Негосударственное образовательное учреждение
дополнительного профессионального образования
«Институт информационных технологий «АйТи»

УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»

И.О. Морозов

«21» октября 2015 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

по направлению «Информационная безопасность»

«Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа»

Виды профессиональной деятельности:
организационно-управленческая, эксплуатационная

Трудоёмкость обучения: 72 часа

Москва
2015

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Общие положения

Настоящая программа повышения квалификации «Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа» (далее – программа повышения квалификации) разработана на основании Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», приказа Минобрнауки России от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» и Приказа Минобрнауки России от 09 января 2014 г. № 2 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Программа повышения квалификации полностью соответствует требованиям «Положения о лицензировании деятельности по технической защите конфиденциальной информации», утвержденного Постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.

Программа повышения квалификации реализуется в Негосударственном образовательном учреждении дополнительного профессионального образования «Институт информационных технологий «АйТи» (далее - НОУДПО «Институт «АйТи»).

Программа повышения квалификации разработана в инициативном порядке.

1.2. Цель реализации программы

Целью реализации программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации, необходимой для профессиональной деятельности в области обеспечения информационной безопасности.

Программа является преемственной к основным образовательным программам высшего образования по:

- направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность автоматизированных систем» квалификация (степень) – бакалавр;
- специальности 10.05.03 «Информационная безопасность автоматизированных систем», квалификация – специалист по защите информации.

1.3. Категории обучающихся

Специалисты органов государственной власти, местного самоуправления, учреждений и организаций различных форм собственности, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу информации ограниченного доступа не содержащую сведений составляющих государственную тайну.

1.4. Характеристика нового вида профессиональной деятельности, новой квалификации

а) Область профессиональной деятельности слушателя, прошедшего обучение по программе повышения квалификации для выполнения нового вида профессиональной деятельности в области информационной безопасности, включает совокупность проблем, связанных с обеспечением защищённости объектов информатизации, в том числе, информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

б) Объектами профессиональной деятельности являются:

– объекты информатизации, в том числе автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

в) Слушатель, успешно освоивший программу повышения квалификации, должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

эксплуатационная деятельность:

– установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности автоматизированных систем и иных объектов информатизации, с учетом установленных требований;

– участие в обследовании автоматизированных систем и иных объектов информатизации, их категорировании, классификации, определении требуемых уровней защищённости и аттестации по требованиям безопасности информации;

– администрирование систем информационной безопасности объектов;

– выполнение работ по защите информации.

организационно-управленческая деятельность:

– осуществление организационно-правового обеспечения информационной безопасности объектов защиты;

– организация работы малых коллективов исполнителей с учетом требований защиты информации;

– управление информационной безопасностью автоматизированных систем;

– контроль эффективности реализации политик информационной безопасности, реализованных в автоматизированных системах и иных объектах информатизации;

– участие в определении потребности в средствах защиты информации, контроль их поставки и правильной эксплуатации;

– разработка проектов нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов.

1.5. Планируемые результаты обучения

Слушатель в результате освоения программы должен обладать следующими профессиональными компетенциями (ПК):

в части эксплуатационной деятельности:

– способностью принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации (ПК-1);

– способностью администрировать подсистемы информационной безопасности различных объектов информатизации (ПК-2);

– способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-3);

– способностью принимать участие в организации контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-4).

в части организационно-управленческой деятельности:

– способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-5);

– способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры автоматизированных систем, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-6);

– способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области защиты информации (ПК-7);

– способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-8);

– способностью разрабатывать проекты нормативных и методических документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-9);

– способностью организовать и сопровождать аттестацию объектов информатизации по требованиям безопасности информации (ПК-10).

Слушатель в результате освоения программы будет способен выполнять следующие должностные обязанности, приведённые в «Квалификационном справочнике должностей руководителей, специалистов и других служащих», утверждённом Постановлением Министерством труда и социальной защиты Российской Федерации от 21 августа 1998 г. № 37 (в редакции Приказа Минтруда России от 12 февраля 2014 № 96).

Главный специалист по защите информации.

Руководит выполнением работ по комплексной защите информации в отрасли, на предприятии, в учреждении, организации, обеспечивая эффективное применение всех имеющихся организационных и инженерно-технических мер в целях защиты сведений, составляющих государственную тайну. Участвует в разработке технической политики и определении перспектив развития технических средств контроля, организует разработку и внедрение новых технических и программно-математических средств защиты, исключающих или существенно затрудняющих несанкционированный доступ к служебной информации, составляющей государственную или коммерческую тайну. Участвует в рассмотрении технических заданий на проекты изделий, научно-исследовательские и опытно-конструкторские работы, подлежащие защите, осуществляет контроль за включением в них требований нормативно-технических и методических документов по защите информации и выполнением этих требований. Готовит предложения для включения в планы и программы работ организационных и инженерно-технических мер по защите информационных систем. Участвует в работе по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации. Организует проведение научно-исследовательских работ в области совершенствования систем защиты информации и повышения их эффективности. Выполняет весь комплекс (в том числе особо сложных) работ, связанных с контролем и защитой информации, на основе разработанных программ и методик. Организует сбор и анализ материалов о возможных каналах утечки ин-

формации, в том числе по техническим каналам, при проведении исследований и разработок, связанных с созданием и производством специальных изделий (продукции), необходимых для проведения работ по обеспечению защиты информации. Обеспечивает координацию проводимых организационно-технических мероприятий, разработку методических и нормативных материалов и оказание необходимой методической помощи в проведении работ по защите информации, оценке технико-экономической эффективности предлагаемых и реализуемых организационно-технических решений. Организует работу по сбору и систематизации необходимой информации об объектах, подлежащих защите, и охраняемых сведениях, осуществляет методическое руководство и контроль за работой по оценке технико-экономического уровня и эффективности разрабатываемых мер по защите информации. Возглавляет работу по обобщению данных о потребности в технических и программно-математических средствах защиты информации, аппаратуре контроля, составлению заявок на изготовление этих средств, организует их получение и распределение между объектами защиты. Содействует распространению передового опыта и внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения ее эффективности. Обеспечивает контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации. Координирует деятельность подразделений и специалистов по защите информации в отрасли, на предприятии, в учреждении, организации.

