Для служебного пользования
Экз. № 1

СОГЛАСОВАНО
Начальник 1 управления
ФСТЭК России

_____ Н.М. Мартинец
«10» февраля 2022 г.

УТВЕРЖДАЮ
Исполнительный директор
АНО ДПО «Учебный центр «Парадигма»

_____ А.В. Гребенкина
«17» февраля 2022 г.

СОГЛАСОВАНО
Федеральное УМО в системе высшего образования по УГСН «Информационная безопасность», председатель ФУМО ВО ИБ

_____ А.Б. Пичкур
«08» 12 2022 г.

Дополнительная профессиональная программа,
программа профессиональной переподготовки

«Информационная безопасность. Обеспечение защиты информации ограниченного доступа не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами»

Ярославль 2022

Содержание

1. Общие положения

Настоящая дополнительная программа профессиональной переподготовки «*Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами»* (далее - Программа) разработана с учетом положений:

Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

Указа Президента Российской Федерации от 21.02.2019 г. № 68 «О профессиональном развитии государственных гражданских служащих Российской Федерации» (вместе с «Положением о порядке осуществления профессионального развития государственных гражданских служащих Российской Федерации»).

Приказа Министерства науки и высшего образования Российской Федерации от 19 декабря 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

Приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. №1427;

Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1455.

Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1459.

Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1458.

Федерального государственного образовательного стандарта высшего образования –

специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1457.

Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 533н.

Профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 525н.

Профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 9 августа 2022 г. № 474н.

Профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 536н.

Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 16 апреля 2018 г.

Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г. № ВК-1032/06).

Примерной программы профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации». М.: ФСТЭК России, 2017 – 114 с. – Для служебного пользования.

Приказа Минкомсвязи России от 30 ноября 2015 г. № 486 «Об утверждении административных регламентов предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и исполнения Министерством связи и массовых коммуникаций Российской Федерации государственной функции по осуществлению государственного контроля и надзора за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти удостоверяющие центры были аккредитованы».

Рекомендаций по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности (письмо Банка России от 24 марта 2014 г. № 49-Т).

Квалификационных требований к должности главного специалиста-эксперта отдела

по защите информации отделения Пенсионного Фонда Российской Федерации (ПФР) (утверждены ПФР 17 февраля 2014 г.).

Программа профессиональной переподготовки позволяет формировать у слушателей компетенции, которые необходимы для решения задач при осуществлении лицензируемых видов деятельности, определяемых Постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»:

а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

в средствах и системах информатизации;

в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

в помещениях со средствами (системами), подлежащими защите;

в помещениях, предназначенных для ведения конфиденциальных переговоров (далее – защищаемые помещения);

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа (НСД) и ее модификации в средствах и системах информатизации;

в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации;

средств и систем информатизации;

помещений со средствами (системами) информатизации, подлежащими защите;

защищаемых помещений;

д) работы и услуги по проектированию в защищенном исполнении средств и систем информатизации (помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений);

е) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Так же программа профессиональной переподготовки позволяет формировать у обучаемых компетенции, которые необходимы для решения задач при осуществления следующих лицензируемых видов деятельности при выполнении работ и оказании услуг, указанных в пунктах 12, 13, 20, 21, 22, 24, 25 и 28 Перечня в Приложении к Положению, утвержденному Постановлением 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)»:

монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;

монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;

передача защищенных с использованием шифровальных (криптографических) средств информационных систем;

передача средств изготовления ключевых документов;

предоставление услуг по шифрованию информации, не содержащей сведений,

составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;

изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Программа профессиональной переподготовки реализуется в Автономной некоммерческой организации дополнительного профессионального образования «Учебный центр «Парадигма» (АНО ДПО «Парадигма»).

Разработчики:

Гребенкина Анна Владимировна, исполнительный директор АНО ДПО «Парадигма», преподаватель, специальность – «Радиофизика и электроника», квалификация – «Радиофизик», методист образовательных программ. Разработчик и куратор программ дополнительного образования взрослых в направлении работы с системой СБИС.

Панасенко Сергей Петрович, преподаватель, кандидат технических наук, более 25 лет активной работы в области информационной безопасности; экспертные знания в данной области (автор/соавтор пяти книг и более 300 публикаций по криптографии и защите информации), с августа 2022 г. является представителем в техническом комитете по стандартизации «Защита информации» (ТК 362).

Кузин Сергей Леонидович, преподаватель, доктор юридических наук, член Всемирной Академии Наук Комплексной Безопасности.

Легкодумов Александр Алексеевич, преподаватель, специальность «Компьютерная безопасность», квалификация – Специалист по защите информации, аспирант МИРЭА - Российского технического университета: технические науки/Информационные технологии и телекоммуникации/ Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Пышкина Наталия Юрьевна, преподаватель, руководитель удостоверяющего центра ООО «Компания «Тензор». Разработчик и куратор технологии выпуска сертификатов электронной подписи обученными квалифицированными специалистами компаний партнеров. Разработчик методических и обучающих материалов. Член экспертного совета по вопросам совершенствования правового регулирования в области применения электронной подписи при Минкомсвязи России, член Общественного совета при агентстве по государственным услугам Ярославской области.

Боровиков Кирилл Сергеевич, преподаватель, специальность «Компьютерная

безопасность», квалификация – Математик, руководитель органа криптографической защиты ООО «Компания «Тензор». Разработчик и куратор проекта юридически значимого электронного документооборота СБИС.

Чеперегин Александр Сергеевич, преподаватель, специальность «Информационные системы в экономике», квалификация – экономист, кандидат экономических наук.

Программа профессиональной переподготовки разработана по заказу ООО «Компания «Тензор».

Программа профессиональной переподготовки обсуждена на заседании комиссии разработчиков программы АНО ДПО «Парадигма», утвержденной приказом исполнительного директора АНО ДПО «Парадигма» №11/П/22 от 02 ноября 2022 г. (Протокол №2 от 02 декабря 2022 г.).

2. Цель реализации программы профессиональной переподготовки

Целью реализации программы профессиональной переподготовки является формирование компетенций, необходимых специалистам для выполнения нового вида профессиональной деятельности «Техническая защита информации» в части защиты информации ограниченного доступа не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами.

Программа переподготовки рассчитана, в том числе, на подготовку руководителей и (или) уполномоченных руководить работами по лицензируемому виду деятельности, а также специалистов (инженерно-технических работников) в области криптографической защиты информации.

Профессиональные компетенции необходимы для выполнения новых видов профессиональной деятельности в части защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств:

- обеспечение безопасности информации в автоматизированных системах;

- защита информации в компьютерных системах и сетях;

- обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД) к ним.

Объектами профессиональной деятельности слушателей по программе профессиональной переподготовки являются:

автоматизированные (информационные) системы различного уровня и назначения, средства и системы информатизации, технические средства (системы), не обрабатывающие конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается, помещения со средствами (системами), подлежащими защите, помещения, предназначенные для ведения конфиденциальных переговоров (далее - объекты информатизации);

технические каналы утечки информации (ТКУИ) на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;

способы обеспечения технической защиты конфиденциальной информации (далее - ТЗКИ), методы контроля защищенности конфиденциальной информации;

технические средства защиты информации, защищенные технические средства обработки информации, технические средства контроля эффективности мер защиты информации, программные (программно-технические) средства защиты информации, защищенные программные (программно-технические) средства обработки информации, программные (программно-технические) средства контроля эффективности защиты

информации (далее - средства ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации);

система нормативных правовых актов, методических документов и национальных стандартов в области технической защиты информации (ТЗИ);

шифровальные (криптографические) средства (средства криптографической защиты информации) (далее – СКЗИ), включая документацию на эти средства;

технологии обеспечения информационной безопасности информационных систем;

системы управления информационной безопасностью информационных систем;

система нормативных правовых актов, методических документов и национальных стандартов в области защиты информации с использованием СКЗИ.

В рамках освоения программы профессиональной переподготовки слушатели готовятся к решению задач профессиональной деятельности следующих типов:

организационно-управленческая;

проектная;

эксплуатационная.

Задачами профессиональной деятельности являются:

а) в организационно-управленческой деятельности:

планирование мероприятий, направленных на защиту информации, организация внедрения и применения политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

организация мероприятий по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;

поддержка и совершенствование деятельности по обеспечению ТЗКИ на объектах информатизации;

проведение аттестационных испытаний и аттестации объектов информатизации по требованиям безопасности информации;

использование нормативных правовых актов и нормативных методических документов для организации технологического процесса защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств в информационных системах.

б) в проектной деятельности:

определение ТКУИ на объектах информатизации и угроз безопасности информации в автоматизированных (информационных) системах;

формирование требований к обеспечению ТЗКИ на объектах информатизации (формирование требований к системе защиты информации объекта информатизации);

проведение контроля (мониторинга) защищенности конфиденциальной информации на объектах информатизации, а также анализа применения политик (правил, процедур) по обеспечению ТЗКИ;

разработка способов и средств для обеспечения ТЗКИ на объектах информатизации (разработка системы защиты информации объекта информатизации);

внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрение системы защиты информации объекта информатизации).

в) в эксплуатационной деятельности:

установка, монтаж, наладка, испытания, ремонт, техническое обслуживание средств защиты информации;

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения защиты информации с учетом установленных требований;

обеспечение ТЗКИ в ходе эксплуатации объектов информатизации;

обеспечение ТЗКИ при выводе из эксплуатации объектов информатизации;

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности криптографическими средствами с учетом установленных требований;

установка, настройка, эксплуатация и поддержание в работоспособном состоянии защищенных с использованием криптографических средств информационных систем с учетом установленных требований;

обслуживание СКЗИ и защищенных с использованием СКЗИ информационных систем.

3. Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение по программе профессиональной переподготовки, - высшее образование, по направлению подготовки в области математических и естественных наук, инженерного дела, технологий и технических наук в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации в соответствии с частью 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», подтвержденный документом об образовании.

4. Планируемые результаты обучения

Процесс освоения программы профессиональной переподготовки направлен на формирование у слушателей следующих компетенций:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области технической и криптографической защиты информации в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области технической и криптографической защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации.

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать и организовывать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность организовывать мероприятия по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ на объектах информатизации;

способность проводить аттестационные испытания и аттестацию объектов информатизации по требованиям безопасности информации;

способность принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

способность организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации.

в проектной деятельности:

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов на объекте информатизации, целей и задач деятельности объекта защиты;

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);

способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации).

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;

способность проводить работы по устранению неисправностей и ремонту (техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации;

способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

способность принимать участие в эксплуатации подсистем управления информационной безопасностью объекта защиты.

В результате освоения программы профессиональной переподготовки слушатель получит знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности и решения задач при осуществлении лицензируемых видов деятельности в области ТЗКИ, определенных Постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. № 541), в области СКЗИ (средств криптографической защиты информации), определенных Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 "Об

утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…».

Программа предназначена для профессиональной переподготовки руководителей и уполномоченных руководить работами по лицензируемым видам деятельности, специалистов (инженерно-технических работников) структурных подразделений в области ТЗКИ от утечки по техническим каналам, в области ТКЗИ от НСД, в том числе занимающихся вопросами обеспечения информационной безопасности, криптографической, физической и правовой защиты информации на объектах информатизации, включающих в себя компьютерные системы.

Освоившие программу должны:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

нормативные руководящие документы, касающиеся защиты информации;

основы функционирования государственной системы противодействия (ПД) иностранным техническим разведкам (ИТР) и ТЗИ, цели и задачи ТЗКИ;

виды конфиденциальной информации, перечни сведений конфиденциального характера;

виды угроз информационной безопасности;

возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ;

типовую структуру, задачи и полномочия подразделения по ТЗИ; принципы работы основных узлов современных технических средств информатизации;

основы построения информационных систем и формирования информационных

ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей;

типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от утечки по техническим каналам, несанкционированных, непреднамеренных воздействий, контроля целостности информации;

порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;

методы и методики контроля (мониторинга) защищенности конфиденциальной информации;

порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;

порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации;

порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства;

программы и методики аттестационных испытаний и аттестации объекта информатизации на соответствие требованиям по защите информации;

порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

порядок устранения неисправностей и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

основные понятия и определения из области обеспечения информационной безопасности;

типы каналов утечки информации;

методы криптографической защиты;

порядок подбора средств защиты информации.

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; формировать требования по ТЗКИ;

определять требования к средствам ТЗКИ на объектах информатизации; организовывать и проводить работы по ТЗКИ;

организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний;

разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации;

осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных;

проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган;

выполнять анализ способов нарушений информационной безопасности;

планировать организационные мероприятия, проводимые при защите информации;

использовать методы и средства криптографической защиты информации.

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ;

выявления ТКУИ и определения угроз безопасности информации;

определения задач, проведения организационных и технических мероприятий по

ТЗКИ;

определения задач проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

применения средств ТЗКИ и средств контроля(мониторинга) эффективности мер защиты информации;

работы в компьютерных сетях с учетом требований по безопасности информации;

работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения, в том числе зарубежными информационными ресурсами;

проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации, оформления материалов аттестационных испытаний;

организации деятельности подразделений и специалистов в области ТЗКИ;

проведения установки, монтажа, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранения неисправности и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

защиты информации на предприятиях как с использованием шифровальных (криптографических) средств, так и с использованием иных технических и программных средств защиты;

установки и настройки криптографических средств защиты информации;

проведения контроля защищенности информации от несанкционированного доступа в соответствии с требованиями действующих нормативных методических документов;

администрирования криптографических средств защиты информации.

Все знания, умения и навыки, полученные в процессе обучения слушатель будет применять в своей дальнейшей профессиональной деятельности.

5. Условия реализации программы

Реализация программы профессиональной переподготовки обеспечивается руководящими и научно-педагогическими работниками организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Все научно-педагогические работники, участвующие в реализации программы профессиональной переподготовки, имеют образование, соответствующее профилю преподаваемой дисциплины, конкретный опыт реализации научно-прикладных разработок или иной формы практической деятельности в области информационной безопасности.

Программа профессиональной переподготовки реализуется квалифицированными кадрами с учеными степенями и званиями в области информационной безопасности. Уровень квалификации работников АНО ДПО «Парадигма» соответствует квалификационным характеристикам по соответствующим должностям.

Учебный процесс по реализуемым Учебным центром образовательным программам осуществляют 5 преподавателей, из них 1 доктор юридических наук, 1 кандидат технических наук, 1 аспирант. В преподавательский состав входят высококвалифицированные преподаватели, имеющие большой практический опыт в области информационной безопасности. Доля работников из числа руководителей и работников учебного центра, деятельность которых связана с направленностью (профилем) реализуемой программы и имеющих стаж работы в данной профессиональной области не менее 3 лет составляет 80%.

Педагогические работники АНО ДПО «Парадигма» проходят повышение квалификации и/или профессиональную переподготовку не реже одного раза в пять лет в образовательных учреждениях, имеющих лицензию на право ведения данного вида образовательной деятельности, в том числе с использованием современных дистанционных образовательных технологий.

Чтение лекций по дисциплине проводится преимущественно с использованием электронных мультимедийных презентаций. При работе используется диалоговая форма ведения лекций с постановкой и решением проблемных задач, современных поправок в законодательстве Российской Федерации, обсуждением дискуссионных моментов и т.д.

Использование презентации позволяет преподавателю чётко структурировать материал лекции, экономить время, затрачиваемое на рисование схем, диаграмм и других сложных графических объектов, что позволяет значительно увеличить объем излагаемого материала без потери его качества. Помимо этого, презентация позволяет очень хорошо иллюстрировать лекцию не только схемами и рисунками, но и цветными фотографиями.

Лекционные, практические и лабораторные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном

порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места слушателей оснащены современным оборудованием, стендами, приборами, лицензионным программным обеспечением, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером, мультимедийным проектором, экраном, доской.

Слушатели обеспечиваются комплектом учебно-методических и раздаточных материалов, а также иными информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляется возможность копирования материала для самоподготовки и подготовки к зачету.

При проведении лабораторных занятий создаются условия для максимально самостоятельного выполнения лабораторных работ. Проведение каждой лабораторной работы включает четыре этапа:

Постановка целей и задач лабораторной работы. Демонстрация и разбор примера.

Выполнение лабораторной работы.

Демонстрация результатов выполнения лабораторной работы и разбор ошибок.

Устранение ошибок и оценивание выполненной работы.

Каждая лабораторная работа включает самостоятельную проработку теоретического материала, изучение методики и технологий решения задачи, приобретение навыка решения задач по управлению данными.

При проведении самостоятельных работ используются следующие формы:

решение слушателем самостоятельных задач обычной сложности, направленных на закрепление знаний и умений;

выполнение самостоятельных работ, направленных на развитие у слушателей мышления и инициативы.

Для осуществления образовательной деятельности Учебный центр располагает необходимыми аудиторными помещениями, обеспечивающими качественную подготовку специалистов. Разрешения органов государственного противопожарного надзора и государственного санитарно-эпидемиологического надзора на все используемые площади имеются. Количество лекционных аудиторий, классов для проведения семинарских и практических занятий – достаточное. Санитарные и гигиенические нормы Учебным центром выполняются, уровень обеспечения безопасности слушателей и работников соответствует установленным требованиям.

Слушателям обеспечен доступ к помещениям, оснащенным компьютерной техникой, в том числе с возможностью подключения к сети Интернет, для самостоятельной работы.

Все учебные аудитории специально оборудованы современными средствами визуализации: доски, видео- и аудиоаппаратура, сетевые подключения локальной компьютерной сети с выходом в Интернет для проведения занятий в формате лекций и семинаров. Для проведения практических занятий, проверки знаний.

Каждый слушатель может воспользоваться учебно-методическими материалами, помогающими организовать его самостоятельную работу при подготовке к итоговой аттестации. Все материалы доступны слушателям на электронных носителях.

Все слушатели получают комплект учебных материалов на электронных носителях, которые используются слушателями в процессе обучения, а также в дальнейшей работе.

Учебно-материальная база Учебного центра включает все элементы, позволяющие в полной мере обеспечить учебный процесс по всем дополнительным профессиональным программам.

В АНО ДПО «Парадигма» используется электронно-библиотечная система (электронная библиотека), доступ к необходимым в соответствии с программой модуля изданиям обеспечивается через электронно-библиотечную систему (электронную библиотеку).

