобретаемые профессиональные компетенции

Слушатель, успешно завершивший обучение по данной Программе, должен обладать следующими профессиональными и общепрофессиональными компетенциями (коды ПК даны в соответствии с ФГОС ВПО 10.05.01 (090301)):

1.3.1.1 Общепрофессиональные

понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ОПК-3);

использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5);

учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности (ОПК-7);

работать с программными средствами прикладного, системного и специального назначения (ОПК-8);

разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ОПК-11);

организовать антивирусную защиту информации при работе с компьютерными системами (ЩПК-13);

1.3.1.2 Профессиональные

1.3.1.2.1 в проектной деятельности:

проводить сбор и анализ исходных данных для проектирования систем защиты информации (ПК-21);

участвовать в разработке проектной документации (ПК-22);

проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-23);

участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы (ПК-24);

оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи (ПК-25).

1.3.1.2.2 в контрольно-аналитической деятельности:

участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований к уровню защищенности компьютерной системы (ПК-26);

к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей (ПК-27);

обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения (ПК-28);

оценивать эффективность систем защиты информации в компьютерных системах (ПК-29);

1.3.1.2.3 в организационно-управленческой деятельности:

организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-30);

разрабатывать оперативные планы работы первичных подразделений (ПК-31);

разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-32);

разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-33);

1.3.1.2.4 в эксплуатационной деятельности:

производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем (ПК-34);

принимать участие в эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем (ПК-35);

производить проверку технического состояния и профилактические осмотры

оборудования по защите информации (ПК-36);

выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации (ПК-37);

разрабатывать и составлять инструкции и руководства пользователей по эксплуатации средств обеспечения информационной безопасности компьютерных систем и аппаратно-программных средств защиты информации (ПК-38).

1.3.2 Приобретаемые знания и умения

Слушатель, успешно завершивший обучение по данной Программе, должен обладать знаниями и умениями в следующих областях науки, техники и технологии, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере:

1.3.2.1 Знать

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации
- сущность и понятие информационной безопасности, характеристику ее составляющих
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области
- правовые основы организации защиты государственной тайны и конфиденциальной информации
- методики оценки и разработки моделей угроз информационной безопасности
- правовые нормы и стандарты по лицензированию в области обеспечения защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну и сертификации средств защиты информации
- систему организации комплексной защиты информации ограниченного доступа в системе, включая защиту персональных данных
- технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации
- методы и способы несанкционированного доступа (НСД) к информации, способы и средства защиты от НСД к информации на объектах информатизации
- методы и способы защиты информации с использованием СКЗИ
- принципы и методы управления системой обеспечения информационной безопасности в ведомстве (предприятии, организации)
- существующие криптографические алгоритмы, используемые для ЗИ, и принципы построения защищенного документооборота с использованием электронной подписи и виртуальных частных систем
- принципы организации информационных систем в соответствии с требованиями по защите информации
- источники угроз информационной безопасности и меры по их предотвращению
- современные программно-аппаратные средства и способы обеспечения информационной безопасности в КС

- состав и принципы работы защищенных компьютерных систем, операционных систем и сред
- особенности применения программно-аппаратных и технических средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных
- источники угроз информационной безопасности и меры по их предотвращению
- требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации
- основные виды политик управления доступом и информационными потоками в компьютерных системах
- принципы построения современных операционных систем и особенности их применения для решения задач защиты информации
- механизмы реализации вредоносных программно-технических и информационных воздействий в компьютерных системах
- защитные механизмы и средства обеспечения сетевой безопасности
- средства и методы предотвращения и обнаружения вторжений
- основные средства и методы анализа программных реализаций
- технические каналы утечки информации и методы защиты
- содержание и порядок аттестации компьютерных систем на предмет их соответствия требованиям по защите
- принципы работы и правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты и другого оборудования
- организацию ремонта и технического обслуживания средств и систем безопасности
- порядок оформления технической документации по защите информации инструкции по соблюдению режима проведения специальных работ
- методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
- порядок оформления документации по приемке и постановке на учет в организации приобретаемых программно-аппаратных средств защиты информации
- правила и нормы охраны труда, техники безопасности, производственной (промышленной) санитарии и противопожарной защиты .

1.3.2.2 Уметь

- применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах
- осуществлять техническое обслуживание и текущий ремонт программно-аппаратных средств обеспечения ИБ
- проводить мониторинг эффективности программно-аппаратных средств обеспечения ИБ в КС
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
- применять технические средства обеспечения информационной безопасности
- участвовать в эксплуатации технических средств обеспечения информационной

безопасности
- проводить мониторинг эффективности технических средств обеспечения ИБ в КС
- участвовать в эксплуатации компонентов подсистем безопасности КС, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности
- выполнять работы по администрированию подсистем безопасности компьютерных систем
- производить установку и адаптацию компонентов подсистем безопасности компьютерных систем
- вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в компьютерных системах
- формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе
- применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
- проводить анализ показателей качества сетей и систем связи
- анализировать и оценивать угрозы информационной безопасности объекта
- оценивать полноту и качество выполнения работниками организации требований политики безопасности
- иметь навыки по установке, настройке, эксплуатации и обслуживанию аппаратно-программных средств защиты информации
- анализировать и оценивать угрозы информационной безопасности объекта
- пользоваться нормативными документами по защите информации
- разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации
- разрабатывать документы, необходимые для аттестации объектов информатизации по требованиям безопасности информации
- правильно эксплуатировать системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации

1.3.2.3 Владеть

- профессиональной терминологией;
- навыками применения средств антивирусной защиты;
- навыками организации и обеспечения режима защиты информации;
- навыками эксплуатации комплексов удостоверяющих центров;
- методами технической защиты информации;
- методами организации и управления деятельностью;
- методиками проверки защищенности объектов информатизации на соответствие требо-

ваниям нормативных документов.

1.3.3 Достигаемый уровень квалификации

Настоящая Программа обеспечивает достижение 5 (пятого) уровня квалификации (при исходном среднем профессиональном образовании) или 6 (шестого) уровня квалификации (при исходном высшем образовании) в соответствии с требованиями Профессионального стандарта «Специалист по информационной безопасности», указанного в п. 1.1.

Наименование вида профессиональной деятельности: деятельность по обеспечению защищенности компьютерных систем от вредоносных технических воздействий.

