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»

**«Комплексное обеспечение
информационной безопасности автоматизированных систем»**

Виды профессиональной деятельности:
организационно-управленческая, эксплуатационная

Трудоёмкость обучения: 104 часа

Москва
2015

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Общие положения

Настоящая дополнительная профессиональная программа повышения квалификации «Комплексное обеспечение информационной безопасности автоматизированных систем» (далее – программа повышения квалификации) разработана на основании Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Приказа Министерства образования и науки 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 Министерства образования и науки 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 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), утвержденного Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

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

Руководители и сотрудники государственных, муниципальных органов и организаций различных форм собственности, физические лица, использующие и (или) планирующие использовать шифровальные (криптографические) средства для обеспечения информационной безопасности. Руководители и сотрудники департаментов (отделов, служб) информационных технологий и информационной безопасности. Специалисты по защите информации.

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 информации, 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 материальных 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 техни-

ческих 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, 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 защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну и сертификации средств защиты информации;
- систему организации комплексной защиты информации ограниченного доступа;
- 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 сетей;
- 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 организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации;
- правильно эксплуатировать системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации;

владеть:

- профессиональной терминологией;
- методами криптографической информации;
- методами организации и управления деятельностью;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
- навыками применения шифровальных (криптографических) средств;
- навыками организации и обеспечения режима защиты информации;

1.6. Трудоёмкость программы

Нормативная трудоемкость обучения по данной программе – 104 часа, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.7. Форма и сроки обучения

Обучение по программе повышения квалификации осуществляется в очно-заочной форме.

Срок обучения составляет: 13 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. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств.**	**16**	**11**	**5**	**0**	**0**	**0**
2.	**Тема №1.** Введение. Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности.	2	2	0	0	0	0
3.	**Тема №2.** Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	6	4	2	0	0	0
4.	**Тема №3**. Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств.	6	4	2	0	0	0

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	За чёт
			Лекции	Практические занятия	Семинары		
5.	**Тема №4.** Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами.	2	1	1	0	0	0
6.	**Раздел №2. Теоретические основы использования шифровальных (криптографических) средств.**	**16**	**11**	**5**	**0**	**0**	**0**
7.	**Тема №5.** Методы и способы криптографической защиты информации.	8	6	2	0	0	0
8.	**Тема №6.** Инфраструктура открытых ключей (ИОК/PKI).	6	4	2	0	0	0
9.	**Тема №7.** Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.	2	1	1	0	0	0
10.	**Раздел №3. Организационные мероприятия по использованию шифровальных (криптографических) средств.**	**16**	**8**	**8**	**0**	**0**	**0**
11.	**Тема №8.** Организация использования СКЗИ и ЭП	4	2	2	0	0	0
12.	**Тема №9.** Регламентация обеспечения информационной безопасности	4	2	2	0	0	0
13.	**Тема №10.** Частные регламенты использования СКЗИ и ЭП в информационных системах	4	2	2	0	0	0
14.	**Тема №11.** Регламентация использования СКЗИ и ЭП на рабочем месте	4	2	2	0	0	0
15.	**Раздел №4. Практическое применение сертифицированных шифровальных (криптографических) средств.**	**52**	**12**	**31**	**0**	**9**	**0**

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	Зачёт
			Лекции	Практические занятия	Семинары		
16.	**Тема №12.** Назначение и порядок использования аппаратных ключей в качестве ключевых носителей на примере аппаратных ключей eToken (JaCarta) (производства компании SafeNet, ЗАО «Аладдин Р.Д.»)	4	1	2	0	1	0
17.	**Тема №13.** Назначение, состав и порядок использования систем управления жизненным циклом аппаратных ключей на примере продуктов TMS (JMS) (производства ЗАО «Аладдин Р.Д.») или SafeNet Authentication Manager (SAM, производства компании SafeNet)	10	2	6	0	2	0
18.	**Тема №14.** Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP» (производства ООО «КритоПро»).	3	1	1	0	1	0
19.	**Тема №15.** Назначение, состав и порядок использования программно-аппаратных средств автоматизации деятельности Удостоверяющих центров на примере ПАК «Удостоверяющий Центр КриптоПро УЦ» (производства ООО «КритоПро»).	18	2	14	0	2	0