Каждый Слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке), содержащей обязательные и дополнительные издания учебной, учебно-методической и иной литературы на портале http://elearning.paradygma.ru/ . Библиотечный фонд учебного центра дополнительно укомплектован печатными изданиями. Фонд дополнительной литературы включает официальные, справочно-библиографические и специализированные отечественные и зарубежные периодические издания, в том числе, правовые нормативные акты и нормативные методические документы в области информационной безопасности.

Перечень основной и дополнительной литературы подлежит обновлению и (или) уточнению АНО ДПО "Парадигма" с учетом введения в действие новых и утративших актуальность нормативных правовых актов и методических документов.

Учебный центр имеет 1 учебную аудиторию вместимостью 32 места для слушателей, оснащенную стационарным мультимедийным оборудованием. Аудитория учебного центра имеет возможность установки дополнительного технического оборудования: мультимедийных проекторов, звукоусиливающей аппаратуры.

Мультимедийное оборудование включает в себя: мультимедийный проектор, проекционный экран, акустическую систему, персональный компьютер, беспроводной

микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI, трибуна преподавателя. Аудитория оснащена высокоскоростным интернетом. Компьютерный класс включает компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети и находятся в едином домене.

Лекционные занятия проводятся в классе, оснащенном компьютером для преподавателя, мультимедийным проектором, экраном, интерактивной доской. При проведении лекционных занятий применяются такие формы как лекции – визуализации, сопровождая изложение теоретического материала презентациями, при этом слушатели заблаговременно обеспечиваются раздаточным материалом.

В процессе преподавания учебных дисциплин в каждом разделе и каждой теме выделяются наиболее важные моменты, и акцентируется на них внимание слушателей.

При проведении лекционных занятий применяются информационные и проблемные лекции, стимулирующие слушателей к самостоятельному поиску решений задач.

При проведении практических и лабораторных занятий ставится цель углубления и закрепления теоретических знаний, овладение методами экспериментальных исследований, в частности, выявления технических каналов утечки информации и характеристик технических средств защиты информации от ее утечки по техническим каналам, привитие навыков анализа полученных результатов исследований.

В период проведения занятий слушателям предоставляется возможность использования Интернет, электронных образовательных ресурсов по соответствующим учебным дисциплинам.

Передача Программы для реализации другой организации не предусматривается.

Допускается внесение изменений в программу профессиональной переподготовки, но не более 10% от общего объема материала, если более, то только по согласованию с ФСТЭК России и ФСБ России.

6. Формы и аттестации и формы оценочных средств

Оценка качества освоения слушателями дополнительной профессиональной программы профессиональной переподготовки «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами» включает текущий контроль знаний, промежуточную и итоговую аттестацию слушателей.

Критерии оценки промежуточной аттестации.

Зачет - ответы на вопросы полностью раскрыты, слушатель способен делать логические и обоснованные выводы. Слушатель свободно ориентируется в материале, владеет терминологией по рассматриваемой проблеме.

Незачет - ответы на вопросы изложены непоследовательно, без соответствующей аргументации и необходимого анализа.

Итоговая аттестация слушателей проводится в форме экзамена. Итоговая аттестация организуется и проводится в соответствии с «Положением об итоговой аттестации АНО ДПО «Учебный центр «Парадигма».

Итоговый экзамен по программе «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами» является формой итоговой аттестации слушателей. Итоговый экзамен по специальности имеет целью определение степени соответствия уровня подготовленности слушателей требованиям данной программы профессиональной переподготовки. При проведении итогового экзамена создается аттестационная комиссия, состав которой утверждается руководителем учебного центра АНО ДПО «Учебный центр «Парадигма».

К итоговой аттестации допускается слушатель, не имеющий задолженности и в полном объеме выполнивший учебный план по программе профессиональной переподготовки.

По результатам итогового экзамена выставляются отметки по пяти - бальной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Отметка «неудовлетворительно» выставляется слушателю, не показавшему освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, допустившему серьезные ошибки в выполнении предусмотренных программой заданий.

Отметка «удовлетворительно» получает слушатель, показавший частичное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, сформированность не в полной мере новых компетенций и профессиональных умений для осуществления профессиональной деятельности, знакомый с литературой по программе.

Отметку «хорошо» заслуживает слушатель, показавший полное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, изучивший рекомендованную программой литературу, способный к самостоятельному пополнению и обновлению знаний в ходе дальнейшего обучения и профессиональной деятельности.

Отметку «отлично» заслуживает слушатель, показавший полное освоение планируемых результатов (знаний, умений, компетенций), всестороннее и глубокое изучение

литературы, публикаций; умение выполнять задания с привнесением собственного видения проблем, своего варианта решения практических задач, проявивший творческие способности в понимании и применении на практике содержания обучения.

Лицам, успешно освоившим программу профессиональной переподготовки «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами» и прошедшим итоговую аттестацию, выдается диплом установленного образца о профессиональной переподготовке с указанием нового вида профессиональной деятельности.

7. Учебный план программы профессиональной переподготовки «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и не криптографическими методами»

7.1. Категория слушателей: специалисты, работающие в области ТЗКИ; руководители и (или) уполномоченные руководить работами по лицензируемому виду деятельности, а также специалисты (инженерно-технических работников) в области криптографической защиты информации.

7.2. Форма и сроки обучения: обучение по программе профессиональной переподготовки осуществляется в очно-заочной (с частичным отрывом от работы) форме.

7.3. Продолжительность обучения устанавливается в соответствии с Приказом Министерства науки и высшего образования Российской Федерации от 19 октября 2020 года №1316[1]: 552 часа (420 аудиторных часов), 15 недель, 4 месяца.

7.4. Режим занятий:

Нагрузка устанавливается не более 40 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Аудиторные занятия проводятся не более 3 раз в неделю.

Для всех видов занятий устанавливается академический час продолжительностью 45 минут.

[1] Приказа Министерства науки и высшего образования Российской Федерации от 19 декабря 2020 г. №1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

План учебного процесса

№ п/п	Наименование учебных дисциплин	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1.	**«Информационная безопасность. Техническая защита конфиденциальной информации»**	**374**	**276**	**58**	**52**	**84**	**82**	**16**	**82**	**-**
1.1.	Организационно-правовые основы ТЗКИ	30	18	6	10	2	-	2	10	Зачет
1.2.	Средства и системы обработки информации	42	32	6	4	8	14	2	8	Зачет
1.3.	Способы и средства ТЗКИ от утечки по техническим каналам	60	46	12	4	6	24	2	12	Зачет
1.4.	Меры и средства ТЗКИ от НСД	60	46	6	4	10	26	2	12	Зачет
1.5.	Техническая защита конфиденциальной информации от специальных воздействий	10	6	2	2	2	-	2	2	Зачет
1.6.	Организация защиты конфиденциальной информации на объектах информатизации	52	38	6	6	26	-	2	12	Зачет
1.7.	Аттестация объектов информатизации по требованиям безопасности информации	48	36	6	4	14	12	2	10	Зачет
1.8.	Контроль состояния ТЗКИ	72	54	14	18	16	6	2	16	Зачет
2.	**«Защита информации ограниченного доступа, не содержащие сведения, составляющие гос. тайну, криптографическими средствами»**	**162**	**140**	**45**	**16**	**44**	**35**	**2**	**20**	**-**
2.1.	Дискретная математика	12	10	8	2	-	-	-	2	-
2.2.	Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации	21	16	8	8	-	-	1	4	Зачет
2.3.	Основные понятия криптографии	6	4	4	-	-	-	-	2	-
2.4.	Криптографические системы с симметричным ключом	10	8	2	-	6	-	-	2	-
2.5.	Криптографические системы с открытым ключом. Электронная подпись	12	10	4	-	6	-	-	2	-
2.6.	Хэш-функции. Обеспечение контроля целостности сообщений	6	4	2	-	2	-	-	2	-
2.7.	Инфраструктура Открытых Ключей (PKI)	20	18	6	-	4	8	-	2	-
2.8.	Криптографические протоколы	12	9	3	6	-	-	1	2	Зачет
2.9.	Обеспечение безопасности информации с использованием СКЗИ	63	61	8	-	26	27	-	2	Зачет
3.	**Итоговая аттестация**	**16**	**4**	**-**	**-**	**-**	**-**	**-**	**12**	**Экзамен**
Итого:		**552**	**420**	**103**	**68**	**128**	**117**	**18**	**116**	**-**

7.5. Сводные данные по бюджету

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практики			
100	30	70/568	552	432	-	104	16	14

8. Календарный учебный график

	Наименование учебной дисциплины	Учебные недели															
		1				2				3				4			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1.	Организационно-правовые основы ТЗКИ	А															
2.	Средства и системы обработки информации	А	А														
3.	Способы и средства ТЗКИ от утечки по техническим каналам		А	А	А												
4.	Меры и средства ТЗКИ от НСД				А	А											
5.	Техническая защита конфиденциальной информации от специальных воздействий					А											
6.	Организация защиты конфиденциальной информации на объектах информатизации						А	А									
7.	Аттестация объектов информатизации по требованиям безопасности информации							А	А								
8.	Контроль состояния ТЗКИ								А	А	А						
9.	Дискретная математика											А					
10.	Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации											А					
11.	Основные понятия криптографии											А					
12.	Криптографические системы с симметричным ключом											А					
13.	Криптографические системы с открытым ключом. Электронная подпись												А				
14.	Хэш-функции. Обеспечение контроля целостности сообщений												А				
15.	Инфраструктура Открытых Ключей (PKI)												А				
16.	Криптографические протоколы													А			
17.	Обеспечение безопасности информации с использованием СКЗИ													А	А		
18.	Итоговая аттестация															И	

9. Рабочая программа учебной дисциплины «Организационно-правовые основы технической защиты конфиденциальной информации»

9.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам организационно-правовых основ в области ТЗКИ.

9.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина является вводной в программу профессиональной переподготовки. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации», «Контроль состояния ТЗКИ».

9.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность организовывать мероприятия по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;

в проектной деятельности:

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности;

конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

В результате освоения дисциплины слушатель получит знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

основы функционирования государственной системы ПД ИТР и ТЗИ, цели и задачи ТЗКИ;

виды конфиденциальной информации, перечни сведений конфиденциального характера;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ;

типовую структуру, задачи и полномочия подразделения по ТЗИ; технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

порядок проведения мониторинга информационной безопасности средств и систем информатизации;

порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

организовывать и проводить работы по ТЗКИ;

организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ;

определения задач, проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения, в том числе зарубежными информационными ресурсами;

организации деятельности подразделений и специалистов в области ТЗКИ.

9.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 30 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	18
лекции (Л)	6
практические занятия (ПЗ)	2
семинары (С)	10
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	10
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	30

9.5. Содержание учебной дисциплины

9.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Цели и задачи ТЗКИ	Основные термины и определения в области ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗКИ. Объекты информатизации: классификация и характеристика. Защищаемые информация и информационные ресурсы. Объекты защиты конфиденциальной информации. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций. Перечень сведений конфиденциального характера, подлежащих защите. Угрозы безопасности конфиденциальной информации. Классификация ТКУИ. Классификация угроз безопасности информации, связанных с НСД. Модель угроз безопасности информации в заданных условиях функционирования объекта зашиты. Методы выявления и оценки возможности реализации угроз безопасности информации.
2.	Основы нормативного правового обеспечения ТЗКИ	Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Стандарты Единой системы конструкторской документации (ЕСКД), Единой системы технологической документации (ЕСТД) и Единой системы программной документации (ЕСПД). Основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации. Требования по защите конфиденциальной информации на объекте информатизации (от утечки по техническим каналам, от НСД и специальных воздействий). Особенности защиты персональных данных. Требования международных и национальных стандартов по защите информации.

9.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин	
		1	2
1.	Средства и системы защиты информации	+	+
2.	Способы и средства ТЗКИ от утечки по техническим каналам	+	+
3.	Меры и средства ТЗКИ от НСД	+	+
4.	Техническая защита конфиденциальной информации от специальных воздействий	+	+
5.	Организация защиты конфиденциальной информации на объектах информатизации	+	+
6.	Аттестация объектов информатизации по требованиям безопасности информации	+	+
7.	Контроль состояния ТЗКИ	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

9.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Цели и задачи ТЗКИ	2	-	-	2	4	8
2.	Основы нормативного правового обеспечения ТЗКИ	4	2	-	8	6	20

9.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

9.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Информация как объект защиты. Цели и задачи ТЗКИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации	2
2.	2	Нормативные правовые акты и методические документы ФСТЭК России в области ТЗИ	2
3.	2	Стандарты ЕСКД, ЕСТД и ЕСПД	2
4.	2	Организационно-правовые основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации	2
5.	2	Требования по ТЗКИ	2

9.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	2	Подготовка документов для получения лицензии на проведение работ и оказания услуг по ТЗКИ	2

9.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности. В 2-х ч. Ч.1. Правовое обеспечение информационной безопасности: учеб. пособие. - М.: МИЭТ, 2013 г. - 184 с.

2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч. Ч. 2. Организационное обеспечение информационной безопасности: учеб. пособие. - М.: МИЭТ, 2013 г. - 172 с.

3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / под ред. А.А. Стрельцова. - М.: Академия, 2008 г. - 256 с.

4. Семкин С.Н., Семкин А.Н. Основы правового обеспечения защиты информации: учеб. пособие для вузов. - М.: Горячая линия - Телеком, 2008 г.

5. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учеб. пособие / Ю.Ю. Коваленко. - М.: Горячая линия - Телеком, 2012 г.

Дополнительная литература:

1. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005 г.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об

утверждении Доктрины информационной безопасности Российской Федерации».

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

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

10. 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».

11. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. № 541).

12. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171 (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. № 541).

13. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

14. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

17. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. № 134.

19. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 17

июля 2017 г. № 133.

20. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

21. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

22. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.

23. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

24. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

25. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

26. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

27. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008 г.

28. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

29. Приказ ФСТЭК России № 55 «Об утверждении Положения о системе сертификации средств защиты информации» от 3 апреля 2018 г.

30. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006 г.

31. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013 г.

32. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014 г.

33. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000 г.

34. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006 г.

35. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005 г.

36. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Госстандарт, 2013 г.

37. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993 г.

38. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998 г.

39. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Росстандарт, 2008 г.

40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014 г.

41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014 г.

42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012 г.

43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

технологий. Часть 2. Функциональные компоненты безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013 г.

44. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности (прямое применение ISO/IEC 15408-3:2008). Росстандарт, 2013 г.

45. ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021 г.

46. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2021 г.

47. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. Росстандарт, 2022 г.

48. ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации. Росстандарт, 2022 г.

49. ГОСТ 34.602-2020 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Росстандарт, 2021 г.

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

51. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

52. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

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

54. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами

беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

55. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

56. Указ Президента Российской Федерации № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» от 5 декабря 2016 г.

57. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76

58. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утверждена ФСТЭК России 25 декабря 2020 г.

59. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

60. Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах. Утверждены приказом ФСТЭК России от 16 февраля 2021 г. №32.

61. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. №77.

Программное обеспечение

Не требуется.

Базы данных, информационно-справочные и поисковые системы:

Правовые справочно-поисковые системы («Гарант», «Консультант Плюс»);

www.fstec.ru;

www.gost.ru/wps/portal/tk362;

bdu.fstec.ru.

9.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, интерфейсами подключения: USB, audio, HDMI, трибуной преподавателя.

9.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основы нормативного правового обеспечения ТЗИ. В процессе изучения учебной дисциплины упор делается на изучение нормативной правовой базы в области ТЗИ, системы стандартизации Российской Федерации и системы документов ФСТЭК России.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗКИ, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы Слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения работать с действующей нормативной правовой и методической базой в области ТЗИ; работать с правовыми базами данных, базами данных, а также формируются навыки реализации требований нормативных и методических документов, а также действующего законодательства по вопросам защиты конфиденциальной информации.

9.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей.

Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в

Российской Федерации.

Цели и задачи ТЗКИ.

Объекты информатизации: классификация и характеристика.

Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий.

Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России.

Методические документы в области ТЗКИ.

Технические документы (документация) в области ТЗКИ.

Плановые документы в области ТЗКИ.

Информационные документы в области ТЗКИ.

Национальные и международные стандарты в области защиты информации.

Стандарты ЕСКД, ЕСТД и ЕСПД.

Лицензионные виды деятельности по ТЗКИ.

Требования по защите акустической речевой информации.

Требования по защите конфиденциальной информации, обрабатываемой в автоматизированных (информационных) системах.

Требования по защите персональных данных.

Правила оформления документов для получения лицензии на проведение работ и оказания услуг по ТЗКИ.

10. Рабочая программа учебной дисциплины «Средства и системы обработки информации»

10.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков, связанных с использованием аппаратных средств и систем обработки информации.

10.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, будут использоваться при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации», «Контроль состояния ТЗКИ».

10.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в проектной деятельности:

способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);

способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность проводить работы по устранению неисправностей и ремонту

(техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Слушатель должен:

а) знать:

принципы работы основных узлов современных технических средств информатизации;

основы построения информационных систем и формирования информационных ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей;

типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами;

порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;

порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

порядок устранения неисправностей и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

б) уметь:

определять требования к средствам ТЗКИ на объектах информатизации;

осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных;

проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности защиты конфиденциальной информации;

устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы в компьютерных сетях с учетом требований по безопасности информации;

установки, монтажа, испытаний и технического обслуживания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранения неисправности и проведения ремонта (технического обслуживания)

средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации.