Начальник отдела (лаборатории, сектора) по защите информации.

Организует разработку и внедрение организационных и технических мероприятий по комплексной защите информации на предприятиях, ведущих работы, содержание которых составляет государственную или коммерческую тайну, обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации. Возглавляет разработку проектов перспективных и текущих планов работы, составление отчетов об их выполнении. Руководит проведением работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработкой технических средств контроля, определяет перспективы их развития. Обеспечивает взаимодействие и необходимую кооперацию соисполнителей работ по вопросам организации и проведения научно-исследовательских и опытно-конструкторских разработок, организует и контролирует выполнение плановых заданий, договорных обязательств, а также сроки, полноту и качество работ, выполняемых соисполнителями. Организует работу по заключению договоров на работы по защите информации, принимает меры по обеспечению финансирования работ, в том числе выполняемых по договорам. Обеспечивает участие подразделения в разработке технических заданий на выполняемые на предприятии исследования и разработки, формулирует цели и задачи работы по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации. Организует проведение специальных исследований и контрольных проверок по выявлению демаскирующих признаков и возможных каналов утечки информации, в том числе по техническим каналам, разрабатывает меры по их устранению и предотвращению, а также работу по составлению актов и другой технической документации о степени защищенности технических средств и помещений. Контролирует соблюдение нормативных требований по надежной защите информации, обеспечивает комплексное использование технических средств, методов и организационных мероприятий. Организует рассмотрение применяемых и предлагаемых методов защиты информации, промежуточных и конечных результатов исследований и разработок. Совершенствует планирование, контроль и организацию выполнения работ, обеспечивает использование в них достижений отечественной и зарубежной науки и техники, передового опыта. Обеспечивает выполнение плановых заданий с наименьшими затратами матери-

альных и финансовых ресурсов, рациональное расходование фонда заработной платы. Согласовывает проектную и другую техническую документацию на вновь строящиеся и реконструируемые здания и сооружения в части выполнения требований по защите информации. Определяет потребность подразделения в оборудовании, материальных, финансовых и других ресурсах, необходимых для проведения работ, и контролирует рациональное использование и сохранность аппаратуры, приборов и другого оборудования. Обеспечивает высокий научно-технический уровень работ, эффективность и качество исследований и разработок. Осуществляет контроль за выполнением предусмотренных мероприятий, анализ материалов контроля, выявление нарушений, разрабатывает и участвует в реализации мер по устранению выявленных недостатков по защите информации. Организует проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности, обеспечивает представление в установленном порядке действующей отчетности. Участвует в подборе кадров, оценке деятельности и аттестации работников подразделения. Определяет направления деятельности подразделений, входящих в состав отдела, организует и координирует их работу. Осуществляет рациональную расстановку кадров с учетом квалификации и деловых качеств работников, принимает меры по повышению их квалификации и творческой активности. Обеспечивает ведение делопроизводства в соответствии с установленным порядком, соблюдение действующих инструкций по режиму работ и своевременно принимает меры по предупреждению нарушений. Следит за безопасным проведением работ, соблюдением правил и норм охраны труда. Руководит работниками подразделения.

Инженер по защите информации.

Выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем, проводит исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации. Участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации. Составляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами. Проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации. Осуществляет разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов. Составляет информационные обзоры по технической защите информации. Выполняет оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвует в проведении проверок учреждений, организаций и предприятий по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию. Готовит предложения по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации, составляет заявки на необходимые материалы, оборудование, приборы. Участвует в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим

классам безопасности. Проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер. Изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны. Выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ.

Специалист по защите информации.

Выполняет сложные работы, связанные с обеспечением комплексной защиты информации на основе разработанных программ и методик, соблюдения государственной тайны. Проводит сбор и анализ материалов учреждений, организаций и предприятий отрасли с целью выработки, и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну. Анализирует существующие методы и средства, применяемые для контроля и защиты информации, и разрабатывает предложения по их совершенствованию и повышению эффективности этой защиты. Участвует в обследовании объектов защиты, их аттестации и категорировании. Разрабатывает и подготавливает к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. Организует разработку и своевременное представление предложений для включения в соответствующие разделы перспективных и текущих планов работ и программ мер по контролю и защите информации. Дает отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений и другие разработки по вопросам обеспечения защиты информации. Участвует в рассмотрении технических заданий на выполнение эскизных, технических и рабочих проектов, обеспечивает их соответствие действующим нормативным и методическим документам, а также в разработке новых принципиальных схем аппаратуры контроля, средств автоматизации контроля, моделей и систем защиты информации, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений. Определяет потребность в технических средствах защиты и контроля, составляет заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролирует их поставку и использование. Осуществляет проверку выполнения требований межотраслевых и отраслевых нормативных документов по защите информации.

Слушатель, освоивший программу повышения квалификации, должен

знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России, (документы ведомства-заказчика программы) 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 за-

щиты 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.