№ п/п	Наименование тем	Всего часов	Аудиторные занятия, час			Самостоятельная работа	Зачёт
			Лекции	Практические занятия	Семинары		
20.	**Тема №16.** Назначение, состав и порядок использования СКЗИ, применяемых для обеспечения безопасности передачи по каналам связи информации ограниченного доступа на примерах продуктов «КриптоПро IPsec» (производства ООО «КритоПро») или АПКШ «Континент» (производства ООО «Код безопасности»), или VipNet CUSTOM (производства ООО ИнфоТеКС).	13	5	6	0	2	0
21	**Тема №17.** Назначение и порядок использования СКЗИ, применяемых для обеспечения защиты от несанкционированного доступа (НСД) к информации ограниченного доступа на примере продукта «Secret Disk» (производства ЗАО «Аладдин Р.Д.») или «StrongDisk» (производства компании «Физтех-софт»).	4	1	2	0	1	0
22.	**Итоговый контроль**	**4**	**0**	**0**	**0**	**0**	**4**
	Всего	**104**	**42**	**49**	**0**	**9**	**4**

2.2. Рабочие программы дисциплин (модулей)

РАЗДЕЛ ПЕРВЫЙ

ЗАКОНОДАТЕЛЬНАЯ И НОРМАТИВНО-МЕТОДИЧЕСКАЯ БАЗА ИСПОЛЬЗОВАНИЯ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ.

Тема 1. Введение. Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности.

Общее понятие «информационная безопасность» в законодательстве Российской Федерации и практика его применения в органах государственной власти и организациях независимо от формы их собственности. Конституция Российской Федерации. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Уголовная и административная ответственность за нарушение законодательства в информационной сфере.

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

Тема 2. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.

Федеральные законы «Об информации, информационных технологиях и о защите информации», «О коммерческой тайне», «Об электронной подписи». Указы Президента Российской Федерации, Постановления Правительства РФ, организационно-распорядительные документы федеральных органов исполнительной власти (Приказы министерств), регулирующие вопросы использования шифровальных (криптографических) средств для обеспечения информационной безопасности.

Обзор правовой базы сертификации средств защиты информации, не содержащей сведений, составляющих государственную тайну. Структура системы сертификации. Декларирование соответствия. Порядок проведения сертификации.

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

Тема № 3. Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств.

Содержание и основные положения «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», ПКЗ-2005, «Состав и содержание 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», «Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» и «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».

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

Тема № 4. Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами.

Обзор правовой базы лицензионной деятельности ФСБ России. Структура системы лицензирования ФСБ России. Порядок лицензирования, лицензионные требования и условия осуществления видов деятельности, связанных с шифровальными (криптографическими) средствами. Формы документов ФСБ России, используемые при лицензировании видов деятельности, связанных с шифровальными (криптографическими) средствами.

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

РАЗДЕЛ ВТОРОЙ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ

Тема № 5. Методы и способы криптографической защиты информации.

Основные понятия и определения криптографической защиты информации. Алгоритмы симметричного шифрования. Алгоритмы асимметричного шифрования. Алгоритмы хэширования. Составные (гибридные) криптографические системы (алгоритмы). Алгоритмы создания и проверки цифровой подписи. Общие сведения о криптоанализе.

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

Тема № 6. Инфраструктура открытых ключей (ИОК/PKI).

Основные понятия и определения PKI. Необходимость наличия PKI. Назначение и взаимодействие элементов PKI. Основные функции Центра Сертификации (ЦС/CA) и Центра Регистрации (ЦР/RA). Назначение сертификата открытого ключа (СОК/РКС). Состав РКС.

Доверие в PKI. Модели доверия. Сравнительный анализ моделей доверия. Построение пути сертификации. Проверка пути сертификации. Примеры моделей доверия.

Системы стандартов в области PKI. Стандарт X.509. Группа стандартов Public Key Cryptography Standards (PKCS). Стандарты сетей TCP/IP (RFC).

Протоколы, используемые в PKI: операционные протоколы, протоколы управления, протоколы валидации, протокол меток времени. Основные группы приложений-потребителей услуг PKI: защищенная электронная почта, защищенный доступ к веб-службам, виртуальные частные сети.

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 № 7. Обзор сертифицированных шифровальных (криптографических) средств защиты информации.

Назначение и возможности основных групп сертифицированных шифровальных (криптографических) средств, включённых в «Перечень средств защиты информации, не содержащей сведений, составляющих государственную тайну». Методика оценки и выбора сертифицированных средств СКЗИ.

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

РАЗДЕЛ ТРЕТИЙ

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ИСПОЛЬЗОВАНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ

Тема № 8. Организация использования СКЗИ и ЭП.

Порядок использования средств криптографической защиты информации и ключевой информации к ним внутри организации. Порядок использования средств криптографической защиты информации и электронной подписи при информационном обмене.