10.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 42 часа.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	32
лекции (Л)	6
практические занятия (ПЗ)	8
семинары (С)	4
лабораторные работы (ЛР)	14
Самостоятельная работа (СР, всего)	8
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	42

10.5. Содержание учебной дисциплины

10.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Технические средства обработки информации	Информация: основные термины и определения. Сбор и обработка информации. Информационные процессы. Технические средства обработки информации. Классификация технические средства обработки информации. Устройства хранения информации. Устройства памяти. Виды памяти. Основные типы и принцип работы клавиатуры, манипулятора «мышь», джойстика и др. устройств. Основные типы, принципы работы и технические характеристики мониторов. Типы, основные компоненты и характеристики видеоадаптеров. Принцип (способы) формирования изображения. Классификация сканеров. Обзор основных современных моделей сканеров и их технических характеристик. Назначение и краткая характеристика сетевого оборудования: кабельная система, сетевые адаптеры, концентраторы, коммутаторы, принт-серверы. Типы модемов, принцип и режимы работы. Основные принципы установки, монтажа, наладки и ремонта технических средств обработки информации.
2.	Информационные технологии	Понятие операционной системы. Структура операционной системы. Основные компоненты операционной системы. Понятие ядра операционной системы. Понятия прерывания и процедуры обработки прерывания. Системные вызовы. Установка операционной системы. Взаимодействие пользователя с операционной системы. Основные понятия и классификация программного обеспечения. Использование программных средств системного и прикладного назначения (форматирования, дефрагментации, архивации, антивирусной защиты и т.д.). Резервное копирование и восстановление системы. Основы администрирования операционной системы. Основы программирования. Синтаксис команд. Использование переменных. Команды для работы с файлами и каталогами. Организация файловых

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		систем. Назначение основных системных каталогов. Типы файлов. Права доступа к файлам и каталогам. Физическая реализация файловой системы. Понятие командной оболочки. Обзор командных интерпретаторов.
3.	Вычислительные сети, сети и системы передачи информации	Вычислительные системы и системы передачи информации. Локальные и глобальные вычислительные сети и системы передачи информации. Модель взаимодействия открытых систем (OSI). Программное обеспечение, поддерживающее работу сети. Оборудование, предназначенное для объединения локальных вычислительных сетей. Технология управления взаимодействием в сети. Обобщенная структура и функции глобальных компьютерных сетей. Технология Ethernet, основные услуги и сервисы сети. Организация и сервис виртуальных частных сетей (VPN). Сети и средства связи: передатчики, приемники, источники излучения, модуляторы, демодуляторы, усилители. Основные типы и принцип работы сетей и средств связи. Радиорелейные линии и спутниковые системы связи Волоконно-оптические системы передачи информации. Структура сети GSM. Подсистема базовой станции, регистры HLR и VLR, центр коммутации подвижной связи, центр аутентификации и регистр идентификации оборудования. Системы связи, построенные с использованием технологии 3G и 4G. Основные сетевые компоненты. Телекоммуникационные системы. Понятие о цифровых системах передачи информации. Формирование группового сигнала. Синхронизация и регенерация (восстановление) цифровых сигналов. Синхронная цифровая иерархия. Асинхронный режим передачи. Сигналы PDH и SDH. Сети интегрального обслуживания. Виртуальные каналы в глобальных сетях, сети передачи данных на основе технологий X.25, FRAME RELAY, ATM. Протокол межсетевого взаимодействия IP. Адресная схема протокола, маршрутизация, маска подсети, расширенный сетевой префикс. Протоколы транспортного уровня TCP и UDP. Протоколы маршрутизации в стеке TCP/IP: протокол OSPF, протоколы политики маршрутизации EGP и BGP. протоколы групповой маршрутизации MBONE, DVMRP, MOSPF и PIM. Услуги телефонной сети общего пользования. Протокол SIP. Мультисервисная сеть связи. Состав оборудования. Цифровые сети интегрального обслуживания (сети ISDN). Широкополосные цифровые сети интегрального обслуживания. Перспективы развития телекоммуникационных систем в России и за рубежом.

10.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин		
		1	2	3
1.	Способы и средства ТЗКИ от утечки по техническим каналам	+	+	+
2.	Меры и средства ТЗКИ от НСД	+	+	+
3.	Техническая защита конфиденциальной информации от специальных воздействий	+	+	+
4.	Организация защиты конфиденциальной информации на объектах информатизации	+	+	+
5.	Аттестация объектов информатизации по требованиям безопасности информации	+	+	+
6.	Контроль состояния ТЗКИ	+	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

10.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Технические средства обработки информации	2	2	4	-	2	10
2.	Информационные технологии	2	-	4	2	2	10
3.	Вычислительные сети, сети и системы передачи информации	2	6	6	2	4	20

10.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	1	Представление информации и основы работы технических средств обработки информации	2
2.	1	Выбор и замена основных элементов средств обработки информации. Настройка периферийных устройств	2
3.	2	Установка, настройка, устранение неисправностей системного и прикладного программного обеспечения	4
4.	3	Установка, настройка и ремонт технических средств обработки информации	4
5.	3	Технические устройства, выполняющие функции сопряжения средств обработки информации с каналами связи, особенности их технического обслуживания	2

10.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	2	Системы связи, построенные с использованием технологии 3G и 4G	2
2.	3	Модель взаимодействия открытых систем (OSI)	2

10.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Типы устройств хранения информации и их носители	2
2.	3	Телекоммуникационное оборудование. Способы организации двухсторонней связи систем передачи информации	2
3.	3	Использование программных средств системного и прикладного назначения	2
4.	3	Стандарты Hiperlan. Wi-Fi, WiMax	2

10.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Аппаратные средства вычислительной техники: учеб. пособие / Е.И. Шкелев. - Н. Новгород: Изд-во Нижегородского государственного университета, 2011 г. - 222 с.

2. Аппаратные средства вычислительной техники: учебник / В.А. Минаев [и др.]. - Орел: ГТУ ОГУ, 2010 г. - 461 с.

3. Аппаратные средства вычислительной техники: учебник для студентов вузов: в 2-х кн. / В.А. Минаев [и др.]; Орловский государственный университет. - Орел: ГУУНПК, 2011г.

Дополнительная литература:

1. Корнеев В.В. Вычислительные системы. - М.: Гелиос-АРВ, 2004 г.

2. Таненбаум Э. Архитектура компьютера. - 5-е изд. - СПб: Питер, 2007 г.

3. Таненбаум Э. Распределенные системы. Принципы и парадигмы. - Спб: Питер, 2003 г.

4. Лацис А.О. Параллельная обработка данных: учеб. пособие. - М.: Академия, 2010г.

5. Хорошевский В.Г. Архитектура вычислительных систем. - М.: МГТУ им. Н.Э. Баумана, 2008 г.

Программное обеспечение:

системное и прикладное программное обеспечение;

операционные системы: Windows, Unixx, Linux; драйверы, оболочки, утилиты.

Базы данных, информационно-справочные и поисковые системы:

http://parallel.ru - Информационно-аналитический центр по параллельным вычислениям;

http://gridclub.ru - Интернет-портал по грид-технологиям.

10.10. Материально-Техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, интерфейсами подключения: USB, audio, HDMI, трибуной преподавателя.

Для проведения лабораторных работ и практических занятий есть специализированная лаборатория, оборудованная средствами вычислительной техники (СВТ), локальная вычислительная сеть. Подключение к сети Интернет.

10.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются наиболее важные и сложные вопросы, являющиеся основой в изучении ЭВМ и вычислительных систем.

Практическая часть учебной дисциплины отрабатывается на практических занятиях и в ходе лабораторных работ. На практических занятиях развиваются умения определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. В ходе выполнения лабораторных работ формируются навыки работы с современными операционными системами, восстановления операционных систем после сбоев; установки и настройки современных операционных систем с учетом требований по безопасности информации.

Лабораторные работы и практические занятия по демонстрации аппаратных средств ЭВМ, систем передачи данных, способов их использования в процессе эксплуатации объектов информатизации проводятся в специализированной лаборатории (компьютерном

классе с предварительной установкой необходимого программного обеспечения и оборудованной локальной вычислительной сетью). Занятия проводятся на 4-8 рабочих местах (количество рабочих мест зависит от количества слушателей в учебной группе).

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы слушатели получают консультации у преподавателей.

10.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Основные виды и назначение системного программного обеспечения.

Основные виды и назначение прикладного программного обеспечения.

Понятия кодирования и декодирования информации.

Системы счисления: позиционные и непозиционные; двоичные, десятичные, шестнадцатеричные.

Международные системы байтового кодирования.

Растровые и векторные методы представления цветного изображения.

Типы устройств хранения информации и их носители.

Физическая сущность форматирования носителей информации, создания и удаления файлов, папок (каталогов).

Автоматизированные рабочие места.

Способы объединения технических средств обработки информации в сетевых технологиях.

Технические устройства, выполняющие функции сопряжения технических средств обработки информации с каналами связи.

Оборудование, предназначенное для объединения локальных вычислительных сетей.

Технология IntraNet.

11. Рабочая программа учебной дисциплины «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам»

11.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам ТЗКИ от утечки по техническим каналам.

11.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации», «Контроль состояния ТЗКИ».

11.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение слушателями компетенций:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность организовывать мероприятия по контролю (мониторингу) защищенности

конфиденциальной информации на объектах информатизации;

в проектной деятельности:

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов на объекте информатизации, целей и задач деятельности объекта защиты;

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);

способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность проводить работы по устранению неисправностей и ремонту (техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых Слушателями в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ от утечки по техническим каналам;

виды конфиденциальной информации, перечни сведений конфиденциального характера;

возможные ТКУИ;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения) от утечки по техническим каналам;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации от утечки по техническим каналам, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ от утечки по техническим каналам;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы и требования по ТЗКИ от утечки по техническим каналам; подсистемы защиты информации от утечки по техническим каналам;

порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

порядок устранения неисправностей и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ от утечки по техническим каналам;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ от утечки по техническим каналам; определять возможные ТКУИ;

формировать требования по ТЗКИ от утечки по техническим каналам; определять требования к средствам ТЗКИ от утечки по техническим каналам;

организовывать и проводить работы по ТЗКИ от утечки по техническим каналам;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам;

проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам;

устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ от утечки по техническим каналам;

выявления ТКУИ;

определения задач, проведения организационных и технических мероприятий по ТЗКИ от утечки по техническим каналам;

определения задач, проведение организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации от утечки по техническим каналам, подготовки материалов по результатам контроля;

применения средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам;

проведения установки, монтажа, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам;

устранения неисправности и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам.

11.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 60 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	46
лекции (Л)	12
практические занятия (ПЗ)	6
семинары (С)	4
лабораторные работы (ЛР)	24
Самостоятельная работа (СР, всего)	12
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	60

11.5. Содержание учебной дисциплины

11.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Технические каналы утечки информации	Нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ, цели и задачи ТЗКИ. Термины и определения в области ТЗКИ от утечки по техническим каналам: объект информатизации, защищаемое помещение, основные технические средства и системы (ОТСС), вспомогательные технические средства и системы (ВТСС), случайные антенны, контролируемая зона, ТКУИ. Физические основы возникновения ТКУИ и общая характеристика ТКУИ, обрабатываемой техническими средствами. Технический канал утечки информации за счет побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ). Схема ТКУИ, возникающего за счет ПЭМИ СВТ. Характеристики ПЭМИ СВТ в различных режимах работы. Зона 2. Принципы построения средств перехвата ПЭМИ СВТ. Технический канал утечки информации за счет наводок, возникающих под воздействием ПЭМИ СВТ. Случайные антенны. Характеристики случайных антенн. Схема ТКУИ, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Зона 1. Просачивание сигналов в линии электропитания и заземления СВТ. Схемы ТКУИ, возникающих за счет просачивания информативных сигналов в линии электропитания и заземления СВТ. Технический канал утечки информации, использующий электронные устройства съема информации («закладочные устройства»), внедряемые в СВТ. Физические основы возникновения технических каналов утечки акустической речевой информации. Акустические сигналы. Спектр и типовые уровни речевого сигнала. Классификация технических каналов утечки акустической речевой информации. Прямой акустический канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата информации по прямому акустическому каналу. Средства перехвата акустической речевой информации, использующие микрофоны воздушной проводимости. Вибрационный канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата акустической речевой информации по вибрационному каналу. Средства перехвата акустической речевой информации, использующие вибропреобразователи. Оптико-электронный канал утечки акустической речевой информации из защищаемых помещений. Схема перехвата акустической речевой информации по оптико-электронному каналу. Средства перехвата акустической речевой информации, использующие «лазерные микрофоны». Акустоэлектрический канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектрического канала утечки акустической речевой информации. Схема активного акустоэлектрического канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектрического преобразования речевого сигнала.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		Акустоэлектромагнитный канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектромагнитного канала утечки акустической речевой информации. Схема активного акустоэлектромагнитного канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектромагнитного преобразования речевого сигнала Каналы утечки акустической речевой информации, использующие высокочастотные генераторы.
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок	Классификация способов и средств защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Способы и средства пассивной защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Экранирование технических средств и их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Поглощение электромагнитных волн. Безэховые камеры, поглощающие чехлы и накидки. Способы и средства активной защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Системы пространственного электромагнитного зашумления. Требования к системе пространственного электромагнитного зашумления. Основные характеристики систем пространственного электромагнитного зашумления. Системы линейного электрического зашумления. Требования к системе линейного электрического зашумления. Основные характеристики систем линейного электрического зашумления. Особенности зашумления инженерных коммуникаций. Требования к системам электроснабжения и заземления ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. Способы и средства защиты информации от утечки по цепям электроснабжения и заземления. Установка, монтаж, настройка, испытания, ремонт и техническое обслуживание средств защиты информации от утечки за счет ПЭМИН. Устранение неисправностей и организация ремонта средств защиты информации от утечки за счет ПЭМИН.
3.	Способы и средства защиты акустической речевой информации от утечки по техническим каналам	Классификация способов и средств защиты акустической речевой информации от утечки по техническим каналам. Способы и средства пассивной защиты акустической речевой информации от утечки по техническим каналам. Звукоизоляция и экранирование защищаемых помещений, звукопоглощающие материалы. Способы и средства пассивной защиты акустической речевой информации от утечки по акустоэлектрическим каналам, каналам ВЧ-навязывания и ВЧ-прокачки (ограничение сигналов по амплитуде, установка НЧ- фильтров в соединительных линиях

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		ВТСС, отключение акустоэлектрических преобразователей сигналов). Способы и средства активной защиты акустической речевой информации от утечки по техническим каналам. Акустическая и вибро-акустическая маскировка. Требования к системе вибро-акустической защиты. Системы и средства вибро-акустической защиты. Особенности установки акустических излучателей и вибро-излучателей. Способы и средства активной защиты акустической речевой информации от утечки по акустоэлектрическому каналу, каналам ВЧ-навязывания и ВЧ-прокачки. Специальные технические средства подавления электронных устройств негласного получения акустической речевой информации, порядок их установки и настройки. Установка, монтаж, настройка, испытание, ремонт и техническое обслуживание средств защиты акустической речевой информации от утечки по техническим каналам. Устранение неисправностей и организация ремонта средств защиты акустической речевой информации от утечки по техническим каналам.

11.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин		
		1	2	3
1.	Меры и средства ТЗКИ от НСД	+	+	+
2.	Техническая защита конфиденциальной информации от специальных воздействий	+	+	+
3.	Организация защиты конфиденциальной информации на объектах информатизации	+	+	+
4.	Аттестация объектов информатизации по требованиям безопасности информации	+	+	+
5.	Контроль состояния ТЗКИ	+	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

11.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование раздела учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Технические каналы утечки информации	4	2	8	2	4	20
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	4	2	8	1	4	19
3.	Способы и средства защиты акустической речевой информации от утечки по техническим каналам	4	2	8	1	4	19

11.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	1	Исследование ПЭМИН СВТ	4
2.	1	Исследование акустических каналов утечки информации	4
3.	2	Исследование основных характеристик систем пространственного электромагнитного и линейного электрического зашумления. Установка и настройка систем пространственного электромагнитного и линейного электрического зашумления	4
4.	2	Исследование характеристик помехоподавляющих фильтров	4
5.	3	Исследование характеристик системы вибрационной защиты. Установка и настройка системы вибрационной защиты	4
6.	3	Исследование характеристик средств защиты акустической речевой информации	4

11.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Технические каналы утечки информации	2
2.	2,3	Способы и средства защиты информации от утечки по техническим каналам	2

11.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Определение возможных ТКУИ на объектах информатизации	2
2.	2	Определение и устранение основных неисправностей систем пространственного электромагнитного и линейного электрического зашумления	2
3.	3	Определение и устранение основных неисправностей средств защиты информации от утечки акустической речевой информации	2

11.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Меньшаков Ю.К. Теоретические основы технических разведок. - М.: МГТУ им. Н.Э. Баумана, 2008 г.

2. Технические средства и методы защиты информации: учеб. пособие для студентов вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков [и др.]; под ред. А.П. Зайцева, А.А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия - Телеком, 2009 г.

3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. - М.: Аналитика, 2010 г.

4. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, 2008 г.

Дополнительная литература:

1. Защита информации от утечки по информации техническим каналам: учеб. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. - М.: Горячая линия - Телеком, 2005 г.

2. Меньшаков Ю.К. Виды и средства иностранных технических разведок / под ред. М.П. Сычева. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2009 г.

3. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров, В.Б. Голованов [и др.]. - М.: БДЦ-пресс, 2006 г.

4. Зегжда Д.П. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000 г.

5. Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. - М.: Радио и связь, 2000 г.

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы

Федеральной службы по техническому и экспортному контролю».

7. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

8. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

9. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

10. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993 г.

11. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006 г.

12. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006 г.

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

14. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Программное обеспечение

Специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники.

Базы данных, информационно-справочные и поисковые системы

www.fstec.ru;

bdu.fstec.ru;

www.gost.ru/wps/portal/tk362.

11.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, интерфейсами подключения: USB, audio, HDMI, трибуной преподавателя.

Для проведения лабораторных работ и практических занятий есть специализированная лаборатория, оборудованная:

средствами вычислительной техники (СВТ);

локальной вычислительной сетью;

анализатором спектра R&S FPH (1321.1111K02) 5 кГц-2ГГц, с опцией HA-Z220;

набором антенн электрических и магнитных: антенна измерительная рабочная АИР3-2, антенна измерительная дипольная АИ5-0;

генераторами пространственного и линейного зашумления: генератор сигналов низкочастотный ГЗ-131, генератор СПФ АКИП-3409/1;

комплектом аппаратуры для проведения акустических и вибрационных измерений: Четырехканальный шумометр, виброметр, анализатор спектра «Экофизика-110А» (исполнение «HF»), Микрофон М-201;

комплектом средств ТЗИ для демонстрации способов защиты информации от утечки по техническим каналам: Соната –Р2, Соната-АВ», модель 3м;

подключением к сети Интернет.

11.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся фундаментальной основой практических рекомендаций по мерам и средствам, используемым для ТЗИ объектов информатизации.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития

навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗКИ, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Умения и навыки организации внедрения способов и средств защиты конфиденциальной информации от утечки по техническим каналам отрабатываются на лабораторных работах.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы слушатели получают консультации у преподавателей.

11.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Способы перехвата акустической речевой информации из защищаемых помещений по прямому акустическому каналу.

Способы перехвата акустической речевой информации из защищаемых помещений по вибрационным каналам.

Способы перехвата акустической речевой информации из защищаемых помещений по акустооптическому каналу.

Способы перехвата акустической речевой информации из защищаемых помещений по акустоэлектрическим каналам.