уметь:

– 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;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

владеть:

– профессиональной терминологией;

– навыками применения средств антивирусной защиты;

– навыками организации и обеспечения режима защиты информации;

– навыками эксплуатации технических средств по оценке защищённости информации;

– методами технической защиты информации;

– методами организации и управления деятельностью;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

1.6. Трудоёмкость программы

Нормативная трудоемкость обучения по данной программе – 72 часа, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.7. Форма и сроки обучения

Обучение по программе повышения квалификации осуществляется в очной форме. Срок обучения составляет: 9 дней;

1.8. Режим занятий

Режим занятий составляет не более 8 академических часов в день, с перерывом на обед – не менее 45 минут.

Для всех аудиторных занятий академический час устанавливается продолжительностью 45 минут.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	Зачёт
			Лекции	Практические занятия	Семинары		
1.	**Раздел № 1. Общие вопросы технической защиты информации ограниченного доступа.**	**16**	**6**	**5**	**2**	**3**	**0**
2.	**Тема № 1.** Основные термины и определения в области технической защиты информации ограниченного доступа.	4	2	1	0	1	0
3.	**Тема № 2.** Нормативные правовые акты по технической защите информации ограниченного доступа.	4	2	1	0	1	0
4.	**Тема № 3.** Организационно-распорядительные документы по технической защите информации ограниченного доступа.	2	0	0	1	1	0
5.	**Тема № 4.** Нормативные и методические документы по технической защите информации ограниченного доступа.	4	1	3	0	0	0

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	За чёт
			Лекции	Практические занятия	Семинары		
6.	**Тема № 5.** Сравнительный анализ международных и национальных стандартов в области защиты информации.	2	1	0	1	0	0
7.	**Раздел № 2. Защита информации от утечки по техническим каналам.**	**16**	**5**	**9**	**2**	**0**	**0**
8.	**Тема № 6.** Угрозы утечки информации по техническим каналам.	6	2	2	2	0	0
9.	**Тема № 7.** Методы, способы и средства защиты информации от утечки по техническим каналам.	6	2	4	0	0	0
10.	**Тема № 8.** Методы, способы и средства оценки защищённости информации от утечки по техническим каналам.	4	1	3	0	0	0
11.	**Раздел № 3. Защита информации от несанкционированного доступа (НСД).**	**24**	**6**	**16**	**2**	**0**	**0**
12.	**Тема № 9.** Угрозы несанкционированного доступа к информации.	8	2	4	2	0	0
13.	**Тема № 10.** Методы, способы и средства защиты информации от несанкционированного доступа.	12	3	9	0	0	0
14.	**Тема № 11.** Методы, способы и средства оценки защищённости от несанкционированного доступа к информации.	4	1	3	0	0	0
15.	**Раздел № 4. Организация и обеспечение работ по технической защите информации ограниченного доступа.**	**12**	**4**	**7**	**0**	**1**	**0**

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	Зачёт
			Лекции	Практические занятия	Семинары		
16.	**Тема № 12.** Общие вопросы организации работ по технической защите информации ограниченного доступа.	4	1	2	0	1	0
17.	**Тема № 13.** Подготовка объектов информатизации к аттестации по требованиям безопасности информации.	4	1	3	0	0	0
18.	**Тема № 14.** Сертификация средств защиты информации и аттестация объектов информатизации.	2	1	1	0	0	0
19.	**Тема № 15.** Лицензирование деятельности по технической защите конфиденциальной информации.	2	1	1	0	0	0
20.	**Итоговый контроль**	**4**	**0**	**0**	**0**	**0**	**4**
21.	**Всего**	**72**	**21**	**35**	**4**	**8**	**4**

2.2. Рабочие программы дисциплин (модулей)

РАЗДЕЛ ПЕРВЫЙ

ОБЩИЕ ВОПРОСЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Тема № 1. Основные термины и определения в области технической защиты информации ограниченного доступа.

Основные понятия, термины и определения в области технической защиты информации (ТЗИ), определяемые правовыми, нормативными и методическими документами Российской Федерации: «информация», «безопасность информации», «техническая защита конфиденциальной информации», «угрозы безопасности информации», «уязвимости», «источники угроз» и т.д. Целостность, конфиденциальность и доступность информации. Концептуальные основы ТЗИ.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-4, ПК-5, ПК-8.

Тема № 2. Нормативные правовые акты по технической защите информации ограниченного доступа.

Государственная система защиты информации в Российской Федерации. Система документов по ТЗИ и краткая характеристика ее основных составляющих. Законодатель-

ные и иные правовые акты, регулирующие вопросы ТЗИ. Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи и функции Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи и функции управлений ФСТЭК России по федеральным округам. Основные Федеральные законы Российской Федерации, указы и распоряжения Президента Российской Федерации и постановления Правительства Российской Федерации в области защиты информации.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-4, ПК-5, ПК-8, ПК-9.

Тема № 3. Организационно-распорядительные документы по технической защите информации ограниченного доступа.

Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Общий обзор положений ФСТЭК России, определяющих основные направления деятельности по технической защите информации ограниченного доступа.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-4, ПК-5, ПК-8, ПК-9.

Тема № 4. Нормативные и методические документы по технической защите информации ограниченного доступа.

Обзор нормативных и методических документов в области технической защиты информации. Основные ГОСТы и специальные нормативные документы. Руководящие документы: «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации», «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-4, ПК-5, ПК-8, ПК-9.

Тема № 5. Сравнительный анализ международных и национальных стандартов в области защиты информации.

Общий сравнительный анализ правовых, нормативных и методических документов Российской Федерации и международных стандартов в области защиты информации. История разработки и развития национальных стандартов Российской Федерации в области построения систем управления информационной безопасностью.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-4, ПК-5, ПК-8, ПК-9.