Функциональная карта вида профессиональной деятельности

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень квалификации
A	Эксплуатация защищенных КС и применение методов и средств обеспечения их безопасности	Пятый	Применение программно-аппаратных средств обеспечения информационной безопасности в КС	A/01.5	Пятый
			Применение технических средств обеспечения информационной безопасности защищенных КС	A/02.5	Пятый
			Эксплуатация комплексных систем обеспечения информационной безопасности в КС	A/03.5	Пятый
B	Администрирование и эксплуатация аппаратно-программных средств защиты информации в компьютерных системах	Шестой	администрирование систем безопасности КС	B/01.6	Шестой
			организация профилактических проверок, регламентов технического обслуживания и текущего ремонта систем безопасности КС	B/02.6	Шестой
			приемка и освоение программно-аппаратных средств защиты информации	B/03.6	Шестой

2 СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Настоящая Программа разработана и реализуется с учётом основных особенностей профессиональной деятельности руководителей и специалистов подразделений информационной безопасности и защиты конфиденциальной информации, а именно:

- сложностью единовременного отрыва от работы на продолжительное время для освоения учебных дисциплин, обусловливающей необходимость реализации возможности поэтапного модульного обучения;
- высокой динамикой изменений в сфере ИТ, в области угроз безопасности, технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации, требующей постоянной актуализации соответствующих модулей (курсов, дисциплин) обучения;
- наличием существенных различий в исходных образовательных уровнях и профессиональной подготовленности обучающихся.

С учетом вышесказанного, Программа построена по модульному принципу и предполагает определённую вариативность, позволяющую в наибольшей степени обеспечить соответствие обучения конкретным направлениям и подвидам профессиональной деятельности (специализациям) и адаптивность к задачам, решаемым специалистами в рамках своих должностных или функциональных обязанностей (в дальнейшем называемую актуализацией).

Часть плановых часов обучения по специальному (профессиональному) циклу Программы) отводятся на вариативную часть для актуализации знаний и углубленного изучения нескольких выбранных для специализации модулей (курсов, дисциплин).

Модули актуализации (курсы вариативной части для углубленного изучения материала отдельных разделов и тем) выбираются из заданного для данного направления списка самим обучающимся (специалистом) либо организацией, направившей его на обучение, в соответствии с поставленными перед ним задачами и его профессиональными интересами.

Возможность обучения по Программе специалистов с различными исходными образовательными уровнями и профессиональной подготовленностью обеспечивается наличием в Учебном плане и Программе переподготовки дисциплин (модулей, курсов) подготовительного естественнонаучного (инженерно-технического) цикла и вариативной части специального (профессионального) цикла.

При освоении Программы может производиться перезачет учебных дисциплин (модулей, курсов) как естественнонаучного, так и профессионального цикла, освоенных обучающимися ранее (или изучаемых параллельно) в ходе освоения ими основных образовательных программ профессионального образования соответствующего уровня, и (или) дополнительных профессиональных образовательных программ того же направления, в т.ч. в иных образовательных организациях/учреждениях.

Наименование		Общая трудоемкость, час.	По учебному плану с использованием								Самостоятельная работа, час	Текущий контроль			Промежуточная аттестация	
			Очные занятия, час.				Дистанционные занятия, час									
			всего	из них			всего	из них				РК РГР Реф.	КР	КП	Зачет	Экзамен
				лекц	лаб. Раб.	прак. зан., семинары		лекц.	лаб. Раб	прак. зан., семинары						
1		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Естественнонаучный цикл		**144**														
Дискретная математика	вариант О	**48**	**38**	24		14					6		*2 (Т)*		*2 (Т)*	
	вариант Д						**38**	24		14	6		*2 (Д)*		*2 (Д)*	
Теория вероятностей и математическая статистика	вариант О	**48**	**38**	24		14					6		*2 (Т)*		*2 (Т)*	
	вариант Д						**38**	24		14	6		*2 (Д)*		*2 (Д)*	
Информационные технологии	вариант О	**48**	**38**	16		22					6		*2 (Т)*		*2 (Т)*	
	вариант Д						**38**	16		22	6		*2 (Д)*		*2 (Д)*	
Профессиональный цикл		**360**														
Базовая (обязательная) часть		**200**														
Базовый курс по безопасности информационных технологий		**52**	**38**	36		2					10		*2 (Т)*		*2 (Т)*	
Безопасность компьютерных сетей		**40**	**30**	16	8	8					6				*2 (Т)*	
Безопасность операционных систем		**56**	**44**	20	12	12					10				*2 (Т)*	
Работа органа криптографической защиты		**20**	**16**	8		8					2				*2 (Т)*	
Использование ЭП и ИОК (PKI)		**32**	**24**	10	10	4					6				*2 (Т)*	
Вариативная (актуализируемая) часть (дисциплины на выбор обучающихся по направлениям специализации, не менее, час.)		160														
Дисциплины по теме «Криптографическая защита информации, PKI и электронная подпись» (не менее, час.)		24													*2 (Т\Д)*	
Дисциплины по теме «Администрирование средств защиты информации» (не менее, час.)		30													*2 (Т\Д)*	
Дисциплины по теме «Защита информации от утечек по техническим каналам» (не менее, час.)		24													*2 (Т\Д)*	

Дисциплины по теме «Защита персональных данных» (не менее, час.)	24													*2 (Т\Д)*	
Дисциплины по теме «Защищенный электронный документооборот» (не менее, час.)	8													*2 (Т\Д)*	
Дисциплины по теме «Управление информационной безопасностью» (не менее, час.)	40													*2 (Т\Д)*	
Итого	**504**														
Итоговая аттестация	**8**													*8 (Т)*	

Сокращения и обозначения в таблице:
«Т» - прием, осуществляемый по традиционной образовательной технологии;
«Д» - прием, осуществляемый с использованием дистанционных образовательных технологий.
КП - курсовой проект, КР - курсовая работа, РК - контрольная работа, РГР - расчетно-графическая работа, Реф. – реферат.

2.2 Рабочие программы дисциплин (модулей)

Наименование дисциплин (модулей, курсов), разделов, тем	Общее кол-во часов	В том числе			
		Лекции	Практические занятия, семинары	Самостоятельная работа	Контроль (зачет экзамен)
2	3	4	5	6	7
Естественнонаучный цикл					
Дискретная математика	**48**	**24**	**14**	**6**	**4**
Основы теории множеств	4	3	1		
Комбинаторика	7	4	2	1	
Математическая логика	7	4	2	1	
Переключательные функции	5	2	2	1	
Теория алгоритмов	8	4	3	1	
Основы теории конечных автоматов	7	4	2	1	
Теория графов	6	3	2	1	
Контрольные занятия	4				4
Теория вероятностей и математическая статистика	**48**	**24**	**14**	**6**	**4**
Случайные события	4	3	1		
Случайные величины	8	4	3	1	
Случайные векторы	7	4	2	1	
Случайные последовательности	7	4	2	1	
Математическая статистика	10	5	4	1	
Приложения математической статистики	8	4	2	2	
Контрольные занятия	4				4
Информационные технологии	**48**	**16**	**22**	**6**	**4**
Информация, ИТ и ИС	1,5	0,5	1		
Технологии обработки различных видов информации	11	5	4	2	
Информационные хранилища. Архивирование файлов. Файловые серверы и базы данных	3	1	2		
Централизованные и распределённые системы обработки данных. Облачные ИТ	5	1	4		
Сетевые технологии обработки и передачи информации	18	6	8	4	
Интеграция ИТ на рабочем месте пользователя. Корпоративные ИС	2	1	1		
Системы удалённого доступа к государственным и коммерческим услугам	2	1	1		
Информационные сервисы сети Интернет	1,5	0,5	1		
Контрольные занятия	4				4