Классификация способов и средств защиты конфиденциальной информации от утечки по техническим каналам.

Пассивные способы и средства защиты конфиденциальной информации от утечки по техническим каналам.

Активные способы и средства защиты конфиденциальной информации от утечки по техническим каналам.

Основные характеристики систем линейного электрического зашумления.

Способы и средства защиты конфиденциальной информации от утечки по цепям электропитания и заземления.

Средства защиты акустической речевой информации.

Средства защиты акустической речевой информации от утечки по акустоэлектрическим каналам в ВТСС.

Пассивные способы защиты акустической речевой информации от утечки по акустоэлектрическим каналам в ВТСС.

Активные способы защиты акустической речевой информации от утечки по акустоэлектрическим каналам в ВТСС.

Принципы построения средств защиты конфиденциальной информации ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот.

Принципы построения средств защиты конфиденциальной информации в ВТСС, основанных на отключении акустоэлектрических преобразователей.

Принципы построения средств защиты конфиденциальной информации в ВТСС, основанных на использовании низкочастотных генераторов шума.

12. Рабочая программа учебной дисциплины «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа»

12.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам ТЗКИ от НСД.

12.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, будут использоваться при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации», «Контроль состояния ТЗКИ».

12.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение слушателями компетенций:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ;

способность организовывать мероприятия по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;

в проектной деятельности:

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов на объекте информатизации, целей и задач деятельности объекта защиты;

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);

способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность проводить работы по устранению неисправностей и ремонту (техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых Слушателями в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ от НСД;

виды конфиденциальной информации, перечни сведений конфиденциального характера;

возможные угрозы безопасности информации в результате НСД;

действующую систему сертификации средств защиты информации по требованиям

безопасности информации;

требования по ТЗКИ от НСД (требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по ТЗКИ от НСД, состав и содержание необходимых документов;

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации от НСД, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ от НСД;

методы и требования по ТЗКИ от НСД;

подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от несанкционированных, непреднамеренных воздействий, контроля целостности информации;

порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;

методы и методики контроля (мониторинга) защищенности конфиденциальной информации;

порядок проведения мониторинга информационной безопасности средств и систем информатизации;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

средства ТЗКИ и контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ от НСД;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ от НСД;

определять возможные угрозы безопасности информации в результате НСД и специальных воздействий;

формировать требования по ТЗКИ от НСД;

определять требования к средствам ТЗКИ на объектах информатизации; организовывать и проводить работы по ТЗКИ от НСД;

организовывать и проводить работы по контролю (мониторингу) защищенности

конфиденциальной информации от НСД, оформлять материалы по результатам контроля;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных;

проводить установку и настройку средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранять неисправности средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗКИ;

определение угроз безопасности информации;

определение задач проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации от НСД, подготовки материалов по результатам контроля;

применение средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

работы в компьютерных сетях с учетом требований по безопасности информации;

работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения, в том числе зарубежными информационными ресурсами;

проведения установки, настройки, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранения неисправности средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации.

12.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 60 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	46
лекции (Л)	6
практические занятия (ПЗ)	10
семинары (С)	4
лабораторные работы (ЛР)	26
Самостоятельная работа (СР, всего)	12
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	60

12.5. Содержание учебной дисциплины

12.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Угрозы безопасности информации, связанные с НСД	Понятие и общая классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД. Методы оценки угроз безопасности, выявления уязвимостей в автоматизированных (информационных) системах. Банк данных угроз безопасности информации, содержащий сведения об уязвимостях программного обеспечения, используемого в автоматизированных (информационных) системах. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей информационных систем, базы данных, содержащие описание уязвимостей информационных систем, в том числе CVE. Общая система оценки уязвимостей информационных систем (стандарт CVSS).
2.	Меры и средства защиты информации от НСД	Общая характеристика и классификация мер и средств защиты информации от НСД. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Средства зашиты информации от НСД. Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		целостности информации. Перспективные технологии биометрической аутентификации. Система предотвращения утечки данных, их возможности и перспективы применения. Общий порядок разработки и производства средств защиты информации от НСД. Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности.

12.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин	
		1	2
1.	Техническая защита конфиденциальной информации от специальных воздействий	+	+
2.	Организация защиты конфиденциальной информации на объектах информатизации	+	+
3.	Аттестация объектов информатизации по требованиям безопасности информации	+	+
4.	Контроль состояния ТЗКИ	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

12.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Угрозы безопасности информации, связанные с НСД	2	4	-	2	2	10
2.	Меры и средства защиты информации от НСД	4	6	26	2	10	48

12.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	2	Установка и настройка антивирусных программ	4
2.	2	Установка программно-аппаратного комплекса защиты и его настройка по соответствующему классу защищенности	4
3.	2	Установка и настройка программно-аппаратного комплекса доверенной загрузки	4
4.	2	Установка средств сетевой безопасности и их настройка по классу защищенности	4
5.	2	Инструментальный контроль защищенности автоматизированной системы на соответствие требованиям по защите информации от НСД	4
6.	2	Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры)	4
7.	2	Восстановление системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия	4

12.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем	2
2.	2	Классификация мер и средств защиты информации от НСД (управление доступом, регистрация и учет, обеспечение целостности, антивирусная защита, межсетевое экранирование и сегментирование сетей, анализ защищенности и обнаружение вторжений и т.д.)	2

12.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Разработка модели угроз безопасности информации	4
2.	2	Установка и настройка программных средств формирования и контроля полномочий доступа в информационных (автоматизированных) системах	4
3.	2	Порядок проведения работ, выполняемых при осуществлении контроля защищенности информации от НСД	2

12.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа: пособие. - Воронеж: Кварта, 2015 г. - 440 с.

2. Программно-аппаратная защита информации: учеб. Пособие / П.Б. Хорев. - М.: Форум, 2012 г. - 352 с.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие / В.Ф. Шаньгин. - М.: ДМК Пресс, 2008 г. - 544 с.;

Дополнительная литература:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учеб. пособие / под ред. Ю.Ф. Каторина - СПб: НИУ ИТМО, 2012 г. - 416 с.

2. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. - М.: Финансы и статистика, 2003 г.

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

4. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

5. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008 г.

6. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

7. Приказ ФСТЭК России «Об утверждении Положения о системе сертификации средств защиты информации» от 03.04.2018 г. № 55.

8. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.

9. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

10. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

11. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

12. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

13. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

14. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

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

16. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

Ростехрегулирование, 2006 г.

17. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998 г.

18. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Росстандарт, 2008 г.

19. ГОСТ Р 51275-2006 Зашита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006 г.

20. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014 г.

21. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000 г.

22. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005 г.

23. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Ростехрегулирование, 2006 г.

24. ГОСТ Р 54581-2011/ISO/IEC TR 15443-1:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы. Росстандарт, 2011 г.

25. ГОСТ Р 54582-2011/ISO/IEC TR 15443-2:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия. Росстандарт, 2011 г.

26. ГОСТ Р 54583-2011/ISO/IEC TR 15443-3:2007 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия. Росстандарт, 2011 г.

27. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012 г.

28. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013 г.

29. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

технологий. Часть 3. Компоненты доверия к безопасности (прямое применение ISO/IEC 15408-3:2008). Росстандарт, 2013 г.

30. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Сетевая безопасность. Часть 1. Обзор и концепции. Росстандарт, 2012 г.

31. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий (прямое применение ISO/IEC 18045:2008). Росстандарт, 2013 г.

32. ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021 г.

33. ГОСТ Р ИСО/МЭК 27001-20021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2021 г.

34. ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации. Росстандарт, 2022 г.

35. ГОСТ Р ИСО/МЭК 27004-2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Росстандарт, 2022 г.

36. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции, Госстандарт, 2011 г.

37. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. Ростехрегулирование, 2008 г.

38. Методический документ. Безопасность информационных технологий. Типовые методики оценки профилей защиты и заданий по безопасности. Утвержден ФСТЭК России 16 января 2008 г.

39. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

40. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла первого класса защиты. ИТ.СОВ.У1.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

41. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла второго класса защиты. ИТ.СОВ.У2.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

42. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла третьего класса защиты. ИТ.СОВ.У3.ПЗ. Утвержден ФСТЭК России 12 марта 2012 г.

43. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России 3 февраля 2012 г.

44. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты. ИТ.СОВ.У5.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

45. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла шестого класса защиты. ИТ.СОВ.У6.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

46. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети первого класса защиты. ИТ.СОВ.С1.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

47. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети второго класса защиты. ИТ.СОВ.С2.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

48. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети третьего класса защиты. ИТ.СОВ.С3.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

49. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России 3 февраля 2012 г.

50. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети пятого класса защиты. ИТ.СОВ.С5.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г.

51. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты. ИТ.СОВ.С6.ПЗ. Утвержден ФСГЭК России 6 марта 2012 г.

52. Методический документ. Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты. ИТ.СДЗ.УБ4.ПЗ.

Утвержден ФСТЭК России 30 декабря 2013 г.

53. Методический документ. Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ.ПР4.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г.

54. Методический документ. Профиль защиты средства доверенной загрузки уровня загрузочной записи пятого класса защиты. ИТ.СДЗ.335.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г.

55. Методический документ. Профиль защиты средства доверенной загрузки уровня загрузочной записи шестого класса защиты. ИТ.СДЗ.ЗЗ6.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г.

56. Р 50.1.050-2004 Рекомендации по стандартизации. Защита информации. Система обеспечения качества техники защиты информации. Общие положения. Ростехрегулирование, 2004 г.

57. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

58. Положение о банке данных угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9.

59. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76

60. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утверждена ФСТЭК России 25 декабря 2020 г.

61. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

62. Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах. Утверждены приказом ФСТЭК России от 16 февраля 2021 г. № 32.

63. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Программное обеспечение:

АНО ДПО Учебный центр «Парадигма»

Системы авторизации и аутентификации на базе Windows Active Directory, IPA, средства поиска разрушающих программных воздействий (антивирусные программы) - Антивирус Касперского, Dr.Web, средства анализа трафика вычислительных сетей - Netflow, sflow, средства анализа структуры вычислительных сетей Nmap. Lancope. Система мониторинга состояния сети на базе zabbix.

Базы данных, информационно-справочные и поисковые системы:

www.fstec.ru;

bdu.fstec.ru;

www.gost.ru/wps/portal/tk362.

12.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, интерфейсами подключения: USB, audio, HDMI, трибуной преподавателя.

Для проведения лабораторных работ и практических занятий есть специализированная лаборатория, оборудованная:

средствами вычислительной техники (СВТ);

средствами защиты информации от НСД;

программно-аппаратным комплексом доверенной загрузки;

антивирусным пакетом;

межсетевым экраном;

средством создания модели разграничения доступа;

программой контроля полномочий доступа к информационным ресурсам;

программой фиксации и контроля исходного состояния программного комплекса;

программой поиска и гарантированного уничтожения информации на дисках;

системой обнаружения вторжений и анализа защищенности;

сканером безопасности;

локальной вычислительной сетью;

подключением к сети Интернет.

12.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся фундаментальной основой практических рекомендаций по мерам и средствам, используемым для ТЗИ объектов информатизации.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗИ от НСД, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы Слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических и лабораторных занятиях. На практических занятиях развиваются умения проведения работ, выполняемых при осуществлении контроля защищенности конфиденциальной информации от НСД, а также формируются умения использования программных и аппаратных средств ТЗИ.

Практические занятия по демонстрации средств ТЗИ, способов их использования, а также по установке, настройке и эксплуатации систем (средств) защиты конфиденциальной информации от НСД проводятся в специализированных лабораториях (компьютерном классе с предварительной установкой необходимого программного обеспечения). Занятия проводятся на четырёх-восьми рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе) под руководством преподавателя.

12.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Угрозы безопасности информации, связанные с НСД.

Методы анализа угроз безопасности информации.

Требования по защите информации от НСД.

Меры защиты информации от НСД.

Средства защиты информации от НСД.

Методы контроля защищенности информации от НСД.

Сканеры безопасности и их характеристика.

Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

Классификация автоматизированных систем по требованиям защиты информации.

Способы контроля целостности программного обеспечения и аппаратных средств.

Способы и средства контроля доступа к автоматизированным системам и рабочему месту пользователя.

13. Рабочая программа учебной дисциплины «Техническая защита конфиденциальной информации от специальных воздействий»

13.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам ТЗКИ от специальных воздействий.

13.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД.

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации», «Контроль состояния ТЗКИ».

13.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

в проектной деятельности:

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов на объекте информатизации, целей и задач

деятельности объекта защиты;

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых Слушателям в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

возможные угрозы безопасности информации в результате специальных воздействий;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

определять возможные угрозы безопасности информации в результате специальных воздействий;

формировать требования по ТЗКИ;

определять требования к средствам ТЗКИ на объектах информатизации; организовывать и проводить работы по ТЗКИ;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗКИ;

определения угроз безопасности информации;

определения задач, проведения организационных и технических мероприятий по

ТЗКИ;

определения задач, проведение организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

применения средств ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации.

13.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 10 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	6
лекции (Л)	2
практические занятия (ПЗ)	2
семинары (С)	2
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	10

13.5. Содержание учебной дисциплины

13.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Информация как объект защиты от специальных воздействий	Информация как объект защиты от специальных электромагнитных воздействий. Технические средства обработки информации как объекты защиты от специальных электромагнитных воздействий. Физические процессы, возникающие при воздействии мощными электрическими и магнитными полями и токами на технические средства обработки информации. Угрозы безопасности информации от специальных электромагнитных воздействий. Модели угроз. Механизм влияния электромагнитных и электрических воздействий на технические средства обработки информации. Меры и средства защиты информации от специальных воздействий. Принципы использования экранирующих и поглощающих свойств различных материалов для защиты информации от электромагнитных воздействий. Принципы использования фильтрующих и поглощающих устройств и материалов для защиты информации от электрических воздействий. Организация и содержание работ по защите информации от специальных воздействий, состав и содержание необходимых документов

13.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Организация защиты конфиденциальной информации на объектах информатизации	+
2.	Аттестация объектов информатизации по требованиям безопасности информации	+
3.	Аттестация объектов информатизации по требованиям безопасности информации	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

13.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование раздела учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Информация как объект защиты от специальных воздействий	2	2	-	2	2	8

13.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

13.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Меры и средства защиты конфиденциальной информации от специальных электромагнитных и электрических воздействий	2

13.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Разработка организационных и технических мероприятий по ТЗКИ от специальных воздействий, контролю защищенности информации, оценки состояния ТЗКИ от специальных воздействий	2

13.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем / В.Д.Добыкин, А.И. Куприянов, В.Г. Пономарев, Л.Н. Шустов; под. ред. А.И. Куприянова. - М.: Вузовская книга, 2007 г.

2. Методы и средства защиты компьютерной информации: учеб. пособие / И.В.Аникин, В.И. Глова. - Казань, Изд-во КГТУ им. А.Н. Туполева, 2008 г.

3. Основы информационной безопасности: учеб. пособие / Н.В. Медведев, В.В.Баданин, О.А. Акулов. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2008 г.

4. Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты / Н.В. Балюк, Л.Н. Кечиев, П.В. Степанов. - М.: Группа ИДТ, 2008 г.

5. Экранирование технических средств и экранирующие системы / Л.Н. Кечиев, Б.Б.Акбашев, П.В. Степанов. - М.: Группа ИДТ, 2010 г.

Дополнительная литература:

1. Мощные сверх коротко-импульсные и сверхширокополосные электромагнитные излучения и их помеховое и поражающее воздействия на электронную аппаратуру передачи-приема, обработки и хранения информации: монография / под ред. В.Г. Герасименко, В.Б. Авдеева, А.В. Бердышева. - Воронеж: Научная книга, 2008 г.

2. Сахаров К.Ю. Излучатели сверхкоротких электромагнитных импульсов и методы измерений их параметров. -М.: МГИЭМ, 2006 г.

3. ЭМС и информационная безопасность в системах телекоммуникаций / Л.Н.Кечиев, П.В. Степанов. - М.: Технологии, 2005 г.

4. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

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

6. ГОСТ 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. - М.: Госстандарт России, 2000 г.

7. ГОСТ Р 51275-2006 Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения. - М.: Ростехрегулирование, 2006 г.

8. ГОСТ Р 56093-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования. Госстандарт, 2014 г.

9. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в

защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Госстандарт, 2014 г.

10. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Госстандарт, 2014 г.

Программное обеспечение:

Не требуется.

Базы данных, информационно-справочные и поисковые системы:

www.fstec.ru;

bdu.fstec.ru;

www.pravo.gov.ru;

www.gost.ru/wps/portal/tk362;

правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

13.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, специальными учебными комплексами, содержащими образцы различных материалов с экранирующими и поглощающими свойствами для защиты информации от электромагнитны воздействий, стенды с образцами фильтрующих и поглощающих устройств и материалов для защиты информации от электрических воздействий и стенды, разъясняющие способы защиты информации от специальных электромагнитных и электрических воздействий.

13.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по ТЗКИ от специальных воздействий.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗИ, а также с целью обсуждения других, наиболее важных вопросов учебной

дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала, подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы слушатели получают консультацию у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения применять меры и средства по защите информации от специальных воздействий и проведения специальных проверок защищенности информации от специальных воздействий.

13.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине, в соответствии с перечнем примерных вопросов, выносимых для контроля знаний слушателей:

Информация как объект защиты от специальных электромагнитных воздействий.

Технические средства обработки информации как объекты защиты от специальных электромагнитных и электрических воздействий.

Перечень угроз безопасности информации от специальных электромагнитных и электрических воздействий.

Механизм влияния электромагнитных и электрических воздействий на технические средства обработки информации.

Организация и содержание работ по защите информации от преднамеренных силовых электромагнитных воздействий.

Принципы использования экранирующих и поглощающих свойств различных материалов для защиты информации от электромагнитных воздействий.

Принципы использования фильтрующих и поглощающих устройств и материалов для защиты информации от электрических воздействий.

Средства обнаружения силовых электромагнитных воздействий.

14. Рабочая программа учебной дисциплины «Организация защиты конфиденциальной информации на объектах информатизации»

14.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам организации защиты конфиденциальной информации на объектах информатизации.

14.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, будут использоваться при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Аттестация объектов информатизации по требованиям безопасности информации» и «Контроль состояния ТЗКИ».