РАЗДЕЛ ВТОРОЙ

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Тема № 6. Угрозы утечки информации по техническим каналам.

Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации и в том числе защищаемых помещений. Классификация ТКУИ. Характеристики информационных сигналов, определяющие степень их опасности.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-4, ПК-5, ПК-7, ПК-9, ПК-10.

Тема № 7. Методы, способы и средства защиты информации от утечки по техническим каналам.

Общая характеристика методов и средств защиты информации от утечки по техническим каналам. Их назначение, реализуемые функции, состав. Фильтры частотные. Ограничители малых сигналов. Генераторы шума. Принципы их работы. Конструктивные решения. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору средств защиты информации по видам объектов обрабатывающих конфиденциальную информацию: каналы связи, помещения для ведения конфиденциальных переговоров, автоматизированные системы и т.д. Рекомендации по установке, настройке и эксплуатации.

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения видео-кинофильмов. Защита информации при проведении магнитной звукозаписи. Защита речевой информации при ее передаче по каналам связи.

Обзор средств активной защиты: акустика, виброакустика, системы виброакустического зашумления, средства защиты слаботочных линий, постановщики помех сотовым телефонам, диктофонам.

Обзор средств выявления демаскирующих признаков закладочных устройств. Средства радио контроля, поисковая техника, средства неразрушающего контроля, досмотровая техника, средства дозиметрии. Изучение универсальных поисковых приборов, средств контроля проводных коммуникаций, средств активной защиты, подавителей диктофонов, сотовых телефонов, постановщиков помех.

Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных.

Средства защиты от утечки по каналам ПЭМИН. Назначение. Обзор моделей. Технические характеристики, особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации. Генераторы шума. Диапазон. Размещение и выбор в зависимости от уровня опасного сигнала. Доработанные по специальным требованиям основные технические средства и системы. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.

Средства защиты сети питания. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Частотные фильтры. Особенности и принципы работы. Задерживающие и поглощающие. Построение системы электропитания и заземления. Линейное зашумление. Ограничители малых сигналов. Оценка эффективности. Линейные генераторы шума. Особенности применения. Оценка эффективности. Разнос, экранирова-

ние линий.

Устройства защиты телефонных линий. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

Тема № 8. Методы, способы и средства оценки защищённости информации от утечки по техническим каналам.

Методы и средства выявления ТКУИ на типовом объекте информатизации и в защищаемых помещениях. Содержание и порядок организации и проведения специальных исследований технических средств обработки информации. Оценка защищённости помещений от утечки речевой информации по акустическому, виброакустическому каналам и по каналу электроакустических преобразований во вспомогательных технических средствах и системах. Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-2, ПК-4, ПК-7, ПК-10.

РАЗДЕЛ ТРЕТИЙ

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема № 9. Угрозы несанкционированного доступа к информации.

Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

Тема № 10. Методы, способы и средства защиты информации от несанкционированного доступа.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов защиты. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Основные требования и рекомендации по защите персональных данных. Основные рекомендации по защите информации, составляющей коммерческую тайну.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

Тема № 11. Методы, способы и средства оценки защищённости от несанкционированного доступа к информации.

Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Программы поиска и гарантированного уничтожения информации, контроля состояния сертифицированных программных средств защиты информации. Программные средства создания модели системы разграничения доступа и контроля полномочий доступа к информационным ресурсам.

Методика проведения аттестационных испытаний системы защиты от несанкционированного доступа к информации. Анализ и оценка технологического процесса обработки защищаемой информации. Испытания подсистем управления доступом, обеспечения целостности, регистрации и учета.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

РАЗДЕЛ ЧЕТВЁРТЫЙ

ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ РАБОТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Тема № 12. Общие вопросы организации работ по технической защите информации ограниченного доступа.

Цели и задачи технической защиты информации ограниченного доступа. Способы и средства их реализации. Классификация способов и средств технической защиты информации ограниченного доступа. Основные механизмы защиты. Подходы к созданию комплексной системы защиты информации в организации. Определение перечня сведений конфиденциального характера, составляющих коммерческую тайну в организации. Общая последовательность и методика принятия управленческого решения на организацию защиты информации. Оценка обстановки. Выявление проблем. Постановка задачи на организацию технической защиты конфиденциальной информации. Определение путей и очередности решения вопросов технической защиты информации. Разработка вариантов дальнейших действий. Моделирование, оценка эффективности и выбор оптимального варианта организационно-технических мер защиты. Формулирование управленческого решения. Разработка директивных указаний подчиненным.

Структура, функции и задачи подразделений технической защиты информации. Основные принципы построения системы защиты информации ограниченного доступа в организации. Разработка концепции и политики информационной безопасности организации.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

Тема № 13. Подготовка объектов информатизации к аттестации по требованиям безопасности информации.

Планирование работ по технической защите информации ограниченного доступа. Обоснование требований к системе защиты информации. Требования к применяемым техническим средствам защиты информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации. Особенности подготовки к аттестации по требованиям безопасности информации защищаемых помещений, автоматизированных систем и информационных систем персональных данных.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-4, ПК-5, ПК-7, ПК-8, ПК-9, ПК-10.

Тема № 14. Сертификация средств защиты информации и аттестация объектов информатизации.

Назначение и состав системы сертификации средств защиты информации по требованиям безопасности информации. Обзор правовой базы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Структура системы сертификации и подсистемы аттестации объектов информатизации по требованиям безопасности информации. Обзор средств защиты подлежащих сертификации. Декларирование соответствия. Объекты информатизации, подлежащие аттестации. Порядок проведения сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации. Программы и методики, разрабатываемые для проведения аттестационных испытаний.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

Тема № 15. Лицензирование деятельности по технической защите конфиденциальной информации.