Профессиональный цикл					
Базовая (обязательная) часть					
Безопасность информационных технологий	**52**	**38**	**2**	**10**	**2**
Основы безопасности ИТ	14	12		2	
Правовые основы обеспечения информационной безопасности	10	8		2	
Организационные меры защиты	10	8		2	
Средства защиты от внутренних нарушителей	7	4	1	2	
Обеспечение безопасности компьютерных сетей	9	6	1	2	
Контрольные занятия	2				**2**
Безопасность компьютерных сетей	**40**	**16**	**16**	**6**	**2**
Типовая IP-сеть организации	0,5	0,5			
Классификация сетевых уязвимостей и атак. Работа с базами атак и уязвимостей	0,5	0,5			
Защитные механизмы и средства обеспечения безопасности	1	0,5		0,5	
Базовые принципы сетевого взаимодействия	2,5	0,5		2	
Безопасность физического и канального уровней	2	1	1		
Проблемы безопасности протокола разрешения адресов ARP	2	1	1		
Стандарт 802.1x. Безопасность на уровне порта	2	1	1		
Защита периметра сети	6	2	2	2	
Защита трафика на сетевом уровне	4	2	2		
Безопасность транспортного уровня модели OSI	4	2	2		
Анализ защищённости корпоративной сети как превентивный механизм защиты	4	1	2	1	
Защита трафика на транспортном уровне	2	1	1		
Обнаружение сетевых атак	3,5	1	2	0,5	
Общие проблемы безопасности служб прикладного уровня	2	1	1		
«Honeynet» или сеть-приманка для изучения поведения нарушителей	2	1	1		
Контрольные занятия	2				**2**
Работа органа криптографической защиты	**20**	**8**	**8**	**2**	**2**
Основы криптографии	4	2	2		
Нормативное регулирование вопросов криптографической защиты информации	5	2	1	2	
Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ	4	2	2		

Обеспечение юридической значимости электронных документов	3	1	2		
Корпоративные информационные и телекоммуникационные системы, защищенные с использованием шифровальных (криптографических) средств	2	1	1		
Контрольные занятия	2				**2**
Использование ЭП и ИОК (PKI)	**32**	**10**	**14**	**6**	**2**
Традиционные бумажные и электронные документы	0,5	0,5	-		
Правовые вопросы применения ЭП и СКЗИ в России	2,5	0,5	-	2	
Криптографические методы защиты информации	0,5	0,5	-		
Электронный сертификат: структура сертификата, издание, импорт и экспорт сертификатов	1	0,5	0,5		
Электронные ключи	2	0,5	1,5		
Электронные идентификаторы	2	0,5	1,5		
Криптопровайдеры (CSP)	1,5	1	0,5		
Интернет-банкинг. Проблемы безопасности. при применении электронных подписей	3,5	1,5	2		
Компоненты PKI	3	1	0	2	
Принципы доверия PKI	4	1	3		
Управление доверием	2	0,5	0,5	1	
Проверка подлинности цифровых сертификатов в инфраструктуре PKI	2,5	0,5	2		
Процедуры аннулирования сертификатов в PKI. Списки отозванных сертификатов, OCSP Server, Revocation Provider	2,5	0,5	1	1	
Сервер меток времени (TSP Server)	1,5	0,5	1		
Усовершенствованная подпись	1	0,5	0,5		
Контрольные занятия	2				**2**
Безопасность операционных систем	**56**	**20**	**24**	**10**	**2**
Риски, угрозы, уязвимости, атаки	3	2		1	
Встроенные средства защиты Windows	8	2	4	2	
Идентификация и аутентификация	7	3	4		
Разграничение доступа к ресурсам	5	2	2	1	
Защита сетевого взаимодействия	8	3	3	2	
Повышение уровня защищенности рабочей среды пользователей	4	1	2	1	
Анализ параметров безопасности и конфигурирование безопасности	7	2	4	1	
Обеспечение объективного контроля работы пользователей и системных администраторов	5	2	2	1	

Повышение защищенности служб	4,5	2	2	0,5	
Поддержание программного обеспечения в актуальном состоянии	2,5	1	1	0,5	
Контрольные занятия	2				2

Набор курсов вариативной части профессионального цикла

Профессиональный цикл ***Вариативная (актуализируемая) часть*** *(дисциплины на выбор обучающихся по направлениям, не менее, час.)*	*160*
Дисциплины по теме «Криптографическая защита информации, PKI и электронная подпись» (не менее, час.)	**24**
Использование ЭП и PKI	24
Автоматизация управления жизненным циклом сертификатов, изданных с помощью "КриптоПро УЦ"	8
Разработка и управление инфраструктурой открытых ключей на базе Microsoft Windows	32
Использование ЭП и PKI с применением продуктов «Сигнал-КОМ»	16
Организационно-правовые основы применения ЭП и деятельности удостоверяющих центров	8
Оператор удостоверяющего центра	16
Инфраструктура открытых ключей на Microsoft Windows Server 2008 R2	8
Дисциплины по теме «Администрирование средств защиты информации» (не менее, час.)	30
Порядок развертывания и применения PKI на основе ПАК "КриптоПро УЦ" 2.0	16
Эксплуатация и техническое обслуживание PKI на основе ПАК «КриптоПро УЦ»	16
Применение «КриптоПро IPsec» для обеспечения защиты данных передаваемых в IP-сетях	16
Порядок миграции на ПАК "КриптоПро УЦ" 2.0	16
Внедрение системы управления доступом Cisco Secure ACS Implementing Cisco Secure Access Control System (ACS)	24
ArcSight Express 4.0: администрирование и эксплуатация (ArcSight Express 4.0, CORR-Engine Administration and Operations)	40
ArcSight ESM Administrator 6 CORR Engine	32
ArcSight ESM Security Analyst	20
Построение и эксплуатация инфраструктуры аутентификации на основе продуктов: электронные ключи eToken и SafeNet Authentication Manager 8.0	32
Эксплуатация инфраструктуры аутентификации на основе продуктов: электронные ключи eToken и SafeNet Authentication Manager 8.0	24
Построение корпоративной системы защиты конфиденциальной информации на основе линейки продуктов Secret Disk компании «Аладдин Р.Д.»	16
Построение инфраструктуры аутентификации на основе продуктов компании Аладдин Р.Д. Электронные ключи eToken и система Token Management System	32