14.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность организовывать мероприятия по контролю (мониторингу) защищенности

конфиденциальной информации на объектах информатизации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ на объектах информатизации;

в проектной деятельности:

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);

способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность проводить работы по устранению неисправностей и ремонту (техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых слушателями в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

основы функционирования государственной системы ПД ИТР и ТЗИ, цели и задачи ТЗКИ;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от утечки по техническим каналам, несанкционированных, непреднамеренных воздействий, контроля целостности информации;

методы и методики контроля (мониторинга) защищенности конфиденциальной информации;

порядок проведения мониторинга информационной безопасности средств и систем информатизации;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

формировать требования по ТЗКИ;

организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ;

выявления ТКУИ и определения угроз безопасности информации;

определения задач, проведения организационных и технических мероприятий по

ТЗКИ;

применения средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения, в том числе зарубежными информационными ресурсами;

проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации, оформления материалов аттестационных испытаний;

организации деятельности подразделений и специалистов в области ТЗКИ.

14.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 52 часа.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	38
лекции (Л)	6
практические занятия (ПЗ)	26
семинары (С)	6
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	12
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	52

14.5. Содержание учебной дисциплины

14.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Организация защиты конфиденциальной информации на объектах информатизации	Организация работ по созданию и эксплуатации объектов информатизации и их систем защиты информации. Положение о порядке организации и проведения работ по защите конфиденциальной информации. Перечень сведений конфиденциального характера, подлежащих защите. Планирование работ по ТЗКИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.
2.	Реализация требований по ТЗКИ	Реализация требований по защите акустической речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам. Реализация требований по защите информации от НСД и специальных воздействий на эксплуатируемом (функционирующем) объекте информатизации. Реализация требований по защите информации от

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		НСД и специальных воздействий при создании нового объекта информатизации в защищенном исполнении. Особенности реализации требований по защите персональных данных.
3.	Проектирование систем защиты конфиденциальной информации	Создание и функционирование систем защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания систем защиты конфиденциальной информации. Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении. Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации.

14.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин		
		1	2	3
1.	Аттестация объектов информатизации по требованиям безопасности информации	+	+	+
2.	Контроль состояния ТЗКИ	+	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

14.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Организация защиты конфиденциальной информации на объектах информатизации	2	2	-	-	2	6
2.	Реализация требований по ТЗКИ	2	-	-	6	2	10
3.	Проектирование систем защиты конфиденциальной информации	2	24	-	-	8	34

14.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

14.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	2	Особенности реализации требований по защите информации от НСД на эксплуатируемом (функционирующем) объекте информатизации	2
2.	2	Особенности реализации требований по защите информации от НСД при создании нового объекта информатизации в защищенном исполнении	2
3.	2	Особенности реализации требований по защите персональных данных	2

14.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Разработка руководства по ТЗКИ в организации	2
2.	3	Формирование требований к средствам и системам информатизации в защищенном исполнении	2
3.	3	Проектирование средств и систем информатизации в защищенном исполнении	4
4.	3	Разработка аналитического обоснования необходимости создания системы защиты информации на объекте информатизации	2
5.	3	Разработка технического задания на создание системы защиты информации объекта информатизации	2
6.	3	Разработка эскизного проекта системы защиты информации объекта информатизации	2
7.	3	Разработка технического проекта системы защиты информации объекта информатизации	2
8.	3	Разработка аналитического обоснования необходимости создания системы защиты информации защищаемого помещения	2
9.	3	Разработка технического задания на создание системы защиты информации защищаемого помещения	2
10.	3	Разработка эскизного проекта системы защиты информации защищаемого помещения	2
11.	3	Разработка технического проекта системы защиты информации защищаемого помещения	2
12.	3	Разработка рабочей и эксплуатационной документации на систему защиты информации объекта информатизации (защищаемого помещения), а также организационно-распорядительной документации по защите информации на объекте информатизации	2

14.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. - М.: Горячая линия - Телеком, 2006 г.

2. Технические средства и методы защиты информации: учеб. пособие для студентов вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков [и др.]; под ред. Зайцева А.П. и Шелупанова А.А. Изд. 4-е испр. и доп. - М.: Горячая линия-Телеком, 2009 г.

3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. - М.: НПЦ «Аналитика», 2010 г.

Дополнительная литература:

1. Зегжда, Д.П. Основы безопасности информационных систем - М.: Горячая линия - Телеком, 2000 г.

2. Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. - М.: Радио и связь, 2000 г.

3. Герасименко В.А., Малюк А.А. Основы защиты информации: учебник. - М.: «МИФИ», 1997 г.

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

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

8. 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».

9. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

12. Требования о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

13. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

14. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

15. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.

16. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

17. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

18. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

19. Приказ ФСТЭК России от 3 апреля 2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

20. Об утверждении образца формы уведомления об обработке персональных данных. Приказ Федеральной службы по надзору в сфере связи и массовых коммуникаций от 17 июля 2008 г. № 08.

21. ГОСТ 34.602-2020 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Росстандарт, 2021 г.

22. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993 г.

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

24. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006 г.

25. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998 г.

26. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Росстандарт, 2008 г.

27. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014 г.

28. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000 г.

29. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Госстандарт, 2013 г.

30. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Ростехрегулирование, 2006 г.

31. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Ростехрегулирование, 2008г.

32. ГОСТ Р 56093-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014 г.

33. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014 г.

34. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014 г.

35. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов

информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013 г.

36. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Ростехрегулирование, 2006 г.

37. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. Ростехрегулирование, 2006 г.

38. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012 г.

39. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013 г.

40. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности (прямое применение ISO/IEC 15408-3:2008). Росстандарт, 2013 г.

41. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Сетевая безопасность. Часть 1. Обзор и концепции. Росстандарт, 2012 г.

42. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий (прямое применение ISO/IEC 18045:2008). Росстандарт, 2013 г.

43. ГОСТР ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021 г.

44. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Росстандарт, 2021 г.

45. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. Росстандарт, 2022 г.

46. ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации. Росстандарт, 2022 г.

47. ГОСТ Р ИСО/МЭК 27004-2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Росстандарт, 2022 г.

48. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Росстандарт, 2010 г.

49. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции, Росстандарт, 2011 г.

50. ГОСТ 2.610-2019 ЕСКД. Правила выполнения эксплуатационных документов. Росстандарт, 2019 г.

51. ГОСТ 2.001-2013 ЕСКД. Общие положения. Росстандарт, 2013 г.

52. ГОСТ 2.004-88 ЕСКД. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ. Госстандарт СССР, 1988 г.

53. ГОСТ 3.1102-81 ЕСТД. Стадии разработки и виды документов. Общие положения. Госстандарт СССР, 1981 г.

54. ГОСТ 3.1109-82 ЕСТД. Термины и определения основных понятий. Госстандарт СССР, 1982 г.

55. ГОСТ 19.507-79 ЕСПД. Ведомость эксплуатационных документов. Госстандарт СССР, 1979 г.

56. ГОСТ 19.508-79 ЕСПД. Руководство по техническому обслуживанию. Требования к содержанию и оформлению. Госстандарт СССР, 1979 г.

57. Методика оценки угроз безопасности информации. Утверждена ФСТЭК России 5 февраля 2021 г.

58. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

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

60. Временная методика оценки защищенности информации ограниченного

доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

61. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

62. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

63. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Программное обеспечение:

Программное средство автоматизированного проектирования - Nano CAD версия 5.1.

Базы данных, информационно-справочные и поисковые системы:

www.fstec.ru;

bdu.fstec.ru;

www.gost.ru/wps/portal/tk362.

14.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера;

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным проектором, проекционным экраном, акустической системой, персональным компьютером, беспроводным микрофоном, блоком управления оборудования, интерфейсами подключения: USB, audio, HDMI, трибуной преподавателя.

Учебные аудитории и средства вычислительной техники прошли аттестацию в установленном порядке.

14.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся

фундаментальной основой нормативной базы и практических рекомендаций по созданию систем защиты информации объектов информатизации.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗИ, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы Слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения организации ТЗКИ, а также формируются навыки проведения мероприятий по ТЗИ.

14.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Планирование работ по ТЗКИ.

Организация и проведение работ по обеспечению ТЗКИ на объектах информатизации.

Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.

Создание и функционирование системы защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации.

Стадии создания системы защиты конфиденциальной информации объекта информатизации.

Особенности реализации требований по защите акустической речевой информации и информации, обрабатываемой в СВТ от утечки по техническим каналам.

Особенности реализации требований по защите информации от НСД на эксплуатируемом (функционирующем) объекте информатизации.

Особенности реализации требований по защите персональных данных.

Стадии и этапы создания систем защиты конфиденциальной информации.

Формирование требований к средствам и системам информатизации в защищенном исполнении.

Аналитическое обоснование необходимости создания системы защиты информации на объекте информатизации.

Порядок проектирования средств и систем информатизации в защищенном исполнении.

Порядок проектирования защищаемых помещений.

Внедрение системы защиты информации.

Аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие.

Сопровождение системы защиты информации в ходе эксплуатации объекта информатизации.

Разработка эксплуатационной документации на систему защиты информации.

15. Рабочая программа учебной дисциплины «Аттестация объектов информатизации по требованиям безопасности информации»

15.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

15.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, будут использоваться для изучения последующей учебной дисциплины программы профессиональной переподготовки «Контроль состояния ТЗКИ».

15.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

способность проводить аттестационные испытания и аттестацию объектов информатизации по требованиям безопасности информации;

в проектной деятельности:

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых слушателями в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

основы лицензирования деятельности по ТЗКИ;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации;

программы и методики аттестационных испытаний и аттестации объекта информатизации на соответствие требованиям по защите информации;

порядок, содержание, условия и методы испытаний для оценки характеристик и

показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний;

разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации;

разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ;

выявления ТКУИ и определения угроз безопасности информации;

определения задач, проведения организационных и технических мероприятий по ТЗКИ;

применения средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

работы в компьютерных сетях с учетом требований по безопасности информации;

проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации;

оформления материалов аттестационных испытаний;

проведения установки, монтажа, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации.

15.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 48 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	36
лекции (Л)	6
практические занятия (ПЗ)	14
семинары (С)	4
лабораторные работы (ЛР)	12
Самостоятельная работа (СР, всего)	10
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	48

15.5. Содержание учебной дисциплины

15.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции). Задачи, функции, права и обязанности органов по аттестации. Требования к органам по аттестации объектов информатизации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.
2.	Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия). Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации. Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно-документальный метод;

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		измерение и оценка уровней ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их выполнением; попытки «взлома систем защиты информации»). Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации.

15.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин	
		1	2
1.	Контроль состояния ТЗКИ	+	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

15.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	2	-	-	2	2	6
2.	Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	4	14	12	2	8	40

15.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	2	Аттестационные испытания и аттестация объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам за счет ПЭМИН	4
2.	2	Аттестационные испытания автоматизированных систем по требованиям безопасности информации от НСД	4
3.	2	Аттестационные испытания и аттестация объектов информатизации на соответствие требованиям по защите информации от утечки акустической речевой информации	4

15.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Полномочия, функции, права и обязанности участников аттестации объектов информатизации по требованиям безопасности информации	2
2.	2	Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объекта информатизации. Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия	2

15.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	2	Разработка программ и методик аттестационных испытаний различных объектов информатизации (средств и систем информатизации, защищаемых помещений)	2
2.	2	Проверка выполнения требований по безопасности информации от утечки по техническим каналам и по защите информации от НСД	4
3.	2	Проверка выполнения защищенности акустической речевой информации от утечки по техническим каналам	4
4.	2	Проверка выполнения требований по результатам аттестационных испытаний, разработка заключения по результатам аттестационных испытаний (аттестата соответствия)	4

15.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература[2]:

1. Белов Е.Б. Основы информационной безопасности: учеб. пособие/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М.: Горячая линия - Телеком, 2006 г. - 544 с.

2. Запечников С.В. Информационная безопасность открытых систем. Часть 1: учебник для вузов / С.В. Запечников, М.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: Горячая линия - Телеком, 2006 г. - 686 с.

3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3т. Т.1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008 г. – 436 с.

4. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: учеб. пособие. - 2-е изд., расширен, и дораб. Воронеж: ГУЛ ВО «Воронежская областная типография - издательство им. Е.А. Болховитинова», 2011 г. - 354 с.

5. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: учеб. пособие. - М.: ИТК «Дашков и К», 2006 г. - 336 с.

6. Кондратьев А.В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки: справочное пособие. М.: МАСКОМ, 2011 г. - 256 с.

7. Некоторые вопросы защиты информации: методич. пособие. - М.: НОВО, 2012 г. – 164 с.

8. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: учеб. пособие / В.С. Горбатов, С.В. Дворянкин, А.П. Дураковский, Р.С. Енгалычев [и др.]; под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014 г.- 560 с.

9. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: учеб. пособие /А.А. Голяков, В.С. Горбатов, А.П.Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014 г. – 208 с.: ил.

10. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: учеб. пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницын, А.Е. Панин; под общ. ред.

[2] Перечень основной литературы может дополняться руководителями образовательных организаций при поступлении новых (уточненных) учебных пособий.

Ю.Н.Лаврухина. - М: НИЯУ МИФИ, 2014 г. - 248 с.: ил.

11. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: Учебное пособие / А.П. Дураковский, И.В. Куницын, Ю.Н. Лаврухин. - М: НИЯУ МИФИ, 2015 г. - 152 с.

Дополнительная литература:

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: учеб. пособие. - М.: «Горячая линия» - Телеком, 2005 г.

2. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос-АРВ, 2003 г.

3. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005 г.

4. Хорев А.А. Аттестация объектов информатизации и выделенных помещений // Специальная техника. – 2006 г. - № 4.

5. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

6. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

7. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993 г.

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

9. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006 г.

10. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998 г.

11. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014 г.

12. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000 г.

13. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013 г.

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

15. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

16. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

17. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.

18. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

19. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Программное обеспечение:

Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2), средство создания модели системы разграничения доступа «Ревизор - 1 XP», программа контроля полномочий доступа к информационным ресурсам «Ревизор - 2 XP», программа поиска и гарантированного уничтожения информации на дисках «TERRIER» (версия 3.0).

Базы данных, информационно-справочные и поисковые системы:

www.fstec.ru;

bdu.fstec.ru;

www.gost.ru/wps/portal/tk362.

15.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера (с приводом лазерных дисков типа

DVD-RW, звуковым сопровождением и т.п.);

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным персональным компьютером преподавателя (сервером) и пользовательскими терминалами по числу слушателей, объединенных локальной сетью («компьютерный» класс).

Учебные аудитории и средства вычислительной техники аттестованы в установленном порядке.

Для изучения учебной дисциплины имеется специализированная учебная лаборатория для проведения:

аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок;

аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации;

аттестационных испытаний и аттестация объектов информатизации на соответствие требованиям по защите информации от утечки акустической речевой информации.

Специализированная лаборатория оснащена полным комплексом контрольно-измерительного и испытательного оборудования, средствами контроля защищенности, тест-объектами, эквивалентами строительных и иных конструкций, позволяющих полностью имитировать реальные ситуации при выполнении аттестационных испытаний объектов информатизации.

Для проведения занятий в Учебном центре имеется:

а) контрольно-измерительное и испытательное оборудование:

- генератор шумовых сигналов СПФ АКИП-3409/1. Диапазон частот 1мкГц...5 МГц;

- низкочастотный генератор сигналов ГЗ-131, диапазон частот 2...2 МГц, выходное напряжение не менее 2 В;

- активная акустическая система «Прибой», диапазон частот 20...20 кГц, мощность 150 Вт. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 95 дБ. Неравномерность АЧХ не более ±6 дБ;

- микровольтметр селективный В6-9, диапазон частот 20Гц... 100 кГц, погрешность измерения ±15 %;

- переносной анализатор спектра R&S FPH, диапазон измеряемых параметров 5 кГц - 2 ГГц, погрешность измерения не более 2 дБ, с опцией HA-Z220;

- селективный нановольтметр Unipan-233, диапазон частот 1,5 Гц...150 кГц,

погрешность измерения ±6 %;

- измерительный микрофон М-201, диапазон частот 2...40000 Гц, чувствительность 14 мВ/Па, неравномерность АЧХ не более ±1 дБ;

- антенна измерительная дипольная АИ5-0, диапазон измеряемых частот по электрической составляющей 9 кГц... 2000 МГц, погрешность измерения не более ±2 дБ;

- антенна измерительная рамочная АИР 3-2 по магнитной составляющей 9 кГц... 30 МГц погрешность измерения не более ±2 дБ;

- вибропреобразователь АР2038Р-10, диапазон частот 0,5...12000 Гц, чувствительность не хуже 1 мВ/(мс)$^{-2}$, неравномерность АЧХ на промежутке от 175 ... 5600 Гц не превышает ± 2%;

- измерительный пробник напряжения «ПН-102» - диапазон измеряемых параметров 3кГц... 400 МГц;

- четырехканальный шумометр, виброметр, анализатор спектра «Экофизика-110А» (исполнение «HF») - диапазон частот: 1/1-октавные спектры 1 Гц - 16 кГц (синтезированные), 1/3-октавные спектры 0,8 Гц - 20 кГц, 1/12-октавные спектры 102,9 Гц до 9716 Гц, Номинальное затухание 0 дБ, 1 класс точности по ГОСТ Р 8.714-2010 (МЭК 61260-1995), АЧХ в соответствии с ГОСТ 17168-82; в диапазоне частот 2 Гц ... 20 кГц диапазон измерений уровней звука 22 ... 150 дБ;

- осциллограф АКИП – 4115/4А Диапазон частот (синус) 1 мкГц – 5 МГц; Вид шумового сигнала: синусоидальный, прямоугольный, треугольный, импульс, белый шум;

- тестер-рефлектометр оптический «Топаз-7317-ARX», длина волны калибровки, нм 850, 1300, 1310, 1550, диапазон измерений оптической мощности дБ, от минус 85 до 6, разрешающая способность - 0,1 дБ, разрешение по затуханию, дБ - 0,001.

б) средства контроля защищенности:

- программа контроля полномочий доступа к информационным ресурсам «Ревизор – 2 XP», сертификат соответствия ФСТЭК №990 от 08.02.2005 г.;

- средство контроля эффективности применения средств защиты информации «Ревизор Сети» (версия 3.0), сертификат соответствия ФСТЭК №3413 от 02.06.2015 г.;

- программное средство контроля целостности программ и программных комплексов «ФИКС» (версия 2.0.2), сертификат соответствия ФСТЭК №1548 от 15.01.2008 г.;

- система контроля (анализа) защищенности информационных систем, средство, предназначенные для осуществления тестирования на проникновение: сетевой сканер уязвимостей Xspider 7.8, сертификат соответствия ФСТЭК №3247 от 24.10.2014 г.