Обзор правовой базы лицензионной деятельности ФСТЭК России. Структура системы лицензирования ФСТЭК России. Порядок лицензирования, лицензионные требования и условия осуществления деятельности по технической защите конфиденциальной информации. Формы документов ФСТЭК России, используемые при лицензировании деятельности по технической защите конфиденциальной информации.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-10.

2.3. Календарный учебный график

Наименование темы	Объём нагрузки, час.	Учебные дни								
		1	2	3	4	5	6	7	8	9
Раздел № 1. Общие вопросы технической защиты информации ограниченного доступа.	**16**									
Тема № 1. Основные термины и определения в области технической защиты информации ограниченного доступа.	4	4								
Тема № 2. Нормативные правовые акты по технической защите информации ограниченного доступа.	4	4								
Тема № 3. Организационно-распорядительные документы по технической защите информации ограниченного доступа.	2		2							
Тема № 4. Нормативные и методические документы по технической защите информации ограниченного доступа.	4		4							

Тема № 5. Сравнительный анализ международных и национальных стандартов в области защиты информации.	2		2							
Раздел № 2. Защита информации от утечки по техническим каналам.	**16**									
Тема № 6. Угрозы утечки информации по техническим каналам.	6			6						
Тема № 7. Методы, способы и средства защиты информации от утечки по техническим каналам.	6			2	4					
Тема № 8. Методы, способы и средства оценки защищённости информации от утечки по техническим каналам.	4				4					
Раздел № 3. Защита информации от несанкционированного доступа (НСД).	**24**									
Тема № 9. Угрозы несанкционированного доступа к информации.	8					8				
Тема № 10. Методы, способы и средства защиты информации от несанкционированного доступа.	12						8	4		
Тема № 11. Методы, способы и средства оценки защищённости от несанкционированного доступа к информации.	4							4		
Раздел № 4. Организация и обеспечение работ по технической защите информации ограниченного доступа.	**12**									
Тема № 12. Общие вопросы организации работ по технической защите информации ограниченного доступа.	4								4	
Тема № 13. Подготовка объектов информатизации к аттестации по требованиям безопасности информации.	4								4	
Тема № 14. Сертификация средств защиты информации и аттестация объектов информатизации.	2									2
Тема № 15. Лицензирование деятельности по технической защите конфиденциальной информации.	2									2
Итоговый контроль	**4**									4
Всего	**72**									

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

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

Лица, желающие освоить дополнительную профессиональную программу повышения квалификации, должны иметь среднее профессиональное или высшее непрофильное техническое образование смежное с УГНПС 10.00.00. Информационная безопасность (Электроника, радиотехника и системы связи, Инфокоммуникационные технологии и системы связи, Информатика и вычислительная техника, Информационные системы и технологии, Радиотехника, Прикладная информатика).

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

Желательно иметь стаж работы (не менее 1 года), связанной с эксплуатацией автоматизированных информационных систем; установкой, настройкой и обслуживанием средств защиты информации; разработкой организационно-распорядительных документов регламентирующих вопросы защиты информации и обеспечения информационной безопасности.

Желательно также иметь опыт работы и навыки по управлению сетевой инфраструктурой на основе ОС Microsoft Windows Server; понимание принципов работы сетей TCP/IP.

При освоении дополнительной профессиональной программы повышения квалификации возможен зачет учебных предметов, курсов, дисциплин (модулей), освоенных в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, порядок которого определяется организацией самостоятельно.

3.2. Требования к кадровым условиям реализации программы

Реализация программы обеспечивается штатными руководящими и научно-педагогическими работниками НОУДПО «Институт «АйТи». В отдельных случаях, по согласованию с заказчиками, в целях более эффективной реализации программы, привлекаются специалисты производителей (вендоров) и дистрибьюторов конкретных средств защиты информации. Привлечение осуществляется на основе гражданско-правового договора. Обязательным условием привлечения внештатных преподавателей является наличие тренерского сертификата (сертификата специалиста по изучаемому продукту) от производителя.

Научно-педагогические работники, осуществляющие преподавание данной программы, имеют образование, соответствующее профилю преподаваемой дисциплины (модуля), конкретный опыт реализации научно-прикладных разработок и иной формы практической деятельности в области информационной безопасности.

3.3. Требования к материально-техническим условиям реализации программы

Учебно-методические материалы включают: учебные и учебно-методические пособия Академии АйТи по рассматриваемым темам; рабочие тетради (презентации, используемые для проведения учебных занятий, распечатанные в формате pdf) по всем темам, читаемым в рамках курса; практикумы по отдельным темам учебной программы; CD – диски с нормативно-методическими и организационно-распорядительными документами, необходимыми для развёртывания и правильной организации эксплуатации различных средств технической и криптографической защиты информации. В ходе практических занятий используется программное обеспечение и техническая документация программ-

ных, аппаратных и программно-аппаратных средств технической и криптографической защиты информации.

В случае поступления заявок от лиц с ограниченными возможностями здоровья, т.е. физических лиц, имеющих недостатки в физическом и (или) психологическом развитии, подтвержденные психолого-медико-педагогической комиссией и препятствующие получению образования без создания специальных условий, в НОУДПО «Институт «АйТи» создаются условия, позволяющие вышеприведённым категориям граждан, освоить Программу повышения квалификации.