Aladdin Token Management System 2.0: установка, настройка и эксплуатация системы	24
Система анализа защищенности Assuria Auditor	16
Внедрение Cisco Clean Agent для контроля доступа к сети	24
Внедрение системы защиты безопасности информации при помощи Check Point Endpoint Security R80	24
Администрирование Check Point Security Administration 2013 (R76)	24
Управление безопасностью средствами Check Point R77 (Check Point Security Administration R77)	24
Расширенные возможности по поиску неполадок в продуктах компании Check Point (Advanced troubleshooting Check Point)	24
Check Point – рекомендованная практика (Check Point best practice)	16
Учебный модуль по управлению работой приложений Check Point	8
Учебный модуль Check Point DLP	8
Учебный модуль Check Point IPS	8
Вводный курс по операционной системе JUNOS	8
Маршрутизация в ОС JUNOS (JUNOS Intermediate Routing (JIR))	16
Контроль доступа средствами JunosPulse (Junos Pulse Access Control (JPAC))	24
Изучение оборудования безопасного удаленного доступа JunosPulse (Junos Pulse Secure Access (JPSA))	32
Программное обеспечение JUNOS. Основные вопросы маршрутизации	8
Внедрение межсетевых экранов Cisco ASA	40
Многофункциональные межсетевые экраны FortiGate. Часть 1	16
Многофункциональные межсетевые экраны FortiGate. Часть 2	24
Использование сетевого оборудования Cisco®. Часть 1	40
Использование сетевого оборудования Cisco®. Часть 2	40
Применение системы сетевой безопасности на базе Cisco IOS	40
Реализация технологий VPN на оборудовании Cisco IOS	40
Внедрение системы предотвращения вторжений Cisco	32
Kaspersky Endpoint Security and Management. Базовый курс.	24
Kaspersky Endpoint Security for Windows. Базовый курс	24
Kaspersky Endpoint Security and Management. Расширенный курс.	40
Kaspersky Endpoint Security for Windows. Расширенный курс	16
Планирование, внедрение и поддержка инфраструктуры службы каталога Microsoft Windows Server 2003	40
Поддержка баз данных в Microsoft SQL Server 2005	40

Разработка безопасности для Microsoft SQL Server 2005	16
Разработка и управление инфраструктурой открытых ключей на базе Microsoft Windows	32
Внедрение и администрирование защиты в сети на базе Microsoft Windows Server 2003	40
Новые возможности Windows Server 2012	8
Управление System Center Operations Manager 2007	40
Deploying and Administering Microsoft Forefront Client Security	24
Deploying and Administering Microsoft Forefront Security for Exchange Server, Microsoft Forefront Security for SharePoint, and Microsoft Forefront Server Security Management Console	16
Обслуживание баз данных в Microsoft SQL Server 2008 R2	40
Установка и настройка операционной системы Windows 7	24
Планирование и управление развертыванием Windows 7	40
Настройка, управление и обслуживание серверов Windows Server 2008	40
Основы Windows Server 2008 R2	40
Настройка сетевой инфраструктуры Windows Server 2008 и устранение неполадок	40
Настройка доменных служб Active Directory на базе Windows Server 2008 и устранение неполадок в их работе	40
Конфигурирование решений идентификации и доступа в среде Active Directory Windows Server 2008	24
Планирование, развертывание и управление Microsoft Systems Center Configuration Manager 2007	40
Регулирование доступа пользователей в сеть с помощью Cisco NAC фаза 2	24
Основы инсталляции, настройки и управления межсетевым экраном Palo Alto	24
Углубленный курс управления межсетевым экраном Palo Alto	16
Построение защищенных виртуальных сетей на основе IPsec с использованием алгоритмов шифрования ГОСТ на базе шлюзов безопасности S-Terra CSP	16
Обеспечение безопасности сетей с помощью маршрутизаторов и коммутаторов Cisco	40
Система централизованного управления Stonesoft Management Center (SMC) 5.4	8
Система защиты от атак Stonesoft IPS and Layer 2 Firewall 5.4	16
Межсетевой экран Stonesoft Firewall/VPN 5.4	16
Внедрение виртуальных частных сетей средствами Cisco ASA	40
Средство криптографической защиты информации «Верба-OW»	8
Система защиты информации «Vipnet»	24
Дисциплины по теме «Защита информации от утечек по техническим каналам» (не менее, час.)	**24**
Защита информации от утечки по техническим каналам	40
Организация защиты от закладочных устройств	24

Дисциплины по теме «Защита персональных данных» (не менее, час.)	**24**
Защита персональных данных	24
Техническая защита персональных данных	16
Сложные проблемы применения законодательства о персональных данных в кредитно-финансовых учреждениях	8
Нетехнические методы защиты персональных данных и коммерческой тайны	8
Регулирование отношений при осуществлении проверок операторов персональных данных	8
Дисциплины по теме «Защищенный электронный документооборот» (не менее, час.)	**8**
Организация конфиденциального делопроизводства	16
Применение технологии управления правами AD RMS для защиты документов	8
Безопасность систем электронной почты	24
Дисциплины по теме «Управление информационной безопасностью» (не менее, час.)	**40**
Управление рисками (Risk Management)	16
Управление информационной безопасностью (InfoSecurity Governance)	16
Система управления инцидентами как основа обеспечения ИБ организации	24
Управление рисками безопасности информационных систем организаций	16
Расследование компьютерных инцидентов	32
Аудит ИБ на соответствие стандартам	32

2.3 Календарный учебный график

На освоение Программы Слушателю отводится 1 календарный год с даты зачисления в Учебный центр.

Обучение по Программе может осуществляться как единовременно (непрерывно), так и поэтапно (дискретно во времени), в том числе посредством освоения отдельных учебных курсов (предметов, дисциплин, модулей), прохождения практик, посредством организации сетевого дистанционного взаимодействия (в порядке, определённом образовательной Программой, договором на обучение и индивидуальным план-графиком освоения программы).

Модули (дисциплины) Программы оформлены в виде отдельных курсов, обучаться на которых можно с разрывом по времени и в различной последовательности (в соответствии с индивидуальным графиком обучения и Расписанием занятий). Однако рекомендуется начинать обучение с модулей базового естественнонаучного и обязательного специального (профессионального) циклов.