15.11. Методические рекомендации по организации изучения учебной

дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по технической защите информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций излагается проблемным методом с привлечением слушателей для решения сформулированной преподавателем задачи. С целью текущего контроля знаний в ходе занятий необходимо использовать различные приёмы тестирования.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам технической защиты информации, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы Слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения по вопросам аттестации объектов информатизации по требованиям безопасности информации, а также формируются навыки применять действующую нормативную правовую и методическую базу в области ТЗИ.

Практические занятия по изучению вопросов аттестации объектов информатизации проводятся с преподавателем на четырёх-восьми рабочих местах с развёрнутым необходимым оборудованием средств технического контроля и средств имитации ТКУИ (количество рабочих мест зависит от количества слушателей в учебной группе).

15.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Цели аттестационных испытаний и аттестации объектов информатизации на

соответствие требованиям по защите информации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).

Участники аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации и их полномочия (компетенции).

Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

Контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.

Основные мероприятия по проведению аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

Требования обеспечения защиты конфиденциальной информации при проведении аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации.

Экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний.

Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.

Проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации.

Проверка подсистем защиты информации от НСД, контроль целостности применяемых средств защиты информации от НСД, в том числе с использованием специальных средств контроля защищенности информации.

Проверка программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации.

Испытания системы защиты информации от НСД путем осуществления попыток НСД к тестовой защищаемой информации в обход используемой системы защиты информации, в том числе с использованием специальных программных тестирующих средств.

Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций.

Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации.

Состав и содержание документов, разрабатываемых для проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации и по результатам аттестации объектов информатизации.

Перечислите основные отчетные документы, разрабатываемые в ходе аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

Основные виды объектов информатизации, предназначенных для обработки информации ограниченного доступа.

Каналы утечки информации, контролируемые при проведении аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

Отличие лабораторных специальных исследований от исследований, проводимых непосредственно в помещении, в котором расположен объект информатизации.

Определение класса средств защиты информации от утечки по техническим каналам в автоматизированной системе.

Основные критерии определения класса защищенности автоматизированных систем от НСД к информации.

Порядок проведения классификации автоматизированных систем, информационной системы персональных данных, государственной информационной системы.

Какая характеристика объекта информатизации определяет класс средств защиты информации от утечки по техническим каналам в защищаемом помещении.

Состав эксплуатационной документации, разрабатываемой на объектах информатизации (защищаемых помещениях).

Документы, разрабатываемые в ходе предварительного обследования объектов информатизации.

Порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

Программа и методики аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации.

16. Рабочая программа учебной дисциплины «Контроль состояния технической защиты конфиденциальной информации»

16.1. Цель учебной дисциплины - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам контроля состояния ТЗКИ.

16.2. Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки и при изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин «Организационно-правовые основы ТЗКИ», «Средства и системы обработки информации», «Способы и средства ТЗКИ от утечки по техническим каналам», «Меры и средства ТЗКИ от НСД», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации».

Данная учебная дисциплина является итоговой учебной дисциплиной программы профессиональной переподготовки.

16.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение слушателями таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;

способность организовывать мероприятия по контролю (мониторингу) защищенности

конфиденциальной информации на объектах информатизации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ на объектах информатизации;

способность проводить аттестационные испытания и аттестацию объектов информатизации по требованиям безопасности информации;

в проектной деятельности:

способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

в эксплуатационной деятельности:

способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность проводить работы по устранению неисправностей и ремонту (техническом) обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых Слушателям в результате изучения учебной дисциплины, формируется из приведенного ниже списка.

Слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ;

требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области ТЗКИ;

типовую структуру, задачи и полномочия подразделения по ТЗИ;

технические каналы утечки информации и угрозы безопасности информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

методы и методики контроля (мониторинга) защищенности конфиденциальной информации;

порядок проведения мониторинга информационной безопасности средств и систем информатизации;

требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства;

порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

порядок устранения неисправностей и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области ТЗИ;

выявления ТКУИ и определения угроз безопасности информации;

определения задач, проведение организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

применения средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

организации деятельности подразделений и специалистов в области ТЗКИ.

16.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 72 часа.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	54
лекции (Л)	14
практические занятия (ПЗ)	16
семинары (С)	18
лабораторные работы (ЛР)	6
Самостоятельная работа (СР, всего)	16
Вид промежуточной аттестации и его трудоемкость	2 (зачет)
Общая трудоемкость	72

16.5. Содержание учебной дисциплины

16.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Основы организации контроля состояния ТЗКИ	Основные задачи контроля состояния ТЗКИ. Классификация видов контроля состояния ТЗКИ. Система документов по контролю состояния ТЗКИ. Вопросы, подлежащие проверке при контроле состояния ТЗКИ. Организационный и технический контроль состояния ТЗКИ.
2.	Методы и средства контроля защищенности конфиденциальной информации	Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам. Методы и средства контроля защищенности конфиденциальной информации от НСД. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации.
3.	Мониторинг информационной безопасности средств и	Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации. Состав и структура системы мониторинга.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
	систем информатизации	Основные принципы системы мониторинга информационной безопасности средств и системы информатизации. Обнаружение и идентификация инцидентов безопасности информации, а также событий, приводящих к возникновению инцидентов. Анализ инцидентов безопасности информации, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий. Планирование мер по устранению инцидентов безопасности информации, в том числе по восстановлению систем информатизации, их сегментов и средств, входящих в их состав, в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Планирование мер по предотвращению повторного возникновения инцидентов безопасности информации. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации. Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации. Анализ и оценка функционирования систем защиты информации систем информатизации, включая выявление, анализ и устранение недостатков в функционировании систем защиты информации систем информатизации. Периодический анализ изменения угроз безопасности информации в средствах и системах информатизации, возникающих в ходе их эксплуатации. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработка предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ по оценке эффективности систем защиты информации систем информатизации.

16.5.2. Разделы учебной дисциплины и виды занятий

№ п/п	Наименование раздела учебной дисциплины	Л	ПЗ	ЛР	С	СР	Всего
1.	Основы организации контроля состояния ТЗКИ	2	-	-	4	2	8
2.	Методы и средства контроля защищенности конфиденциальной информации	8	14	-	10	10	42
3.	Мониторинг информационной безопасности средств и систем информатизации	4	2	6	4	4	20

16.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	3	Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих конфиденциальную информацию	2
2.	3	Мониторинг парольной защиты и контроль надежности пользовательских паролей. Мониторинг целостности программного обеспечения	2
3.	3	Мониторинг попыток несанкционированного доступа. Мониторинг производительности автоматизированных систем	2

16.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	1	Организация и порядок проведения контроля состояния ТЗКИ	4
2.	2	Методики оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	2
3.	2	Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	2
4.	2	Методика инструментального контроля выполнения норм показателя защищенности акустической речевой конфиденциальной информации	2
5.	2	Методы и средства контроля защищенности акустической речевой конфиденциальной информации от утечки по техническим каналам	2
6.	2	Методы и средства контроля защищенности конфиденциальной информации от НСД	2
7.	3	Порядок и методы мониторинга информационной безопасности средств и систем информатизации	4

16.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	2	Проведение контроля защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов	4
2.	2	Проведение контроля защищенности акустической речевой конфиденциальной информации от утечки по техническим каналам с использованием программно-аппаратных комплексов	2
3.	2	Установка, монтаж, наладка, испытания, ремонт (техническое обслуживание) технических средств контроля (мониторинга) эффективности мер защиты информации от утечки по техническим каналам	2
4.	2	Порядок проведения работ, выполняемых при осуществлении контроля защищенности конфиденциальной информации от НСД и ее модификации в средствах и системах информатизации	4
5.	2	Установка, монтаж, наладка, испытания, ремонт (техническое обслуживание) технических средств контроля (мониторинга) эффективности мер защиты информации от НСД	2
6.	3	Порядок анализа инцидентов безопасности информации, устранение их последствий	2

16.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 3. Контроль эффективности защиты информации. - М.: НПЦ «Аналитика», 2008 г.

2. Хорев А.А. Организация контроля эффективности противодействия техническим средствам разведки и защиты информации: учеб. пособие. - М.: Министерство обороны Российской Федерации, 2006 г.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: Горячая линия - Телеком, 2011 г.

4. Меньшаков Ю.К. Теоретические основы технических разведок. - М.: МГТУ им. Н.Э. Баумана, 2008 г.

5. Тупота В.И., Петигин А.Ф. Контроль защищенности средств вычислительной техники от утечки информации за счет побочных электромагнитных излучений: учеб. пособие. - Воронеж, 2010 г.

Дополнительная литература:

1. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: учеб. пособие для вузов. - М.: Радио и связь, 2000 г.

2. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. - М.: МО Российской Федерации, 1998 г.

3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учеб. пособие. М.: Гостехкомиссия России, 1998 г.

4. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник. - М.: МИФИ, 1997 г.

5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем - М.: Горячая линия - Телеком, 2000 г.

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

7. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

8. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

9. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

10. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

11. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

12. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

13. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007г.

14. Положение о банке данных угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9.

15. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной

совместимости методом экранирования. Госстандарт России, 1993 г.

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

17. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006 г.

18. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998 г.

19. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014 г.

20. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000 г.

21. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005 г.

22. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования. Ростехрегулирование, 2007 г.

23. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014 г.

24. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013 г.

25. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий (прямое применение ISO/IEC 18045:2008). Росстандарт, 2013 г.

26. ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021 г.

27. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Росстандарт, 2021 г.

28. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения

информационной безопасности. Росстандарт, 2022 г.

29. ГОСТ Р ИСО/МЭК 27004-2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Росстандарт, 2022 г.

30. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Росстандарт, 2010 г.

31. ГОСТ Р ИСО/МЭК 27006-2020 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Росстандарт, 2022 г.

32. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

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

34. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2017 г.

35. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

36. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.

37. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

38. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Программное обеспечение:

Средства разграничения доступа к компонентам вычислительных сетей, средства

разграничения доступа к данным – системы авторизации и аутентификации на базе Windows Active Directory, IPA.

Средства поиска разрушающих программных воздействий (антивирусные программы) – Антивирус Касперского, Dr.Web.

Средства анализа трафика вычислительных сетей – Netflow, sflow.

Средства анализа структуры вычислительных сетей – Nmap. Lancope. Система мониторинга состояния сети на базе zabbix.

Базы данных, информационно-справочные и поисковые системы:

www.fstec.ru;

bdu.fstec.ru;

www.gost.ru/wps/portal/tk362.

16.10. Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе:

мультимедийного персонального компьютера (с приводом лазерных дисков типа DVD-RW, звуковым сопровождением и т.п.);

мультимедийного проектора с дистанционным управлением.

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным персональным компьютером преподавателя (сервером) и пользовательскими терминалами по числу слушателей, объединенных локальной сетью («компьютерный» класс).

Учебные аудитории и средства вычислительной техники аттестованы в установленном порядке.

Для изучения учебной дисциплины имеется специализированная учебная лаборатория для проведения мониторинга информационной безопасности средств и систем информатизации.

Специализированная лаборатория оснащена полным комплексом программно-технических средств, соответствующих реальному оборудованию, необходимому для проведения демонстраций средств защиты информации и контроля, необходимым количеством тест-объектов, позволяющих полностью имитировать реальные ситуации при проведении контроля защищенности автоматизированных систем, защиты информации от утечки по каналам ПЭМИН, а также мониторинга информационной безопасности средств и систем информатизации.

Для проведения занятий в Учебном центре имеется:

а) контрольно-измерительное и испытательное оборудование:

- генератор шумовых сигналов СПФ АКИП-3409/1. Диапазон частот 1мкГц...5 МГц;

- низкочастотный генератор сигналов ГЗ-131, диапазон частот 2...2 МГц, выходное напряжение не менее 2 В;

- активная акустическая система «Прибой», диапазон частот 20...20 кГц, мощность 150 Вт. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 95 дБ. Неравномерность АЧХ не более ±6 дБ;

- четырехканальный шумометр, виброметр, анализатор спектра «Экофизика-110А» (исполнение «HF») - диапазон частот: 1/1-октавные спектры 1 Гц - 16 кГц (синтезированные), 1/3-октавные спектры 0,8 Гц - 20 кГц, 1/12-октавные спектры 102,9 Гц до 9716 Гц, Номинальное затухание 0 дБ, 1 класс точности по ГОСТ Р 8.714-2010 (МЭК 61260-1995), АЧХ в соответствии с ГОСТ 17168-82; в диапазоне частот 2 Гц ... 20 кГц диапазон измерений уровней звука 22 ... 150 дБ;

- микровольтметр селективный В6-9, диапазон частот 20Гц...100 кГц, погрешность измерения ±15 %;

- переносной анализатор спектра R&S FPH, диапазон измеряемых параметров 5 кГц - 2 ГГц, погрешность измерения не более 2 дБ, с опцией HA-Z220;

- селективный нановольтметр Unipan-233, диапазон частот 1,5 Гц...150 кГц, погрешность измерения ±6 %;

- измерительный микрофон М-201, диапазон частот 2...40000 Гц, чувствительность 14 мВ/Па, неравномерность АЧХ не более ±1 дБ;

- антенна измерительная дипольная АИ5-0, диапазон измеряемых частот по электрической составляющей 9 кГц... 2000 МГц, погрешность измерения не более ±2 дБ;

- антенна измерительная рамочная АИР 3-2 по магнитной составляющей 9 кГц...30 МГц погрешность измерения не более ±2 дБ;

- вибропреобразователь АР2038Р-10, диапазон частот 0,5...12000 Гц, чувствительность не хуже 1 мВ/(мс)$^{-2}$, неравномерность АЧХ на промежутке от 175 ... 5600 Гц не превышает ± 2%;

- измерительный пробник напряжения «ПН-102» - диапазон измеряемых параметров 3кГц... 400 МГц;

- осциллограф АКИП – 4115/4А Диапазон частот (синус) 1 мкГц – 5 МГц; Вид шумового сигнала: синусоидальный, прямоугольный, треугольный, импульс, белый шум; оптические тестеры (измерители мощности), длина волны калибровки, нм 850, 1310, 1550, диапазон измерений оптической мощности дБ, от 3 до минус 10 - минус 73, разрешающая способность, дБ - 0,1... 0,001;

- тестер-рефлектометр оптический «Топаз-7317-ARX», длина волны калибровки, нм 850, 1300, 1310, 1550, диапазон измерений оптической мощности дБ, от минус 85 до 6, разрешающая способность - 0,1 дБ, разрешение по затуханию, дБ - 0,001.

б) средства контроля защищенности:

программные средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах: «Ревизор-1 XP», сертификат соответствия ФСТЭК №989 от 08.02.2005 г. и «Ревизор-2 XP», сертификат соответствия ФСТЭК №990, от 08.02.2005 г.;

средство контроля эффективности применения средств защиты информации «Ревизор Сети» (версия 3.0), сертификат соответствия ФСТЭК №3413 от 02.06.2015 г.;

программное средство контроля целостности программ и программных комплексов «ФИКС» (версия 2.0.2), сертификат соответствия ФСТЭК №1548 от 15.01.2008 г.;

система контроля (анализа) защищенности информационных систем: сетевой сканер уязвимостей Xspider 7.8, сертификат соответствия ФСТЭК №3247 от 24.10.2014 г.;

межсетевой экран, построенный на базе Linux, ограничивающий адреса и порты подключения;

средство антивирусной защиты, предназначенное для применения на серверах и автоматизированных рабочих местах информационных систем, и средство их централизованного администрирования: Kaspersky Endpoint Security для Windows сертификат соответствия ФСТЭК № 4068 от 22.01.2019 г.;

система обнаружения вторжения: ПАК ViPNet IDS, сертификат соответствия ФСТЭК № 4329 от 24.11.2020 г.;

средство автоматизированного реагирования на инциденты информационной безопасности;

замкнутая система предварительного выполнения программ;

система управления информацией об угрозах безопасности информации;

система управления событиями безопасности информации;

система управления инцидентами информационной безопасности;

средство защиты каналов передачи данных: VipNet Client, сертификат соответствия ФСТЭК № 3727 от 30.11.2016 г., действителен до 30.11.2024 г., VipNet Coordinator, сертификат соответствия ФСТЭК № 3692 от 26.01.2017 г.;

система мониторинга и оповещения, построенная на базе ПО Grafana.

16.11. Методические рекомендации по организации изучения учебной

дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по основам контроля состояния (организации и эффективности) защиты информации.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗИ, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым конце каждого занятия с указанием из отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы Слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения осуществлять контроль защищенности информации, мониторинг информационной безопасности средств и систем информатизации, а также формируются навыки использования программных и аппаратных средств ТЗИ.

Практические занятия по демонстрации методов и средств контроля защищенности информации, мониторинга информационной безопасности средств и систем информатизации и способов их использования, а также по обучению выполнению работ по контролю защищенности информации в процессе эксплуатации проводятся в специализированных лабораториях (компьютерном классе с предварительной установкой необходимого программного обеспечения). Занятия проводятся на четырёх-восьми рабочих местах (количество рабочих мест зависит от количества слушателей в учебной группе). За каждым рабочим местом закреплен преподаватель, развернуто необходимое оборудование технического контроля и средства имитации угроз безопасности конфиденциальной информации.

16.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме устного опроса.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет

преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Основные задачи контроля состояния ТЗКИ.

Нормативные и методические документы по контролю ТЗКИ.

Вопросы, подлежащие проверке при контроле состояния ТЗКИ.

Организация и порядок проведения контроля состояния ТЗКИ.

Оценка защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Проведение контроля защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов.

Методика инструментального контроля выполнения норм показателя защищенности акустической речевой конфиденциальной информации.

Оценка защищенности акустической речевой информации.

Методы и средства контроля защищенности акустической речевой информации.

Проведение контроля защищенности акустической речевой информации с использованием программно-аппаратных комплексов.

Методы контроля защищенности конфиденциальной информации от НСД.

Средства контроля защищенности конфиденциальной информации от НСД.

Порядок проведения сертификационных испытаний средств защиты информации основных классов.

Задачи и функции мониторинга информационной безопасности средств и систем информатизации.

Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации.

Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации.

Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

17. Рабочая программа учебной дисциплины «Дискретная математика»

17.1. Цель учебной дисциплины – обучить слушателей основным понятиям и методам дискретной математики, необходимым для освоения разделов части модуля «Защита информации ограниченного доступа, не содержащие сведения, составляющие государственную тайну, криптографическими средствами», так и в работе по специальности.