Общие положения. Функции, права и обязанности оператора конфиденциальной связи и органа криптографической защиты. Порядок допуска сотрудников к работе с СКЗИ. Права и обязанности пользователей СКЗИ.

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 № 9. Регламентация обеспечения информационной безопасности.

Порядок обеспечения безопасности информации при защищенном обмене электронными документами в системе электронного документооборота. Порядок обеспечения безопасности средств криптографической защиты 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.

Тема № 10. Частные регламенты использования СКЗИ и ЭП в информационных системах.

Организация защищённого корпоративного документооборота с использованием средств криптографической защиты информации и электронной подписи.

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. Регламентация использования СКЗИ и ЭП на рабочем месте.

Требования к оборудованию помещений и режиму охраны. Требования к эксплуатации ПЭВМ пользователя с установленным СКЗИ. Мероприятия при компрометации ключевой информации. Инструкции пользователю.

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

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СЕРТИФИЦИРОВАННЫХ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ

Тема № 12. Назначение и порядок использования аппаратных ключей в качестве ключевых носителей на примере аппаратных ключей eToken.

Программная и аппаратная архитектуры аппаратных ключей. Преимущества использования аппаратных ключей в качестве функциональных ключевых носителей. Модели аппаратных ключей различных производителей.

Установка, настройка и использование программного обеспечения eToken PKI Client, либо SafeNet Authentication Client, либо JaCarta Unified Client в актуальных версиях совместно с аппаратными ключами семейства eToken (производства компании SafeNet), либо JaCarta (производства ЗАО «Аладдин Р.Д.»).

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. Назначение, состав и порядок использования систем управления жизненным циклом аппаратных ключей на примере продуктов TMS (JMS) (производства ЗАО «Аладдин Р.Д.») или SafeNet Authentication Manager (SAM, производства компании SafeNet).

Жизненный цикл аппаратных ключей. Необходимость использования систем управления жизненным циклом аппаратных ключей.

Установка, настройка и использование системы управления жизненным циклом аппаратных ключей на примере продуктов: Token Management System (TMS, производства ЗАО «Аладдин Р.Д.»), либо SafeNet Authentication Manager (SAM, производства компании SafeNet), либо JaCarta Management System (JMS, производства ЗАО «Аладдин Р.Д.») в сети, построенной на основе технологии Microsoft Active Directory.

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

Тема № 14. Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP» (производства ООО «КритоПро»).

Принципы встраивания СКЗИ в состав ОС на примере ОС Microsoft Windows. Состав и структура сертифицированных СКЗИ, встраиваемых в ОС и предназначенных для совместного использования с другими приложениями, реализующими процесс непосредственной обработки информации.

Установка и настройка СКЗИ «КриптоПро CSP». Настройка и применение аппаратных ключей eToken (JaCarta) в качестве функциональных ключевых носителей для «КриптоПро CSP».

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. Назначение, состав и порядок использования программно-аппаратных средств автоматизации деятельности Удостоверяющих центров на примере ПАК «Удостоверяющий Центр КриптоПро УЦ» (производства ООО «КритоПро»).

Состав и структура сертифицированных СКЗИ, используемых для автоматизации деятельности Удостоверяющих центров.

Настройка и практическое использование программно-аппаратного комплекса (ПАК) «Удостоверяющий Центр КриптоПро УЦ» (производства ООО «КриптоПро») для построения системы юридически значимой электронной подписи (ЭП).

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 № 16. Назначение, состав и порядок использования СКЗИ, применяемых для обеспечения безопасности передачи по каналам связи информации ограниченного доступа на примерах продуктов «КриптоПро IPsec» (производства ООО «КритоПро») или АПКШ «Континент» (производства ООО «Код безопасности»), или VipNet Custom (производства ООО ИнфоТеКС).

Состав, структура и основные функции, реализуемые сертифицированными СКЗИ, используемыми для обеспечения безопасности передачи по каналам связи информации ограниченного доступа.

Использование протокола IPsec для построения защищенных соединений по различным сценариям. Состав, назначение и порядок применения программного обеспечения «КриптоПро IPsec» (производства ООО «КритоПро») для построения защищенных корпоративных сетей (сегментов сетей).

Назначение, состав, модельный ряд и основные возможности аппаратно-программного комплекса (АПКШ) «Континент» (производства ООО «Код безопасности». Варианты применения АПКШ «Континент» для защиты корпоративных сетей. Установка и настройка компонентов АПКШ «Континент»: центр управления сетью, сервер доступа, криптошлюз, криптокоммутатор, АРМ администратора сети, абонентский пункт пользователя. Настройка и эксплуатация защищенных АПКШ соединений.