Наименование дисциплины	Общ. дист. нагрузки,	Порядок прохождения дисциплин			
		Первая очередь	Вторая очередь	Третья очередь	Четвертая очередь
1	2	3	4	5	6
Естественнонаучный цикл	**146**				
Дискретная математика	48				
Теория вероятностей и математическая статистика	48				
Информационные технологии	50				
Профессиональный цикл	**360**				
Базовая (обязательная) часть	***200***				
Базовый курс по безопасности информационных технологий	52				
Безопасность компьютерных сетей	40				
Безопасность операционных систем	56				
Работа органа криптографической защиты	20				
Использование ЭП и ИОК (PKI)	32				
Вариативная (актуализируемая) часть (дисциплины на выбор обучающихся по направлениям специализации, не менее, час.)	160				
Дисциплины по теме «Криптографическая защита информации, PKI и электронная подпись» (не менее, час.)	24				
Дисциплины по теме «Администрирование средств защиты информации» (не менее, час.)	30				
Дисциплины по теме «Защита информации от утечек по техническим каналам» (не менее, час.)	24				
Дисциплины по теме «Защита персональных данных» (не менее, час.)	24				
Дисциплины по теме «Защищенный электронный документооборот» (не менее, час.)	8				
Дисциплины по теме «Управление информационной безопасностью» (не менее, час.)	40				

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1 Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Обучение по Программе осуществляется на основе договоров об образовании, заключаемых со слушателями и (или) с физическими или юридическими лицами, обязующимися оплатить обучение слушателей, зачисляемых на обучение.

Профессиональная переподготовка по настоящей Программе осуществляется на базе высшего и среднего профессионального образования. Лица, желающие освоить дополнительную профессиональную программу, должны иметь:

- имеющие среднее профессиональное и (или) высшее образование;
- получающие среднее профессиональное и (или) высшее образование, при условии, что они получат дипломы об первичном образовании в процессе обучения по программе.

Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования. Наличие указанного образования должно подтверждаться документом государственного или установленного образца. Желательно иметь стаж работы (не менее 1 года), связанной с процессами обеспечения информационной безопасности в компаниях или организациях, или связанного с внедрением/эксплуатацией информационных систем.

При зачислении обучающегося экспертной комиссией учебного центра на основе предоставленных документов осуществляется анализ и зачёт (перезачёт) дисциплин (курсов, модулей) естественнонаучного цикла и вариативной части профессионального цикла, освоенных слушателем в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, после чего для него формируется индивидуальный План-график изучения базовых дисциплин и дисциплин вариативной части Программы.

Формы обучения и конкретные сроки освоения Программы определяются с учётом исходного уровня основного образования (квалификации и компетенций) слушателя, набора выбранных им курсов вариативной части Программы, расписания проведения назначенных курсов в Учебном центре и указываются в договоре об образовании.

3.2 Трудоемкость обучения

Нормативная трудоемкость обучения по данной программе – не менее 512 часов, включая все виды очной, дистанционной и самостоятельной учебной работы слушателя.

3.3 Форма обучения

Переподготовка специалистов по данной Программе реализуется в форме обучения с частичным отрывом от работы.

Обучение по модулям (курсам, дисциплинам) Программы проводится в очной форме с отрывом от работы и/или с использованием дистанционных образовательных технологий в форме онлайн-вебинаров с частичным отрывом от работы.

Обучение по Программе осуществляется на основе модульного принципа построения её содержания и индивидуальных учебных планов слушателей по освоению дисциплин (курсов) Программы, с использованием различных форм обучения и образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Конкретная форма обучения устанавливается при зачислении слушателей на прохождение программы на этапе составления индивидуального плана-графика обучения.

Освоение программы может проводится как в очной, так и дистанционной форме. При этом, объем дистанционно изученных учебных курсов не может превышать 80% лекционного и 50% лабораторных и практических занятий (семинаров).

3.4 Режим занятий

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Учебные занятия организованы в одну смену.

Продолжительность академического часа соответствует нормативным требованиям (45 мин).

Время проведения очных занятий и онлайн-вебинаров проводятся по рабочим дням с 10:00 до 17:30 по московскому времени.

Доступ к учебным пособиям и стендам для дистанционного выполнения лабораторных работ предоставляется слушателям круглосуточно.

3.5 Материально-технические условия реализации программы

Аудиторные занятия по модулям (курсам, дисциплинам) Программы включают лекции с демонстрацией презентаций на экране, практические работы с конкретными аппаратно-программными и техническими средствами защиты, а также лабораторные практикумы в специально оборудованных лабораториях:

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
Лекционная аудитория	Лекции	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции
Лаборатория для изучения дисциплины по теме «Криптографическая защита информации, PKI и электронная подпись» (не менее, час.)	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 2 GBt Жесткий диск 500.0 Gb DVD-ROM
Дисциплины по теме «Администрирование средств защиты информации» (не менее, час.)	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Intel Core i7 3.6 ГГц Память 32 GBt Жесткий диск 500.0 Gb DVD-ROM
Дисциплины по теме «Защита персональных данных» (не менее, час.)	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции
Дисциплины по теме «Защищенный электронный документооборот» (не менее, час.)	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 2 GBt Жесткий диск 500.0 Gb DVD-ROM
Дисциплины по теме «Управление информационной безопасностью» (не менее, час.)	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Intel Core i7 3.6 ГГц Память 32 GBt Жесткий диск 500.0 Gb DVD-ROM
Класс для изучения дисциплин по теме защиты информации от утечки по техническим каналам	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 2 GBt Жесткий диск 500.0 Gb На класс:

		Оборудование для защиты от утечки по техническим каналам а) Слаботочным линиям: • Программируемое устройство защиты телефонных линий «КИПАРИС»; • Устройство защиты абонентских телефонных линий «Октава – 10Т»; • Многофункциональный модуль защиты телефонных линий «SEL – 17/D»; • Прибор защиты телефонной линии формирующий синфазную и дифференциальную шумовую помеху «SI - 2060». б) Сотовым телефонам: • Блокиратор сотовой связи «Октава – БС», • Интеллектуальный блокиратор сотовой связи «RS Jammini»; • Интеллектуальный блокиратор сотовой связи «Имбирь»; • Автоматизитрованный блокиратор сотовой связи ST 202 «UDAV»; • Акустические сейфы для сотовых телефонов «Кокон», «Ладья»; • Акустический сейф с селекцией угроз «Свирель». г) Акустическим и виброакустическим каналам: • Виброакустический стационарный генератор «SI - 3002»; • Виброакустический стационарный генератор «Барон» • Адаптивный генератор виброакустической помехи «Кедр»; • Генераторы виброакустического зашумления SEL SP – 55, «Октава-ВА», «Соната-АВ»; • Акустический маскиратор конфиденциальных переговоров в помещении «Букет»; • Акустические маскираторы конфиденциальных переговоров в помещении «Шаман», «Бубен». д) Пространственным каналам ПЭМИН: • Система для защиты от утечки информации по каналам ПЭМИН «Гром – ЗИ-4А» с дискоконусной антенной SI -5002.1; • Генератор пространственного зашумления

		SEL SP - 21 «Баррикада»; • Генератор пространственного зашумления SEL SP – 22 «Блокада»; • Устройство комбинированной защиты «Соната –РС1» е) Каналам ПЭМИН по электросети: • Фильтры «Фаза-1-10», «ФСП-1Ф-7А», ЛФС-10-1Ф», «ЛФС-40-1Ф», «ФСПК-10»; • Генератор зашумления электросети «SEL SP-41/С»; • Генератор зашумления электросети Гром-ЗИ-4А; • Широкополосный генератор помех для электросети «Октава -С»; • Генератор зашумления электросети «Соната – Р2».