17.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Настоящая дисциплина относится к циклу математических и естественнонаучных дисциплин. Для освоения учебной дисциплины, слушатели должны владеть знаниями и навыками в объеме программы средней школы по математике. Дисциплина занимает особое место в учебном плане и составляет основу математического образования слушателя. Знания, полученные при изучении дисциплины «Дискретная математика», позволяют перейти к изучению дисциплин «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы».

Знания, навыки и умения, приобретенные в результате изучения дисциплины, будут востребованы при изучении других дисциплин математического и естественнонаучного, а также экономического циклов, и при выполнении курсовых и выпускной квалификационной работы.

17.3. Требования к результатам освоения учебной дисциплины

В результате освоения дисциплины студенты должны получить представление об основных терминах, понятиях и методах дискретной математики как о языке и средствах построения моделей в прикладных исследованиях. Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность учиться, приобретать новые знания, умения, в том числе в области, отличной от профессиональной;

способность использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать собственную деятельность, выбирать типовые методы и

способы выполнения профессиональных задач, оценивать их эффективность и качество;

в проектной деятельности:

способность решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях;

способность осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития

в эксплуатационной деятельности:

способность использовать основные методы естественнонаучных дисциплин в профессиональной деятельности для теоретического и экспериментального исследования.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

основные понятия и алгоритмы, лежащие в основе теории чисел, комбинаторики.

б) уметь:

логически мыслить;

использовать типовые алгоритмы решения задач по разделам теории чисел, комбинаторики.

в) владеть навыками:

применения методов дискретной математики для решения практических задач.

17.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 12 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	10
лекции (Л)	8
практические занятия (ПЗ)	-
семинары (С)	2
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	12

17.5. Содержание учебной дисциплины

17.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Элементы теории множеств. Комбинаторика.	Элементы теории множеств. Понятие множества. Способы задания множеств. Операции над множествами. Диаграммы Эйлера-Венна. Системы множеств. Законы алгебры множеств. Декартово произведение множеств. Соответствия, отношения, функции. Композиция соответствий. Свойства отношений. Отношение эквивалентности. Отношение порядка. Взаимно-однозначное соответствие. Мощность множеств. Счетные и несчетные множества. Задачи комбинаторики. Правила суммы и произведения. Типы выборок. Размещения. Перестановки. Сочетания. Бином Ньютона. Свойства биномиальных коэффициентов. Треугольник Паскаля. Перестановки с повторениями. Полиномиальная формула. Комбинаторные тождества. Производящие функции. Основы теории графов.

17.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации	-
2.	Основные понятия криптографии	+
3.	Криптографические системы с симметричным ключом	+
4.	Криптографические системы с открытым ключом. Электронная подпись	+
5.	Хэш-функции. Обеспечение контроля целостности сообщений	+
6.	Инфраструктура Открытых Ключей (PKI)	+
7.	Криптографические протоколы	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

17.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Дискретная математика	8	2	-	-	2	12

17.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

17.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

17.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	1	Множества и операции над ними. Проверка свойств операций над множествами. Решение комбинаторных задач.	2

17.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Капитонова и др. Лекции по дискретной математике. – СПб.: БХВ-Петербург, 2004 г.

2. Москинова Г.И. Дискретная математика. Математика для менеджера. М.: Логос, 2007 г.

3. Новиков Ф. А. Дискретная математика. СПб.: Питер, 2011 г.

4. Судоплатов С. В., Овчинникова Е. В. Дискретная математика: М.: Инфра-М, 2007г.

5. Триумфгородских М.В. Дискретная математика и математическая логика для информатиков, экономистов и менеджеров. М.: Диалог-МИФИ, 2011 г.

Дополнительная литература:

1. Краснов М.Л. и др. Вся Высшая математика. Том 7. М.: КомКнига, 2006 г.

2. Хаггарти Р. Дисретная математика для программистов. М.: Техносфера, 2012 г.

3. Поздняков С.Н.,Рыбин С.В. Дискретная математика. М.: Издательский центр «Академия», 2008 г.

4. Кузнецов О.П., Адельсон-Вельский Г.М., Дискретная математика для инженера. М.: Энергоатомиздат, 1998 г.

Программное обеспечение

Не требуется.

Базы данных, информационно-справочные и поисковые системы:

1. Интернет-страница ДИСКРЕТНАЯ МАТЕМАТИКА И МАТЕМАТИЧЕСКАЯ КИБЕРНЕТИКА http://new.math.msu.su/department/dm/dmmc/index.htm

2. Электронная библиотечная система АНО ДПО Парадигма.

17.10. Материально-техническое обеспечение учебной дисциплины

1. Аудитории для проведения лекционных и семинарских занятий оснащенное

проектором, ноутбуком, аудио оборудованием для просмотра видео.

2. Аудитории, оборудованные интерактивными досками.

3. Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет 1 сервер и 16 рабочих мест (MS Office).

17.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по основам обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств в информационных системах.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в форме систематической отработки лекционного материала.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам учебной дисциплины, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

17.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в форме тестирования.

Задание № 1

Мощностью конечного множества называется … а) количество элементов, входящих в это множество; б) множество всех подмножеств этого множества; в) количество всех подмножеств этого множества; г) произведение всех его элементов.

Задание № 2

Булеаном множества М называется …

а) множество подмножеств, объединение которых равно множеству М; б) любое множество попарно непересекающихся подмножеств множества М; в) множество попарно непересекающихся подмножеств множества М, объединение которых равно множеству М; г) множество всех его подмножеств.

Задание № 3

Декартовому произведению множеств A = {x ∈ N | 4 < x< 9} и

B = {x ∈ N| x >6} принадлежит упорядоченная пара …

Задание № 4

Количество упорядоченных пар, которые принадлежат прямому произведению множеств A = {*, +, #} и B = {1, 2, 3, 4} и в которых на первом месте стоит элемент #, равно …

а) 12; б) 3; в) 4; г) 9

Задание № 5

Отношение порядка, наряду с другими свойствами, обладает свойством …

а) симметричности;

б) антитранзитивности;

в) антисимметричности;

г) антирефлексивности.

Задание № 6

Множество (A \ C) ∪ (B∩ A) пусто, если B = {1, 2, 5, 9}, C = {2, 3, 4, 5,7} и A равно …

а) {3, 4, 5}; б) {2, 3, 4, 5}; в) {4, 5, 7, 8}; г) {3, 4, 7}.

Задание № 7

Даны заданные списками множества: A = {1, {a,2}, {1,a,b,c}, a, b}, B = {b, c, {2, a}}. Мощность симметрической разности множеств A и B равна …

(В ответе введите число.)

Задание № 8

На множестве M = {2, 3, 4, 7, 9, 27} задано отношение эквивалентности R = {(x, y)| НОД(x, y) > 1}. Класс эквивалентности элемента $[9]_R$ равен …

а) {3, 9, 27}; б) {9}; в) {3, 9}; г) {9, 27}.

Задание № 9

Инъективными функциями, заданными на множестве целых чисел Z, являются …

1) y = – x+1 ; 2) y = x–1 ; 3) $y = -x^2 + x - 1$;

4) $y = x^2 - x + 1$; 5) $y = x^3 - x^2 + 1$; 6) $y = x^3 + x - 1$.

Задание № 10

Мощность соответствия $G \subset X_1 \times X_2$, где $X_1 = \{1,2,3\}$, $X_2 = \{1,2,3,4\}$ и G ={(1, 1),(1, 2),(1, 3),(1, 4),(2, 1),(2, 2),(2, 3),(2, 4)} равна …

а) 8; б) 16; в) 7; г) 12.

18. Рабочая программа учебной дисциплины «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации»

18.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам организационно-правовых основ защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации (СКЗИ).

18.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

18.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством Российской Федерации, национальными стандартами, нормативными правовыми актами и нормативными методическими документами ФСБ России, Минцифры России, Банка России;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты

информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность использования нормативных правовых актов и нормативных методических документов для организации технологического процесса защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

правовые основы применения электронной подписи (ЭП);

принципы государственного регулирования в области СКЗИ: лицензирование, сертификация, контроль и надзор;

документы национальной системы стандартизации и стандарты международных организаций в области криптографической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

определять правила и процедуры управления системой защиты информации;

разрабатывать документы для получения лицензии на проведение работ и оказанию услуг, определенных постановлением Правительства Российской Федерации от 16.04.2012 г.

№ 313 для их представления в лицензирующий орган;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

навыками определения правил и процедур управления системой защиты информации;

навыками организации деятельности подразделений и специалистов в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

18.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 21 час.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	16
лекции (Л)	8
практические занятия (ПЗ)	-
семинары (С)	8
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	4
Вид промежуточной аттестации и его трудоемкость	1 (зачет)
Общая трудоемкость	21

18.5. Содержание учебной дисциплины

18.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации	Законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ. Правовые основы применения электронной подписи (ЭП). Понятие удостоверяющего центра (УЦ). Статус и функции УЦ. Аккредитация УЦ. Уполномоченный орган в сфере электронной подписи в Российской Федерации. Государственное регулирование в области СКЗИ: лицензирование, сертификация, контроль и надзор. Документы национальной системы стандартизации и стандарты международных организаций в области криптографической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. Деятельность Технического комитета по стандартизации «Криптографическая защита информации» ТК 26.

18.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Основные понятия криптографии	+
2.	Криптографические системы с симметричным ключом	+
3.	Криптографические системы с открытым ключом. Электронная подпись	+
4.	Хэш-функции. Обеспечение контроля целостности сообщений	+
5.	Инфраструктура Открытых Ключей (PKI)	+
6.	Криптографические протоколы	+
7.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

18.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации	8	-	-	8	4	20

18.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

18.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	2	Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации.	8

18.8. Практические занятия

В процессе изучения учебной дисциплины практические занятия не предусмотрены.

18.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013 г. – 184 с.

2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013 г. – 172 с.

3. Организационно-правовое обеспечение информационной безопасности: учебное пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / Под ред. А.А. Стрельцова. – М.: «Академия», 2008 г. - 256 с.

4. Семкин С.Н., Семкин А.Н. Основы правового обеспечения защиты информации: учеб. пособие для вузов. – М.: «Горячая линия – Телеком», 2008 г.

5. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учеб. пособие / Ю.Ю. Коваленко. – М.: Горячая линия – Телеком, 2012 г.

Дополнительная литература:

1. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005 г.

2. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 г.

3. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 05.12.2016 г. № 646.

4. Гражданский кодекс Российской Федерации. Принят Федеральным законом от 18 декабря 2006 г. № 230-ФЗ.

5. Закон РФ № 195-ФЗ от 30 декабря 2001 г. «Кодекс Российской Федерации об административных правонарушениях».

6. Закон РФ № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации».

7. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями и дополнениями).

8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

9. Федеральный закон Российской Федерации от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями).

10. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями).

11. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями и дополнениями).

12. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

13. Указ Президента Российской Федерации от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

14. Указ Президента Российской Федерации от 23.09.2005 г. № 1111 «О внесении изменения в перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 г. № 188».

15. Указ Президента Российской Федерации от 31.12.2016 г. № 683 «О Стратегии национальной безопасности Российской Федерации».

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

17. 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».

18. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608. В редакции Постановления Правительства от 21.04.2010 г. № 266 «Положение о сертификации средств защиты информации».

19. Распоряжение Правительства РФ от 12.07.2011 г. № 1214-р «О Плане подготовки правовых актов в целях реализации Федеральных законов "Об электронной подписи" и "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об электронной подписи"».

20. Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» (с изменениями и дополнениями).

21. Постановление Правительства РФ от 28.11.2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

22. Постановление Правительства РФ от 09.02.2012 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».

23. Постановление Правительства РФ от 16.04.2012 г. № 313 (в ред. Постановления Правительства РФ от 18.05.2017 г. № 596) «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)».

24. Национальный стандарт Российской Федерации ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

25. Национальный стандарт Российской Федерации ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

26. Национальный стандарт Российской Федерации ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».

27. Национальный стандарт Российской Федерации ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

28. Национальный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».

29. Национальный Стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27002-2021 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».

30. Рекомендации по стандартизации Росстандарта Р 50.1.115-2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля».

31. Национальный Стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

32. Национальный Стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

33. Стандарт ISO/IEC 27001:2013 «Information technology - Security techniques -

Information security management systems - Requirements»

34. ISO/IEC 27002:2013 «Information technology - Security techniques - Code of practice for information security management».

35. Приказ Минкомсвязи России от 29.09.2011 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».

36. Приказ Минкомсвязи России от 05.10.2011 г. № 250 «Об утверждении Порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

37. Приказ Минкомсвязи России от 23.11.2011 г. № 321 г. «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».

38. Приказ Минкомсвязи России от 30.11.2015 г. № 486 «Об утверждении административных регламентов предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и исполнения Министерством связи и массовых коммуникаций Российской Федерации государственной функции по осуществлению государственного контроля и надзора за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом "Об электронной подписи" и на соответствие которым эти удостоверяющие центры были аккредитованы».

39. Приказ ФАПСИ от 13.06.2001 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».

40. Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)».

41. Приказ ФСБ России от 12.04.2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (с изменениями и дополнениями).

42. Приказ ФСБ России от 27.12.2011 г. № 795 «Об утверждении Требований к

форме квалифицированного сертификата ключа проверки электронной подписи».

43. Приказ ФСБ России от 27.12.2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

44. Приказ ФСБ России от 29 декабря 2020 г. № 641 "Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по лицензированию 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)".

45. Письмо Банка России от 31.03.2008 г. № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга».

46. «Положение о порядке создания, ведения и хранения баз данных на электронных носителях». Утв. Банком России 21.02.2013 г. № 397-П (Ред. от 07.08.2015).

47. Письмо Банка России от 05.08.2013 г. № 146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети "Интернет».

48. Письмо Банка России от 24.03.2014 г. № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».

49. Стандарт ЦБ РФ СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». (Принят и введен в действие Распоряжением Банка России от 17.05.2014 г. № Р-399).

50. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Утв. Банком России 09.06.2012 г. № 382-П,

ред. от 05.06.2013г., с изм. и доп., вступившими в силу с 07.01.2014 г.

51. Распоряжение Банка России от 10.07.2014 г. № Р-556. О вводе в действие рекомендаций в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» РС БР ИББС-2.6-2014.

Программное обеспечение:

Не требуется.

Базы данных, информационно-справочные и поисковые системы:

Правовые справочно-поисковые системы («Гарант», «Консультант Плюс»);

Сайт Минцифры России, http://minsvyaz.ru/;

Сайт Минтруда России, http://rosmintrud.ru/;

Сайт ФСБ России, http://fsb.ru/;

Сайт Банка России, http://www.cbr.ru/;

Сайт Технического комитета по стандартизации «Криптографическая защита информации» ТК-26, http://tc26.ru/.

18.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

18.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основы нормативного правового обеспечения защиты информации с использованием криптографических средств. В процессе изучения учебной дисциплины упор делается на изучение нормативной правовой базы в области защиты информации с использованием криптографических средств в Российской Федерации, системы стандартизации Российской

Федерации, системы документов ФСБ России, Минцифры России, Банка России.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам защиты информации с использованием криптографических средств, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

18.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей [3]:

Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСБ России, Минцифры России, Банка России.

Методические документы в области защиты информации с использованием криптографических средств.

Технические документы (документация) в области защиты информации с использованием криптографических средств.

Плановые документы в области защиты информации с использованием криптографических средств.

Информационные документы в области защиты информации с использованием криптографических средств.

---

[3] Перечень вопросов определяется образовательными организациями, осуществляющими образовательную деятельность, самостоятельно

Национальные и международные стандарты в области защиты информации с использованием криптографических средств.

Лицензионные виды деятельности по защиты информации с использованием криптографических средств.

Правовые основы применения электронной подписи.

Понятие удостоверяющего центра (УЦ). Статус и функции УЦ.

Лицензирование, сертификация, контроль и надзор в области защиты информации с использованием криптографических средств в Российской Федерации.

Правила оформления документов для получения лицензии на проведение работ и оказание услуг по защите информации с использованием криптографических средств.

19. Рабочая программа учебной дисциплины «Основные понятия криптографии»

19.1 Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам решения задач защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации.

19.2 Место учебной дисциплины в структуре программы профессиональной переподготовки.

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

19.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

основные понятия криптографии;

основные криптографические алгоритмы, протоколы, используемые для защиты информации в средствах и системах информатизации;

б) уметь:

использовать криптографические средства защиты информации;

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

определять правила и процедуры управления системой защиты информации;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

19.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 6 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	4
лекции (Л)	4
практические занятия (ПЗ)	-
семинары (С)	-
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	6

19.5. Содержание учебной дисциплины

19.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Основные понятия криптографии	Задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований

19.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с симметричным ключом	+
2.	Криптографические системы с открытым ключом. Электронная подпись	+
3.	Хэш-функции. Обеспечение контроля целостности сообщений	+
4.	Инфраструктура Открытых Ключей (PKI)	+
5.	Криптографические протоколы	+
6.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

19.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Основные понятия криптографии	4	-	-	-	2	6

19.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

19.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

19.8. Практические занятия

В процессе изучения учебной дисциплины практические занятия не предусмотрены.

19.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2006 г.

3. Введение в криптографию / Под общ. ред. В.В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012 г. - 348 с.

4. Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011 г.

5. Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации. Учебник для академического бакалавриата. - М.: Юрайт, 2017 г.

6. Лось А.Б., Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. — Москва: Издательство Юрайт, 2022 г. - ISBN 978-5-534-12474-3.

7. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

8. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

9. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 г.

10. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые

основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

19.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

19.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные понятия криптографии. В процессе изучения учебной дисциплины упор делается на изучение основных понятий криптографии, основные криптографические алгоритмы, протоколы, используемые для защиты информации в средствах и системах информатизации.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

19.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

20. Рабочая программа учебной дисциплины «Криптографические системы с симметричным ключом»

20.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам использования криптографических систем с симметричным ключом, различия между синхронными и асинхронными шифрами.

20.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

20.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

основные криптографические алгоритмы, протоколы, используемые для защиты информации в средствах и системах информатизации;

б) уметь:

использовать криптографические средства защиты информации;

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

определять правила и процедуры управления системой защиты информации;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

20.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 10 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	8
лекции (Л)	2
практические занятия (ПЗ)	6
семинары (С)	-
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	10

20.5. Содержание учебной дисциплины

20.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Криптографические системы с симметричным ключом	Поточные шифры: синхронные и асинхронные шифры. Блочные шифры: DES, AES, ГОСТ Р 34.12-2018 («Магма», «Кузнечик»). Режимы работы блочных шифров. ГОСТ Р 34.13-2018. Проблемы распределения ключевой информации. Основы квантового распределения ключей (КРК).