В частности:

- возможно использование специальных педагогических подходов и наиболее подходящих для этих лиц языков, методов, способов общения и условий, в максимальной степени способствующих получению образования определенного уровня и определенной направленности;
- проведение занятий в отдельных классах, группах;
- предоставление возможности проведения занятий с использованием дистанционных образовательных технологий и электронного обучения;
- выделение сотрудников НОУДПО «Институт «АйТи», сопровождающих лиц с ограниченными возможностями здоровья, при нахождении в учебном центре;
- частичное снижение учебной нагрузки с учётом состояния обучаемого;
- сокращение часов аудиторных занятий до приемлемого минимума;
- оборудование учебных классов лабораторным оборудованием, позволяющим пользоваться им в зависимости от возможностей лица с ограниченными возможностями;
- предоставление бесплатно специальных учебников и учебных пособий, иной учебной литературы, а также услуг сурдопереводчиков и тифлосурдопереводчиков;
- обеспечение подготовки педагогических работников, владеющих специальными педагогическими подходами и методами обучения обучающихся с ограниченными возможностями здоровья.

Используемое оборудование и информационные технологии

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
Аудитория	лекции	компьютер, мультимедийный проектор, экран, маркерная доска, фломастеры
Компьютерный класс	лабораторные занятия	Компьютеры и программное обеспечение: лабораторный стенд, где с помощью технологии виртуальных машин VMware смоделирована корпоративная сеть организации.
Компьютерный класс	практические занятия	компьютеры и программное обеспечение: лабораторный стенд с использованием виртуальных технологий VMware Workstation комплексной системы защиты информации от несанкционированного доступа «Панцирь-К», Аккорд, SecretNet, DeviceLock.

Компьютерный класс	практические занятия	компьютеры и программное обеспечение: лабораторный стенд с использованием виртуальных технологий VMware Workstation eToken PKI Client (SafeNet Authentication Client, Единый клиент JaCarta); Token Management System (SafeNet Authentication Manager, JaCarta Management System); eToken Network Logon (SafeNet Network Logon); аппаратные ключи eToken.
Компьютерный класс	практические занятия	четыре рабочих места для отработки вопросов использования средств защиты информации от утечки по техническим каналам: средства защиты и контроля защищённости НПО «Анна»; ООО «ЦБИ «Маском».

3.4. Требования к информационному и учебно-методическому обеспечению программы

В процессе реализации программы повышения квалификации используются действующие правовые, нормативные и методические документы в области обеспечения информационной безопасности, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСБ и ФСТЭК России, а также соответствующие учебно-методические пособия и иллюстративный материал (презентации).

Перечень используемых учебно-методических, правовых, нормативных и методических документов в области информационной безопасности, используемых при подготовке и в ходе реализации Программы повышения квалификации, по каждому модулю и темам занятий, приведён в таблице 2 (ссылки на конкретные источники из общего списка литературы).

Таблица 2

Перечень используемых учебно-методических, правовых, нормативных и методических документов в области информационной безопасности

Наименование темы	Порядковый номер из списка литературы		
	Основная литература	Нормативные правовые акты	Нормативные методические документы
Раздел № 1. Общие вопросы технической защиты информации ограниченного доступа.	1, 2	1 - 35	1 - 45
Раздел № 2. Защита информации от утечки по техническим каналам.	4, 5, 8	15, 21, 24, 28	1 - 45
Раздел № 3. Защита информации от несанкционированного доступа (НСД).	5 - 10	15, 21, 24, 28	1 - 45
Раздел № 4. Организация и обеспечение работ по технической защите информации ограниченного доступа.	1, 2, 8 - 10	24	1 - 45

Перечень литературы

Основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. «Основы информационной безопасности»: Учеб. пособие. -М.: Горячая линия-Телеком, 2006.
2. Тихонов В.А., Райх В.В., «Информационная безопасность: концептуальные, правовые, организационные и технические аспекты». Учебное пособие. - М.: Гелиос АРВ, 2006.
3. Шаньгин В.Ф. «Защита компьютерной информации». - М.: ДМК Пресс, 2008.
4. Курило А.П., Зефиров С.Л., Голованов В.Б. «Аудит информационной безопасности». - М.: Издательская группа «БДЦ-пресс», 2006.
5. Хорев А.А. Защита информации от утечки по техническим каналам: Учеб. пособие. -М.: МО РФ, 2006.
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов. Под ре. Зайцева А.П. и Шелупанова А.А. Гриф Министерства образования и науки РФ. – 7-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2012.
7. Курило А.П., Милославская Н.Г., Сенатров М.Ю., Толстой А.И. Серия «Вопросы управления информационной безопасностью. Книга 1-5». Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012.
8. Семенихин И.В., Малахов И.В., Иванов В.В. Организационно-правовые основы защиты информации ограниченного доступа. Учебное пособие. – М.: Академия АйТи, 2012.
9. Семенихин И.В., Малахов И.В., Иванов В.В. Угрозы безопасности информации в информационных системах. Учебное пособие. – М.: Академия АйТи, 2014.
10. Семенихин И.В., Малахов И.В., Иванов В.В. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах. Учебное пособие. – М.: Академия АйТи, 2012.

Нормативные правовые акты

1. Конституция Российской Федерации, принята 12 декабря 1993 г.
2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
4. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
8. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
9. Федеральный закон от 27 декабря 2002 г. № 184 «О техническом регулировании».
10. Закон РФ № 195-ФЗ от 30 декабря 2001 г. «Кодекс Российской Федерации об административных правонарушениях».
11. Закон РФ № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации».
12. Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения».

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

14. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации 12 мая 2009 г. № 537.

15. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

16. Указ Президента Российской Федерации от 12 мая 2008 г. № 724 «Вопросы системы и структуры федеральных органов исполнительной власти».

17. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

18. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации».

19. Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

20. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

21. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

22. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.

23. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

24. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

25. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

26. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

27. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

28. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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».

29. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № 940 «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с федеральной службой безопасности российской федерации и федеральной службой по

техническому и экспортному контролю».

30. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».

31. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

32. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

33. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

34. Постановление Правительства Российской Федерации от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных».

35. Постановление Правительства Российской Федерации от 18 мая 2009 г., «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

Нормативные методические документы

1. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам». Гостехкомиссия России. - М., 2002.

3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России. - М., 1995.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России. - М., 2006.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

6. ГОСТ Р ИСО/МЭК 27001-2006. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

7. ГОСТ Р ИСО/МЭК 27002-2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

8. ГОСТ Р 51583-2014. Защита информации. Порядок создания информационных систем в защищённом исполнении. Общие положения.

9. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.

10. Приказ ФСБ и ФСТЭК России № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

11. Приказ ФСБ России от 1 апреля 2009 г. № 123 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

12. Приказ ФСБ России от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

13. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты».

14. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений».

15. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

16. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

17. Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

18. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

19. Приказ ФСТЭК России № 119 от 27 сентября 2013 г., «Об утверждении требований к средствам доверенной загрузки».

20. Методика определения актуальных угроз в ключевых системах информационной инфраструктуры. Утверждена заместителем директора ФСТЭК России 18 мая 2007 г.

21. Общие требования по обеспечению безопасности в ключевых системах информационной инфраструктуры. Утверждены заместителем директора ФСТЭК России 18 мая 2007 г.

22. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Утверждены заместителем директора ФСТЭК России 19 мая 2007 г.

23. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры. Утверждена заместителем директора ФСТЭК России 18 мая 2007 г.

24. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВРСП-К). Приказ ФСТЭК России № 27 дсп от 15 марта 2012 г.

25. Приказ Минкомсвязи России от 27 октября 2011 г. № 282 «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

26. Приказ Роскомнадзора от 14 ноября 2011 г. № 312 «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

27. Приказ Роскомнадзора от 19 августа 2011 г. № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

28. Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

29. Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

30. Методические рекомендации по применению приказа Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Утверждены Руководителем Роскомнадзора 13 декабря 2013 г.

31. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».

32. Приказ Минкомсвязи России от 23 октября 2011 г. № 321 «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по организации ведения единого государственного реестра сертификатов ключей подписей удостоверяющих центров, обеспечению доступа к нему и к реестру сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, физических лиц и организаций».

33. Приказ Минкомсвязи России от 27 октября 2011 г. № 282 «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

34. Приказ Минкомсвязи России от 05 ноября 2011 г. № 250 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

35. Приказ Минкомсвязи России от 23 ноября 2011 г. № 320 «Об аккредитации удостоверяющих центров».

36. Приказ Минкомсвязи России от 13 апреля 2012 г. № 180 «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».

37. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». - М., 1999.

38. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.

39. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.

40. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.

41. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». - М., 1992.

42. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.

43. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

44. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

3.5. Требования к условиям проведения занятий

Полный учебный цикл включает лекционные, практические и контрольно-проверочные занятия.

Не менее 50% времени курса повышения квалификации уделяется изучению практических вопросов организации защиты информации и эксплуатации изучаемых средств защиты информации. При этом в ходе проведения очных аудиторных занятий не менее 70 % учебного времени уделяется изучению практического использования средств технической и криптографической защиты информации.

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации. Часть лекций излагается проблемным методом с привлечением слушателей для решения сформулированных преподавателем проблем. К чтению лекций приказом руководителя образовательного учреждения допускаются наиболее опытные преподаватели.

На практические (лабораторные) занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программных, программно-аппаратных средств защиты информации при их обработке в автоматизированных информационных системах, проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. При проведении практических занятий отрабатываются задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматриваются занятия с проведением деловых игр.

В процессе практического обучения особое внимание уделяется формированию и развитию у слушателей практических умений и навыков.

Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий.

На практических занятиях отводится время для проверки знаний и навыков слушателей по пройденному материалу и усвоению изучаемой темы.

Для предупреждения несчастных случаев при отработке практических заданий в начале занятий со слушателями обращается внимание на правила техники безопасности. Преподаватель в ходе занятий обязан строго контролировать соблюдение слушателями установленных правил техники безопасности. В ходе занятий преподаватель несёт личную ответственность за правильное использование оборудования, приборов и соблюдение мер техники безопасности слушателями.

В целях повышения эффективности учебного процесса широко используются средства вычислительной техники, интернет технологии, средства виртуализации, презентации, схемы, плакаты, макеты, реальные программно-аппаратные и программные средства, образцы установленных форм документов и другие наглядные пособия.

3.6. Порядок передачи программы повышения квалификации другой организации

Передача программы повышения квалификации другой организации, при необходимости, может быть произведена на договорной основе.

Основными условиями передачи являются:

- наличие у организации лицензии на осуществление образовательной деятельности по указанным в приложении (приложениях) образовательным программам;
- соответствие другой организации требованиям к кадровым и материально-техническим условиям реализации программы, к информационному и учебно-

методическому обеспечению программы и условиям проведения занятий;

– предоставление возможности осуществления предварительной проверки организации на соответствие вышеуказанным требованиям комиссии НОУДПО «Институт «АйТи», а также последующий контроль процесса реализации программы.

Проверка соответствия организации, которой предполагается передача программы повышения квалификации, требованиям к кадровым и материально-техническим условиям реализации программы, требованиям к информационному и учебно-методическому обеспечению программы и требованиям к условиям проведения занятий до заключения договора, возлагается на комиссию назначаемую руководителем НОУДПО «Институт «АйТи».