3.6 Учебно-методическое обеспечение программы

Каждый обучающийся (слушатель) перед началом занятий по каждой изучаемой им дисциплине (модулю, курсу) Программы обучения получает в постоянное пользование:

- оригинальное учебное пособие (руководство слушателя курса в печатном виде и возможность удалённого и локального доступа к его электронному варианту);
- справочные и вспомогательные материалы по изучаемым вопросам, а именно
  - ссылки на и тексты основных нормативных актов и методических документов ФСТЭК и ФСБ России,
  - типовые организационно-распорядительные документы,
  - документация по рассматриваемым аппаратно-программным средствам защиты,
  - инструкции и описания приборов,
  - подборки профильных статей из периодических изданий в электронном виде
  - перечни и ссылки на издания профильной литературу;

  доступны слушателю в системе дистанционного обучения.

Обеспеченность слушателей Центра учебной литературой – 100%.

В автоматизированном режиме производится книговыдача литературы на всех абонементах слушателей.

Приобретение обязательной учебной литературы происходит по заявкам кафедр в соответствии с учебными планами.

В качестве рекомендованной литературы и литературы, используемой для составления пособий Программы используются:

1. «Конституция Российской Федерации», принята всенародным голосованием 12 декабря 1993г.
2. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1.
3. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом РФ 9 сентября 2000г. №Пр-1895.

Кодексы:

4. «Уголовный кодекс Российской Федерации», принят Федеральным законом от 13 июня 1996г. № 63-ФЗ.
5. «Кодекс Российской Федерации об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195-ФЗ.
6. «Гражданский кодекс Российской Федерации (часть первая)», принят Федеральным законом от 30 ноября 1994г. №51-ФЗ.
7. «Гражданский кодекс Российской Федерации (часть вторая)», принят Федеральным законом от 26 января 1996г. №14-ФЗ.
8. «Гражданский кодекс Российской Федерации (часть третья)», принят Федеральным законом от 26 ноября 2001г. №146-ФЗ.
9. «Гражданский кодекс Российской Федерации (часть четвертая)», принят Федеральным законом от 18 декабря 2006г. №230-ФЗ.
10. «Трудовой кодекс Российской Федерации», принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.
11. «Воздушный кодекс Российской Федерации» принят Федеральным законом от 19 марта 1997г. № 60-ФЗ. Статья 85.1. Персональные данные пассажиров воздушных судов.

Федеральные законы:

12. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
13. Федеральный Закон от 11 июля 2011г. № 200-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального Закона «Об информации, информационных технологиях и о защите информации».
14. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
15. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
16. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».
17. Федеральный закон от 2 декабря 1990г. № 395-1 «О банках и банковской деятельности».
18. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

19. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».
20. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».
21. Закон Российской Федерации от 21 июля 1993г. № 5485-1 «О государственной тайне».
22. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».
23. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».
24. Федеральный закон от 7 июля 2003г. № 126-ФЗ «О связи».
25. Федеральный закон от 27 июля 2004г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».
26. Федеральный закон от 2 марта 2007г. № 25-ФЗ «О муниципальной службе в Российской Федерации». Статья 29. Персональные данные муниципального служащего.

Указы Президента Российской Федерации:

27. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
28. Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента Российской Федерации от 23 сентября 2005г. № 1111).
29. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
30. Указ Президента Российской Федерации от 3 апреля 1995г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (в ред. Указа Президента Российской Федерации от 25 июля 2000г. №1358)».
31. Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
32. Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

Постановления Правительства Российской Федерации:

33. Постановление Правительства РСФСР от 5 декабря 1991г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».
34. Постановление Правительства Российской Федерации от 16 марта 2009г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
35. Постановление Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
36. Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

37. Постановление Правительства Российской Федерации от 6 июля 2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
38. Постановление Правительства Российской Федерации от 4 марта 2010г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».
39. Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313 «Об утверждении Положения о лицензирования 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)».
40. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 «о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
41. Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
42. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).
43. Постановление Правительства Российской Федерации от 18 мая 2009г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».
44. Постановление Правительства Российской Федерации от 26 июня 1995г. № 608 «О сертификации средств защиты информации».
45. Постановление Правительства Российской Федерации от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования

(включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

46. Постановление Правительства Российской Федерации от 3 ноября 1994г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
47. Постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Нормативные документы ФСТЭК России:

48. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.
49. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.
50. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.
51. «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.
52. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995г. № 199.
53. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002г. № 282.
54. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.
55. «Сборник временных методик оценки защищённости конфиденциальной информации, обрабатываемой техническими средствами и системами», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 2001г.
56. «Сборник руководящих документов по защите информации от НСД», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 1998г.

57. «Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены Заместителем директора ФСТЭК России 18 мая 2007г. и 19 ноября 2007г.
58. «Методические документы по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.
59. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
60. «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
61. «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 г.
62. «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 г.
63. «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 1992г.
64. «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 1997г.
65. «Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.
66. «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 1999г. № 114.
67. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1, Часть 2, Часть3», утвержден приказом председателя Гостехкомиссии России от 19 июня 2002г. №187.
68. «Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.
69. «Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты», Гостехкомиссия России, 2003г.
70. «Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты», Гостехкомиссия России, 2003г.

71. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.
72. «Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам», утвержден первым заместителем председателя Гостехкомиссии России 8 ноября 2001г.
73. «Общие требования по обеспечению безопасности информации в ключевых системах инфорёёмационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.
74. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007г.
75. Приказ ФСТЭК России № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
76. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Нормативные документы ФСБ России:

77. «Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008г. № 149/54-144.
78. «Об утверждении типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008 г. N 149/6/6-622.
79. Приказ ФСБ Российской Федерации от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
80. Приказ ФАПСИ Российской Федерации от 13 июня 2001г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

Стандарты:

81. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
82. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»

83. ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 814-ст)
84. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. ... Часть 2. Функциональные компоненты безопасности.
85. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
86. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
87. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита bнформации. Процессы формирования ипроверки электронной цифровой подписи»
88. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования»
89. ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения».
90. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
91. BS 7799 1. «Управление информационной безопасностью. Общие требования к управлению информационной безопасностью».
92. BS 7799 2. «Управление информационной безопасности. Требования и руководство по применению».
93. BS 7799 3. «Управление информационной безопасности. Руководство по управлению рисками информационной безопасности».
94. ISO/IEC 27001:2005. «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».2012 г.
95. ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью». 2013 г.
96. ISO/IEC 27006:2007 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью».

Учебные пособия.

97. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006, 400 с.
98. Безопасность информационных технологий. Руководство слушателя курса БТ01. - М.: УЦ Информзащита, 2012. – 308 с.
99. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.- М.: УЦ Информзащита, 2012. – 367 с.
100. Основы TCP/IP. Руководство слушателя курса БТ05. - М.: УЦ Информзащита, 2012. – 108 с.
101. Безопасность ОС Windows 2000/XP/2003. Руководство слушателя курса БТ26. - М.:

УЦ Информзащита, 2012. - 558 с.

102. Руководство слушателя курса Т005. - М.: УЦ Информзащита, 2012. – 245 с.
103. Порядок применения системы защиты Secret Net 5.0 (автономный вариант). Руководство слушателя курса Т005АВ.- М.: УЦ Информзащита, 2012.–138 с.
104. Порядок внедрения и применения системы КУБ. Руководство слушателя курса Т008. - М.: УЦ Информзащита, 2012. – 276 с.
105. Реализация режима коммерческой тайны на предприятии. Руководство слушателя курса КП30. - М.: УЦ Информзащита, 2012. – 85 с.
106. Организация конфиденциального делопроизводства. Руководство слушателя курса КП31. - М.: УЦ Информзащита, 2012. – 218 с.
107. Защита персональных данных. Руководство слушателя курса КП32. - М.: УЦ Информзащита, 2012. – 94 с.

Статьи.

108. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа / Станскова У.М. // Трудовое право в России и за рубежом. – 2011. - № 2.
109. Экспертный анализ методов защиты информации от утечки по техническим каналам / Волков П.П. // Эксперт-криминалист. – 2009.- № 4.
110. О правовой защите компьютерной информации / Воротников В.Л. // Администратор суда. – 2009. - № 2.
111. Актуальные вопросы охраны коммерческой тайны в отношениях с органами государства / Забегайло Л.А., Назарова И.А. // Современное право. – 2011. - № 7.
112. Административная ответственность как средство обеспечения информационной безопасности / Савчишкин Д.Б. // Административное и муниципальное право. – 2011. - № 6.
113. Электронное государственное управление как новая форма взаимоотношений личности, общества и государства / Чеботарева А.А. // Государственная власть и местное самоуправление. – 2011. - № 6.
114. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации / Маркарьян Р.В. // Международное публичное и частное право. – 2011. - № 4.
115. Организация работы с персональными данными / Кузнецова Т.В. // Трудовое право. – 2011. - № 5.
116. О соблюдении баланса интересов при установлении мер защиты персональных данных / Терещенко Л.К. // Журнал российского права. – 2011. - №5.
117. Способы совершения преступлений в сфере компьютерной информации / Будаковский Д.С. // Российский следователь. – 2011. - №4.
118. Киберпреступность: проблемы квалификации преступных деяний / Воронцова С.В. // Российская юстиция. – 2011. - №2.
119. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации / Загузов Г.В. // Административное и муниципальное право. – 2010. - №5.
120. Конфиденциальная информация и институт персональных данных в банковской деятельности / Палехова Е.А. // Предпринимательское право. – 2010. - №3.

Документы RFC и другие ссылки
121. Internet Security Glossary, Version 2 (http://www.ietf.org/rfc/rfc4949.txt)
122. Benchmarking Terminology for Firewall Performance (http://www.ietf.org/rfc/rfc2647.txt)
123. Behavior of and Requirements for Internet Firewalls (http://www.ietf.org/rfc/rfc2979.txt)
124. http://aluigi.altervista.org/adv/termdd_1-adv.txt

3.7 Требования к кадровым условиям реализации программы

Реализация программы обеспечивается штатными преподавателями Учебного центра «Информзащита», а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора из числа специалистов, имеющих опыт практической работы в различных областях обеспечения информационной безопасности, включая проектирование, разработку, эксплуатацию и оценку средств и систем защиты информации. Для проведения занятий по дисциплинам естественнонаучного цикла могут привлекаться преподаватели ведущих вузов страны (на основе договоров).

По состоянию на 1 сентября 2014 г. на постоянной основе (в штате) в Учебном центре работают 17 преподавателей. Преподаватели имеют высшее образование, необходимые сертификации для проведения обучения, ученые степени и звания, регулярно повышают квалификацию, как в России, так и за рубежом.

Все преподаватели занимаются исследовательской деятельностью в области информационной безопасности, результаты которой используются при создании учебных курсов. Среди преподавателей имеющие ученые степени и сертифицированные различными организациями-производителями средств защиты.

Преподаватели Центра являются специалистами-практиками и занимаются исследовательской деятельностью по актуальным проблемам обеспечения безопасности на базе 5-ти кафедр Центра. Результаты исследовательской деятельности и практического опыта специалистов ложатся в основу авторских курсов.

Кафедры Центра:

- **Кафедра безопасности электронных коммуникаций**
  Кафедра существует с 2005 года. При активном участии сотрудников этой кафедры были созданы курсы по обеспечению безопасности электронных коммуникаций, практические курсы по использованию ЭЦП и PKI, деятельности удостоверяющих центров и другие авторские курсы Учебного центра.

- **Кафедра сетевой безопасности**
  С момента основания лаборатории в 2003 году (с 2014 г. Кафедра) результаты

исследовательской деятельности Кафедры используются при создании и обновлении популярных среди заказчиков Учебного центра курсов, посвященных безопасности компьютерных сетей. Аналитические отчеты, выпускаемые Кафедрой, регулярно публикуются в СМИ, как независимые, и пользуются заслуженным авторитетом среди специалистов.

- **Кафедра противодействия мошенничеству и расследования инцидентов**
  В 2005 году в Центре была открыта Лаборатория (с 2014 г. Кафедра) противодействия мошенничеству и расследования инцидентов, специалисты которой неоднократно приглашались в качестве экспертов для проведения судебных экспертиз по гражданским и уголовным делам. Специалистами Кафедры были созданы и проводятся на регулярной основе учебные курсы «Расследование компьютерных инцидентов» и «Предотвращение мошенничества на сетях связи».

- **Кафедра защиты информации от утечки по техническим каналам**
  В 2006 году в Учебном центре была создана Лаборатория (с 2014 г. Кафедра) по защите информации от утечки по техническим каналам. Силами Кафедры были разработаны учебные курсы по проблеме защиты конфиденциальной информации от утечки по техническим каналам, практический курс по защите конфиденциальной информации от закладочных устройств. Специалисты Кафедры являются авторами нескольких изданий учебных пособий по данной тематике для профильных вузов.

- **Кафедра обеспечения экономической безопасности**
  Руководит Кафедрой специалист имеющий большой опыт работы в системе МВД России по расследованию преступлений в сфере информационных технологий. Специалисты Кафедры – отставные сотрудники систем МВД РФ, ФСНП РФ и т.п., владеют практическими навыками оперативной работы и обладают теоретическими и практическими знаниями по экономике и менеджменту.