Назначение, состав и основные возможности программного комплекса «ViPNet CUSTOM» (производства ОАО «ИнфоТеКС»). Порядок развёртывания виртуальной сети ViPNet. Установка и настройка ViPNet [Клиент]. Использование программы ViPNet [Деловая Почта].

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 № 17. Назначение и порядок использования СКЗИ, применяемых для обеспечения защиты от несанкционированного доступа (НСД) к информации ограниченного доступа на примере продукта «Secret Disk» (производства ЗАО «Аладдин Р.Д.») или «StrongDisk» (производства компании «Физтех-софт»).

Необходимость применения СКЗИ для защиты информации ограниченного доступа от несанкционированного доступа (НСД) при ее хранении на различных носителях. Состав, структура и порядок использования СКЗИ для обеспечения НСД к информации ограниченного доступа.

Назначение, состав и основные возможности программного обеспечения «Secret Disk 4» (производства ЗАО «Аладдин Р.Д.»). Установка, настройка и использование программного обеспечения «Secret Disk 4».

Назначение, состав и основные возможности программного обеспечения «Secret Disk NG» (производства ЗАО «Аладдин Р.Д.»). Установка, настройка и использование. Управление программным обеспечением «Secret Disk NG» с помощью групповых политик Microsoft Active Directory.

Назначение, состав и основные возможности программного обеспечения «StrongDisk» (производства компании «Физтех-софт»). Установка, настройка и использование программного обеспечения «StrongDisk».

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	10	11	12	13
Раздел №1. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств.	**16**													
Тема №1. Введение. Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности.	2	2												
Тема №2. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	6	6												
Тема №3. Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств.	6		6											
Тема №4. Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами.	2		2											
Раздел №2. Теоретические основы использования шифровальных (криптографических) средств.	**16**													
Тема №5. Методы и способы криптографической защиты информации.	**8**			8										
Тема №6. Инфраструктура открытых ключей (ИОК/PKI).	**6**				6									

Наименование темы	Объём нагрузки, час.	Учебные дни												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Тема №7. Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.	**2**				2									
Раздел. №3. Организационные мероприятия по использованию шифровальных (криптографических) средств.	**16**													
Тема №8. Организация использования СКЗИ и ЭП	4					4								
Тема №9. Регламентация обеспечения информационной безопасности	4					4								
Тема №10. Частные регламенты использования СКЗИ и ЭП в информационных системах	4						4							
Тема №11. Регламентация использования СКЗИ и ЭП на рабочем месте	4						4							
Раздел №4. Практическое применение сертифицированных шифровальных (криптографических) средств.	**52**													
Тема №12. Назначение и порядок использования аппаратных ключей в качестве ключевых носителей на примере аппаратных ключей eToken (JaCarta) (производства компании SafeNet, ЗАО «Аладдин Р.Д.»)	**4**							4						

Наименование темы	Объём нагрузки, час.	Учебные дни												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Тема №13. Назначение, состав и порядок использования систем управления жизненным циклом аппаратных ключей на примере продуктов TMS (JMS) (производства ЗАО «Аладдин Р.Д.») или SafeNet Authentication Manager (SAM, производства компании SafeNet)	**10**							4	6					
Тема №14. Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP» (производства ООО «КритоПро»).	**3**								2	1				
Тема №15. Назначение, состав и порядок использования программно-аппаратных средств автоматизации деятельности Удостоверяющих центров на примере ПАК «Удостоверяющий Центр КриптоПро УЦ» (производства ООО «КритоПро»).	**18**									7	8	3		

Наименование темы	Объём нагрузки, час.	Учебные дни												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Тема №16. Назначение, состав и порядок использования СКЗИ, применяемых для обеспечения безопасности передачи по каналам связи информации ограниченного доступа на примерах продуктов «КриптоПро IPsec» (производства ООО «КритоПро») или АПКШ «Континент» (производства ООО «Код безопасности»), или VipNet Custom (производства ООО ИнфоТеКС).	**13**											5	8	
Тема №17. Назначение и порядок использования СКЗИ, применяемых для обеспечения защиты от несанкционированного доступа (НСД) к информации ограниченного доступа на примере продукта «Secret Disk» (производства ЗАО «Аладдин Р.Д.») или «StrongDisk» (производства компании «Физтехсофт»).	**4**													4
Итоговый контроль	**4**													4
Всего	**104**													

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 семейства Windows и 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: лабораторные стенды №1 и №2, где с помощью технологии виртуальных машин VMware смоделированы два варианта корпоративной сети организации.