3.7. Порядок внесения изменений в программу повышения квалификации

Данная программа повышения квалификации подлежит переработке не реже, чем раз в три года, или при изменении нормативных правовых и методических документов ФСТЭК России, регламентирующих принципиальные вопросы, связанные с тематикой модулей, рассматриваемой при реализации программы. Порядок внесения изменений в программу повышения квалификации и последующее согласование, определяются действующими на момент переработки нормативными правовыми и иными документами Российской Федерации.

4. ФОРМЫ АТТЕСТАЦИИ И ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

Контрольно-проверочные занятия должны включать входной и текущий контроли, а так же итоговую аттестацию обучающихся.

Входной контроль должен охватывать всех обучаемых и проводится в форме тестирования. Целью его является определение уровня знаний обучаемых для корректировки и адаптации учебного процесса под конкретные потребности обучаемых, с учётом уровня освоения учебного материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Текущий контроль должен охватывать как можно большее число слушателей с обязательной оценкой их знаний, умений и навыков. Он должен стимулировать учебную работу слушателей и проводиться в форме, избранной преподавателем или предусмотренной рабочей программой.

Оценочные средства, включают типовые задания, выполняемые в ходе практических занятий и тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций. В ходе тестирования используются современные способы и формы оценивания обучающихся, включая создание единой информационной среды с электронными формами контроля и оценки.

Основными критериями оценки усвоения слушателями учебного материала при проведении текущего контроля в ходе практических занятий являются: полнота ответов на поставленные вопросы; правильность выполнения действий при отработки практических вопросов эксплуатации изучаемых средств защиты информации; соответствие содержания и объёма выполненного задания поставленной задаче; правильность оформления; правильное форматирование отрабатываемых документов; правильность оформления ссылок на правовые, нормативные и методические документы.

При этом для каждого критерия оценки каждого практического занятия определяются весовые коэффициенты, позволяющие в определённом конкретном случае получать наиболее объективные оценки выполненных слушателями заданий.

Программы текущего контроля и промежуточной аттестации максимально приближены к условиям (требованиям) их будущей профессиональной деятельности.

Конкретные формы и процедуры входного и текущего контроля знаний по каждой теме разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся в течение первого дня обучения.

Для проведения контрольно-проверочных занятий образовательным учреждением разработаны тестовые задания, включающие: организационно-методические указания по прохождению тестирования; вопросы для тестирования (не менее 20 вопросов для входного и промежуточных тестов и не менее 40 вопросов для итогового теста).

Каждый Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).

При этом как в вопросах, так и в ответах учтена возможность многовариантности решений. Вопросы, предлагающие выбрать все правильные варианты ответа, имеют два и более верных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа. Ответ на вопрос считается правильным, если он является полным.

Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы. Во время тестирования запрещается пользоваться какой-либо литературой или заранее подготовленными записями.

При проведении тестирования с использованием единой информационной среды с электронными формами контроля и оценки у каждого слушателя есть три попытки на прохождение тестирования. Время на одну попытку - 40 минут. По окончанию попытки слушатель может видеть результаты теста и полученные баллы через две минуты после отправки результатов. При этом имеется возможность просмотра отчета, показывающего ошибки при прохождении теста. Оценка выставляется по последней попытке.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций. Фонды оценочных средств разрабатываются и утверждаются образовательным учреждением самостоятельно.

Контрольно–оценочная информация включает в себя следующие вопросы для самоконтроля знаний и примерный перечень вопросов при итоговой аттестации:

Вопрос 1: Каковы основные нормативно-правовые акты по технической защите информации ограниченного доступа?

Ответ: Конституция РФ, Указ Президента РФ 537, Доктрина ИБ, ФЗ-390, ФЗ 5485-1, ФЗ-99, ФЗ-63, ФЗ–184, ФЗ-98, ФЗ-149, ФЗ-160, ФЗ-152, ПП 1119, НМД ФСТЭК и ФСБ.

Вопрос 2: Каковы основные виды утечек информации по техническим каналам?

Ответ: утечка речевой информации; утечка видовой информации; утечка информации, представленной в виде электрических импульсов; утечка информации, представленной в виде логических структур.

Вопрос 3: Каковы основные способы защиты информации от утечки по техническим каналам?

Ответ: специальные проверки, специальные исследования, специальные обследования.

Вопрос 4: Каковы основные угрозы несанкционированного доступа к информации?

Ответ: угроза нарушения конфиденциальности информации; угроза нарушения целостности информации; угроза нарушения доступности информации.

Вопрос 5: Какими основными методами оценивается защищённость от несанкционированного доступа к информации?

Ответ: согласно приказов ФСТЭК №17 и №21, РД ФСТЭК и методических рекомендаций, по всем разделам.

Вопрос 6: Какова нормативно-методическая база для проведения лицензирования деятельности в области защиты информации?

Ответ: ФЗ-99, ПП-957, 313, 314, 287, 171, 79; Приказы ФСТЭК 83, 84; Приказы ФСБ 157, 7, 440.

Освоение программы повышения квалификации специалистов завершается обязательной итоговой аттестацией.

Итоговая аттестация проводится в форме тестирования.

Лицам, успешно освоившим соответствующую дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдаётся удостоверение о повышении квалификации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы повышения квалификации и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения, по установленному образцу.

5. СОСТАВИТЕЛИ ПРОГРАММЫ

Заведующий кафедрой Информационной безопасности
Негосударственного образовательного учреждения дополнительного
профессионального образования «Институт информационных технологий «АйТи»
кандидат военных наук, доцент

И.В. Семенихин