  Специалисты Кафедры являются авторами учебных пособий, статей по тематике «экономическая безопасность» в ряде профильных изданий.

Наличие в УЦ руководящих, педагогических работников и учебно-вспомогательного персонала, имеющих необходимый уровень подготовки, позволяет использовать дистанционные образовательные технологии (ДОТ) при проведении части занятий по дисциплинам (курсам) Программы.

4 ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ (ФОРМЫ АТТЕСТАЦИИ, ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ)

Оценка качества освоения программы включает текущую, промежуточную и итоговую аттестацию обучающихся.

Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования (уровень образования специалистов, проходящих профессиональную переподготовку, должен быть не ниже уровня образования, требуемого для нового вида профессиональной деятельности).

При зачислении обучающегося экспертной комиссией учебного центра на основе предоставленных документов осуществляется анализ и зачёт (перезачёт) дисциплин (курсов, модулей) естественнонаучного цикла и вариативной части профессионального цикла, освоенных слушателем в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, после чего для него формируется индивидуальный План-график изучения базовых дисциплин и дисциплин вариативной части Программы.

Помимо документов о высшем или среднем профессиональном образовании к рассмотрению принимаются государственные документы и документы установленного образца о краткосрочном повышении квалификации по направлению информационной безопасности и защите информации, а так же сертификаты и свидетельства о прохождении учебных дисциплин (модулей, курсов) как естественнонаучного цикла, так и вариативной части профессионального цикла, изученных обучаемыми ранее (или изучаемых параллельно) в ходе освоения ими основных образовательных программ профессионального образования в Учебном центре «Информзащита» или иных образовательных учреждениях (выданные не ранее 5 лет с даты зачисления Слушателя в Учебный центр «Информзащита»).

Прохождение каждого курса/модуля/дисциплины Программы завершается зачетом. Зачет принимает преподаватель Учебного центра при предъявлении Слушателем документа, удостоверяющего личность. Зачет может проводиться в форме собеседования или в форме теста, который подразумевает:

- ответы на контрольные вопросы (обязательно);
- выполнение контрольных задач и заданий (опционально);
- выполнение контрольных лабораторных работ (опционально);
- собеседование с представителями работодателя (опционально).

Тестирование при помощи контрольных вопросов, контрольных задач и заданий

может быть организованно в:

- устной форме;
- бумажной форме;
- с использованием электронных методов тестирования.

Для каждого теста разрабатывается система оценки, параметрами которой являются количество вопросов, их сложность, полнота ответа на вопрос. По результатам ответа на вопрос испытуемому присваивается определенное системой оценки количество баллов. Итоговое решение о прохождении теста принимается на основании превышения суммарно набранного количества баллов по всем вопросам над определенным системой оценки пороговым значением.

При использовании средств электронного тестирования, зачет может содержать от 10 до 40 вопросов 3-х уровней сложности. К вопросам предлагаются по три или четыре варианта ответов, сформулированных по принципам:

- Выбора
  - правильный
  - похожий на правильный, но имеющий неточность;
  - совершенно неправильный
  - относящийся к смежной предметной области
- Перечисления, когда из набора правильных и неправильных ответов необходимо выбрать наиболее полный правильный вариант.

Выполнение лабораторных работ производится на компьютерных стендах, воссоздающих или эмулирующих реальные объекты информационных систем, или с реальными приборами/установками/системами. Выполнение работ может проводится как под контролем преподавателя, так и самостоятельно.

Результаты зачета вносятся преподавателем в зачетную ведомость Слушателя. В случае неуспешной попытки, Слушатель вправе запросить время на самоподготовку и углубленное изучение дисциплины и пересдать зачет в любое согласованное с Учебным центром время.

Освоение дополнительной профессиональной образовательной Программы переподготовки завершается обязательной итоговой аттестацией обучающихся в форме зачёта. Итоговая аттестация Слушателей проводится в форме тестирования (возможно в электронном виде) по основным темам изученных базовых дисциплин профессионального цикла и заключительного собеседования с членами аттестационной комиссии. К собеседованию допускаются только успешно прошедшие тестирование Слушатели.

Итоговый аттестационный тест содержит 45 вопросов, выбираемых случайным образом из пула в 120 вопросов. На прохождение теста отводится полтора часа. Проходной бал 2/3 (30) правильных ответов. Допускается использование в Итоговой аттестации вопросов из зачетных материалов к составляющим Программу курсам/модулям/дисциплинам. В случае неуспешной попытки сдачи итогового теста, Слушателю предоставляется время на самоподготовку и возможность повторно пройти тестирование. По результатам успешного тестирования и собеседования по каждому Слушателю оформляется отдельное решение о прохождении (не прохождении) итоговой аттестации.

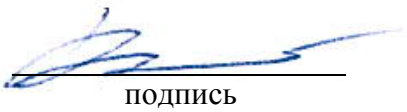
Считается, что обучающийся освоил Программу переподготовки, если он успешно завершил обучение по всем модулям (дисциплинам, курсам) циклов Программы в соответствии со своим индивидуальным учебным планом (План-графиком) в объеме не менее 512 часов с обязательным прохождением базовой части (базовых специальных модулей) профессионального цикла Программы и прошёл итоговую аттестацию.

Слушателям, успешно освоившим Программу, выполнившим все требования учебного плана и прошедшим итоговую аттестацию, по решению аттестационной комиссии (состав которой утверждается руководителем образовательного учреждения) выдаются дипломы о профессиональной переподготовке по направлению «Информационная безопасность», которые удостоверяют право (соответствие квалификации) специалистов заниматься профессиональной деятельностью в сфере «Информационной безопасности».

Слушателям, не прошедшим итоговой аттестации или показавшим на итоговой аттестации неудовлетворительные результаты, а также слушателям, освоившим лишь часть Программы и/или отчисленным из организации, выдается справка об обучении.

При освоении Программы слушателем параллельно с получением среднего профессионального образования и (или) высшего образования диплом о профессиональной переподготовке выдаётся ему после получения соответствующего документа об основном образовании и о квалификации.

5 СОСТАВИТЕЛИ ПРОГРАММЫ

ФИО	Должность	Иное	
ЕРШОВ Дмитрий Вячеславович	Заместитель директора по учебно-методической работе АНО ДПО «Учебный центр Информзащита»	Кандидат технических наук	 подпись
Бондарев Валерий Васильевич	Преподаватель АНО ДПО «Учебный центр Информзащита»	Кандидат военных наук, доцент, профессор Академии военных наук	 подпись
Собецкий Игорь Всеволодович	Заведующий кафедры АНО ДПО «Учебный центр Информзащита»		 подпись
Бузов Геннадий Алексеевич	Заведующий кафедры АНО ДПО «Учебный центр Информзащита»	Кандидат военных наук, старший научный сотрудник, доцент, академик Академии проблем безопасности, обороны и правопорядка	 подпись