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 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. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств.	1, 2, 4, 7	1 - 35	9 - 26
Раздел № 2. Теоретические основы использования шифровальных (криптографических) средств.	3, 5, 6, 10, 12,13	-	1 - 26
Раздел № 3. Организационные мероприятия по использованию шифровальных (криптографических) средств	1,2,7-9,11,12	21 - 29	9 - 26
Раздел № 4. Практическое применение сертифицированных шифровальных (криптографических) средств.	12	-	1 - 26

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. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2005.
4. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.
5. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: Учеб. пособие, М.: Издательский центр «Академия», 2009.
6. Полянская О. Ю., Горбатов В. С. «Инфраструктуры открытых ключей». – М.: Интернет-университет информационных технологий, Лаборатория Знаний, 2007 г.
7. Шаньгин В.Ф. «Защита компьютерной информации». - М.: ДМК Пресс, 2008.
8. Курило А.П., Зефиров С.Л., Голованов В.Б. «Аудит информационной без-

опасности». - М.: Издательская группа «БДЦ-пресс», 2006.

9. 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.

10. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. - СПб.: БХВ-Петербург, 2009.

11. Семенихин И.В., Малахов И.В., Иванов В.В. Организационно-правовые основы защиты информации ограниченного доступа. Учебное пособие. – М.: Академия АйТи, 2012.

12. Семенихин И.В., Малахов И.В., Иванов В.В. Обеспечение информационной безопасности с использованием шифровальных (криптографических) средств. Учебно-методическое пособие. – М.: Академия АйТи, 2012.

13. Шнайер Б. «Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си». 2-е издание. – М.: Триумф, 2006.

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

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

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

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

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

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

18. 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».

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

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

21. 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».

22. 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».

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

24. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

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

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

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

28. Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

29. Постановление Правительства Российской Федерации от 09 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

Нормативные методические документы

1. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

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

3. ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

4. ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита ин-

формации. Функция хэширования.

5. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

6. ГОСТ Р 34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хэширования.»

7. ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».

8. ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

9. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 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 содержащей сведений, составляющих государственную тайну».

10. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

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 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

13. 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».

14. Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

15. Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

16. Приказ ФСБ России от 30 августа 2012 г. № 440 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению 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).

17. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

18. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержа-

щей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

19. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» Утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

20. 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».

21. 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».

22. 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».

23. 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».

24. 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».

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

26. 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».

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 использования и эксплуатации изучаемых СКЗИ. При этом в ходе проведения очных аудиторных занятий не менее 70% учебного времени уделяется изучению практического использования средств 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 про-

граммных, 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 ФСБ России, регламентирующих принципиальные вопросы, связанные с тематикой моду-

лей, 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 также 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 ка-

кой-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: Укажите основные нормативно-методические активы правового регулирования применения СКЗИ и электронной подписи в корпоративных информационных системах?

Ответ: ФЗ-63; ПП – 111, 976, 634, 33; ПКЗ – 2005, Приказы ФСБ – 152, 795, 795, Приказы Минкомсвязи.

Вопрос 2: Каковы базовые методы и способы криптографической защиты информации?

Ответ: Шифрование, стеганография, кодирование, сжатие.

Вопрос 3: Какова методика выбора и применения сертифицированного криптографического средства?

Ответ: строго: обращение на сайт ФСБ, в раздел «Лицензирование деятельности», с целью ознакомления с перечнем сертифицированных СЗИ; согласование применения средства со специалистом ФСБ.

Вопрос 4: В чем суть проведения организационных мероприятий по использованию шифровальных средств?

Ответ: детальное изучение Инструкции 152; создание максимально документированной системы защиты информации; подготовка полной нормативно-методической базы для практической реализации СКЗИ.

Вопрос 5: Каково назначение аппаратных ключей типа eToken (JaCarta)?

Ответ: строгая аутентификация; безопасное хранение секретных данных; выполнение криптографических вычислений; работа с сертификатами и электронными ключами.

Вопрос 6: Каково назначение и порядок использования СКЗИ, реализующих базовый функционал криптозащиты?

Ответ: идентификация и аутентификация пользователя, защита от НСД, скрытие информации с использованием стандартных алгоритмов на всех уровнях работы информационной системы.

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

Преподаватель-эксперт кафедры Информационной безопасности
Негосударственного образовательного учреждения дополнительного
профессионального образования «Институт информационных технологий «АйТи»
кандидат военных наук, доцент

И.В. Малахов