20.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с открытым ключом. Электронная подпись	+
2.	Хэш-функции. Обеспечение контроля целостности сообщений	+
3.	Инфраструктура Открытых Ключей (PKI)	+
4.	Криптографические протоколы	+
5.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

20.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Криптографические системы с симметричным ключом	2	6	-	-	2	10

20.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

20.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

20.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	4	Криптографические системы с симметричным ключом. Поточные шифры. Различие между синхронными и асинхронными шифрами. Использование регистров сдвига с линейной и нелинейной обратной связью для реализации поточных шифров. Основные примеры блочных шифров.	6

20.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN ISBN 978-5-4383-0135-6.

3. Введение в криптографию / Под общ. ред. В.В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012 г. - 348 с.

4. Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011 г.

5. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр Академия, 2005 г. - 144 с.

6. Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации. Учебник для академического бакалавриата. - М.: Юрайт, 2017 г.

7. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. - М.: КУДИЦ-ОБРАЗ, 2002 г.

8. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

9. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

10. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

20.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

20.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные понятия криптографических систем с симметричным ключом. В процессе изучения учебной дисциплины упор делается на изучение основных понятий поточных шифров, блочные шифры.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения определять криптографические системы с симметричным ключом, поточные шифры. Отличать различие между синхронными и асинхронными шифрами. Вопросы использования регистров сдвига с линейной и нелинейной обратной связью для реализации поточных шифров. Рассматриваются основные примеры блочных шифров.

20.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

21. Рабочая программа учебной дисциплины «Криптографические системы с открытым ключом. Электронная подпись»

21.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам использования криптографических систем с открытым ключом, электронной подписи.

21.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

21.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты

информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством;

способность применения способов и технологии применения криптографии в решении задач аутентификации и построения юридически значимого документооборота.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

математические основы, криптографические системы с открытым (асимметричным) ключом;

основные виды электронной подписи, средства электронной подписи;

б) уметь:

использовать криптографические системы с открытым ключом;

правила использования электронной подписи в соответствии с Федеральным законом от 06.04.2011 г. № 63 «Об электронной подписи»;

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

определять правила и процедуры управления системой защиты информации;

в) владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие

государственную тайну с использованием СКЗИ;

21.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 12 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	10
лекции (Л)	4
практические занятия (ПЗ)	6
семинары (С)	-
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	12

21.5. Содержание учебной дисциплины

21.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Криптографические системы с открытым ключом. Электронная подпись.	Математические основы. Криптографические системы с открытым (асимметричным) ключом: система RSA, система Эль-Гамаля (ElGamal). Криптография с использованием эллиптических кривых. Электронная подпись. Схемы электронной подписи: RSA, Эль-Гамаля (ElGamal), Шнорра (Schnorr), ГОСТ Р 34.10-2018 и (EC)DSA. Облачная электронная подпись. Основные виды электронной подписи, средства электронной подписи, сертификат ключа проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63 «Об электронной подписи»

21.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с симметричным ключом	+
2.	Хэш-функции. Обеспечение контроля целостности сообщений	+
3.	Инфраструктура Открытых Ключей (PKI)	+
4.	Криптографические протоколы	+
5.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

21.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Криптографические системы с открытым ключом. Электронная подпись.	4	6	-	-	2	12

21.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

21.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

21.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	5	Криптографические системы с открытым ключом. Электронная подпись. Криптосистемы RSA, Эль-Гамаля (ElGamal) и (EC)DSA	6

21.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN

ISBN 978-5-4383-0135-6.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

4. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

5. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

6. Алабина Ю.Ф., Чаплыгин В.Е., Чефранова А.О. Удостоверяющий центр ViPNet: учебно – методическое пособие. М.: 11 – формат, 2017 г. - 256 с.

7. Аристархов И.В., Баушев С.В., Гаценко О.Ю., Горбачев И.Е., Камышев С.Н., Кузьмин А.С., Максимов С.В., Маршалко Г.Б., Нездоровин Н.В., Сабанов А.Г., Самонов А.В., Синев С.Г. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику. Учебное пособие. СПб.: БХВ –Петербург, 2016 г. - 304 с.

8. Горбатов В.С., Полянская О.Ю. Инфраструктура открытых ключей: Учебное пособие. М.: Интернет – Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2013 г. - 368 с.

9. Иванов О.В., Чугринов А.В., Захаров Л.Н., Зырянов А.В., Калинин С.В., Солтанов А.Г. «Построение юридически значимого электронного документооборота на основе инфраструктуры открытых ключей». — М.: РФК-Имидж Лаб, 2008 г. — 224 с.: ил.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

21.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, лицензионными программными и аппаратными средствами защиты информации,

позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки, отработать соответствующий функционал. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

21.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные понятия криптографических систем с открытым ключом. В процессе изучения учебной дисциплины упор делается на изучение основных видов электронной подписи, средств электронной подписи, сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63 «Об электронной подписи».

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения определять криптографические системы с открытым ключом, использования электронной подписи.

21.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

22. Рабочая программа учебной дисциплины «Хэш-функции. Обеспечение контроля целостности сообщений»

22.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам использования хэш-функции и контроля целостности сообщений.

22.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

22.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

требования обеспечения контроля целостности сообщений;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

определять правила и процедуры управления системой защиты информации;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

22.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 6 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	4
лекции (Л)	2
практические занятия (ПЗ)	2
семинары (С)	-
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	6

22.5. Содержание учебной дисциплины

22.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Хэш-функции. Обеспечение контроля целостности сообщений	Хэш-функции и контроль целостности сообщений. Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11-2018

22.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с симметричным ключом	+
2.	Криптографические системы с открытым ключом. Электронная подпись	+
3.	Инфраструктура Открытых Ключей (PKI)	+
4.	Криптографические протоколы	+
5.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

22.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Хэш-функции. Обеспечение контроля целостности сообщений	2	2	-	-	2	6

22.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

22.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

22.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	6	Хэш-функции SHA-1, SHA-2, SHA-3, ГОСТ Р 34.11-2018	2

22.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN ISBN 978-5-4383-0135-6.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

4. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

5. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

6. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003 г.

7. Лось А.Б., Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022 г. - 473 с. - ISBN 978-5-534-12474-3.

8. Черёмушкин А.В. Криптографические протоколы. Основные свойства и

уязвимости. – М.: Академия, 2009 г.

9. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

22.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

22.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные понятия криптографических систем с открытым ключом. В процессе изучения учебной дисциплины упор делается на изучение основных вопросов обеспечения контроля целостности сообщений, использования хэш-функций.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях.

На практических занятиях развиваются умения определять Хэш-функции SHA-1, SHA-2, SHA-3.

22.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

23. Рабочая программа учебной дисциплины «Инфраструктура открытых ключей (PKI)»

23.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом.

23.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин программы профессиональной переподготовки: «Криптографические протоколы», «Обеспечение безопасности информации с использованием СКЗИ».

23.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

способность решать вопросы реализации PKI;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

основные понятия, термины и определения в области PKI;

основные стандарты в области PKI;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

определять организационные и технические вопросы реализации PKI;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

23.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 20 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	18
лекции (Л)	6
практические занятия (ПЗ)	4
семинары (С)	-
лабораторные работы (ЛР)	8
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	20

23.5. Содержание учебной дисциплины

23.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Инфраструктура открытых ключей (PKI)	Основные понятия, термины и определения в области PKI. Управление сертификатами и ключами. Архитектура, основные компоненты PKI, их функции и взаимодействие. Основные стандарты в области PKI: Стандарты серии X (X.509). Стандарты криптографии с открытым ключом PKCS

23.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с симметричным ключом	+
2.	Криптографические системы с открытым ключом. Электронная подпись	+
3.	Криптографические протоколы	+
4.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

23.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Инфраструктура открытых ключей (PKI)	6	4	8	-	2	20

23.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	7	Вопросы реализации PKI (организационные, технические). Основные стандарты PKI (X.509, PKCS)	8

23.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

23.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	7	Вопросы реализации PKI (организационные, технические). Основные стандарты PKI (PKCS, X.509)	4

23.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN ISBN 978-5-4383-0135-6.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

4. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

5. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

6. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003 г.

7. Лось А.Б., Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И.

Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022 г. — 473 с. - ISBN 978-5-534-12474-3.

8. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 г.

9. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

10. Горбатов В.С., Полянская О.Ю. Инфраструктура открытых ключей: Учебное пособие. М.: Интернет – Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2013 г. - 368 с.

11. Иванов О.В., Чугринов А.В., Захаров Л.Н., Зырянов А.В., Калинин С.В., Солтанов А.Г. «Построение юридически значимого электронного документооборота на основе инфраструктуры открытых ключей». — М.: РФК-Имидж Лаб, 2008 г. — 224 с.: ил.

12. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 г.

13. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

23.10. Материально-техническое обеспечение учебной дисциплины

Лекционные, практические, самостоятельные и лабораторные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

23.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные понятия криптографических систем с открытым ключом. В процессе изучения учебной дисциплины упор делается на изучение основных вопросов ролей, политик, аппаратного, программного обеспечения и процедур, необходимых для создания, управления, распространения, использования, хранения и отзыва цифровых сертификатов, а также управления шифрованием с открытым ключом.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения реализации организационных и технических вопросов PKI.

23.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

24. Рабочая программа учебной дисциплины «Криптографические протоколы»

24.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам использования основных протоколов аутентификации и обмена ключей, обмена защищёнными данными.

24.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующей учебной дисциплины программы профессиональной переподготовки: «Обеспечение безопасности информации с использованием СКЗИ».

24.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность определять задачи защиты информации, решаемые криптографическими методами, и соответствующие виды криптографических преобразований;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

разрабатывать необходимые документы по проведению работ в области защиты

информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минцифры России, Банка России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

основные криптографические алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;

б) уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ.

24.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 12 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего) ,в том числе:	9
лекции (Л)	3
практические занятия (ПЗ)	-
семинары (С)	6
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	1 (зачет)
Общая трудоемкость	12

24.5. Содержание учебной дисциплины

24.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Криптографические протоколы	Понятие криптографического протокола. Протоколы аутентификации. Основные протоколы аутентификации. Сравнение протоколов аутентификации. Безопасное сетевое взаимодействие. Аутентификационный сервис Kerberos. Протокол удаленного безопасного входа SSH. Протоколы передачи данных. Обмен защищёнными данными. Безопасность сетевого трафика. Протоколы сетевого уровня. Безопасность на транспортном уровне. Протоколы транспортного уровня.Протокол TLS/SSL. Безопасность на прикладном уровне. Стандарт защиты электронной почты S/MIME и программное обеспечение PGP. Протоколы распределения ключей. Протоколы передачи ключей на симметричных криптосхемах (протокол Керберос). Протоколы передачи ключей на асимметричных криптосхемах (протокол X.509). Протоколы обмена ключами (IKE). Протокол SESPAKE выработки общего ключа саутентификацией на основе пароля (Документ Р 50.1.115-2016, рекомендации по стандартизации Росстандарта)

24.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Криптографические системы с симметричным ключом	+
2.	Криптографические системы с открытым ключом. Электронная подпись	+
3.	Хэш-функции. Обеспечение контроля целостности сообщений	+
4.	Инфраструктура Открытых Ключей (PKI)	+
5.	Обеспечение безопасности информации с использованием СКЗИ	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

24.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Криптографические протоколы	3	-	-	6	2	11

24.6. Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

24.7. Семинары

№ п/п	№ раздела учебной дисциплины	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	8	Основные протоколы аутентификации и обмена ключей. Сравнение протоколов аутентификации. Безопасное сетевое взаимодействие	3
2.	8	Обмен защищёнными данными. Безопасность сетевого трафика. Протоколы сетевого уровня. Безопасность на транспортном уровне. Протоколы транспортного уровня. Протокол TLS/SSL. Безопасность на прикладном уровне. Стандарт защиты электронной почты S/MIME и программное обеспечение PGP	3

24.8. Практические занятия

В процессе изучения учебной дисциплины практические занятия не предусмотрены.

24.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 г.

2. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

4. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN 978-5-4383-0135-6.

5. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

6. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

7. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 г.

8. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003 г.

9. Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

24.10. Материально-техническое обеспечение учебной дисциплины

Лекционные и самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности информации. Рабочие места (пользовательские терминалы) слушателей объединены в

локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

24.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основные протоколы аутентификации и обмена ключей. В процессе изучения учебной дисциплины упор делается на изучение протоколов аутентификации, безопасное сетевое взаимодействие, обмен защищёнными данными.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам учебной дисциплины, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

24.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Какие требования предъявляются к криптографическим протоколам?

Что понимается под открытыми системами и чем регламентируется их взаимодействие?

Кроме наличия злоумышленника, какие еще предположения выдвигаются относительно участников криптопротокола?

Каковы основные классы прикладных криптографических протоколов?

Чем протокол с арбитражем отличается от протокола с судейством?

Что такое самодостаточный протокол? Какие основные виды атак на криптопротоколы?

Для чего предназначены протоколы типа SSL?

Какими криптографическими методами обеспечивается конфиденциальность и целостность данных в SSL?

Какого типа сертификаты используются SSL для организации взаимодействия с инфраструктурой открытых ключей?

Каково предназначение системы протоколов безопасных электронных транзакций SET?

Для чего предназначен протокол SESPAKE и влияют ли на его работу связные протоколы, действующие в сети?

Каковы основные преимущества обеспечения безопасности информации на основе SESPAKE?

25. Рабочая программа учебной дисциплины «Обеспечение безопасности информации с использованием СКЗИ»

25.1. Цель учебной дисциплины – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством Российской Федерации, документов национальной системы стандартизации, нормативными правовыми актами и нормативными методическими документами ФСБ России, Минцифры России, Банка России.

25.2. Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Нормативные правовые основы защиты информации с использованием СКЗИ в Российской Федерации», «Основные понятия криптографии», «Криптографические системы с симметричным ключом», «Криптографические системы с открытым ключом. Электронная подпись», «Хэш-функции. Обеспечение контроля целостности сообщений», «Инфраструктура Открытых Ключей (PKI)», «Криптографические протоколы».

Данная учебная дисциплина является итоговой учебной дисциплиной программы профессиональной переподготовки.

25.3. Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) слушателями таких компетенций, как:

а) общепрофессиональных:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации в соответствии с законодательством;

способность использовать достижения науки и техники в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

способность организовывать технологический процесс защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств защиты информации;

в проектной деятельности:

способность разрабатывать необходимые документы по проведению работ в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

в эксплуатационной деятельности:

способность выполнять работы по установке, настройке, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных криптографических средств защиты информации.

В результате освоения дисциплины слушатель должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Слушатель должен:

а) знать:

требования законодательства Российской Федерации, документов национальной системы стандартизации, нормативных правовых актов и нормативных методических документов ФСБ России, Минцифры России, Банка России по вопросам защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

основные криптографические алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;

нормативные правовые основы деятельности органа криптографической защиты, удостоверяющего центра и юридически значимого документооборота;

основные понятия криптографии;

основные криптографические алгоритмы, протоколы, используемые для защиты информации в средствах и системах информатизации;

общие принципы функционирования средств криптографической защиты информации в компьютерных сетях;

принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы;

типовые методы и протоколы идентификации, аутентификации и авторизации в

компьютерных сетях;

номенклатура, функциональное назначение и основные характеристики средств и систем защиты информации от НСД;

нормативные требования к составу и содержанию средств и систем защиты информации от НСД;

принципы построения защищенного документооборота с использованием средств электронной подписи и виртуальных частных сетей;

б) уметь:

использовать криптографические средства защиты информации;

определять параметры настройки программного обеспечения системы защиты информации;

определять правила и процедуры управления системой защиты информации;

производить установку, монтаж, настройку информационных систем, защищенных с использованием криптографических средств, в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;

использовать криптографические средства защиты информации;

корректно эксплуатировать средства электронной подписи;

устанавливать, настраивать и эксплуатировать программные и программно-аппаратные средства защиты информации различных производителей (в том числе средства электронной подписи и программно-аппаратные компоненты PKI);

формировать ключи и сертификаты с использованием различных средств электронной подписи;

проводить монтаж (для программных средств - установку) средств и систем криптографической защиты информации;

проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения, средств и систем криптографической защиты информации;

в) владеть:

навыками работы с действующей нормативной правовой и методической базой в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием СКЗИ;

навыками действий в нештатных ситуациях при эксплуатации СКЗИ;

навыками работы с ключевой информацией;

навыками обеспечения защиты информации от несанкционированного доступа при ее хранении и обработке в организации с использованием средств криптографической защиты

информации;

навыками защиты автоматизированных систем предприятия с применением средств криптографической защиты;

навыками проведения необходимых организационных мероприятий.

25.4. Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 63 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	61
лекции (Л)	8
практические занятия (ПЗ)	26
семинары (С)	-
лабораторные работы (ЛР)	27
Самостоятельная работа (СР, всего)	2
Вид промежуточной аттестации и его трудоемкость	-
Общая трудоемкость	63

25.5. Содержание учебной дисциплины

25.5.1. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Обеспечение безопасности информации с использованием СКЗИ	Основные положения Инструкции, утвержденной приказом ФАПСИ от 13.06.2001 № 152, 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. Требования по эксплуатации шифровальных (криптографических) средств защиты информации в соответствии с Положением ПКЗ-2005, утвержденным приказом ФСБ России от 09.02.2005 № 66. Требования приказов ФСБ России от 27.12.2011 № 795 и № 796 соответственно к форме квалифицированного сертификата ключа проверки ЭП, к средствам ЭП и к средствам УЦ. Структура СКЗИ. Состав программного обеспечения СКЗИ. Нештатные ситуации при эксплуатации СКЗИ. Работа с ключевой информацией. Обеспечение защиты информации от несанкционированного доступа при ее хранении и обработке в организации с использованием средств криптографической защиты информации. Защита автоматизированных систем предприятия с применением средств криптографической защиты. Необходимые организационные мероприятия (назначение ответственных лиц, разработка внутренних документов

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		организации и т.д.). Назначение и порядок использования конкретных СКЗИ, реализующих базовый функционал по криптографической защите информации ограниченного доступа. Назначение и порядок использования СКЗИ (ViPNet CSP, КриптоПро CSP), реализующих базовый функционал по криптографической защите информации ограниченного доступа. Назначение, состав и порядок использования программно-аппаратных средств автоматизации деятельности Удостоверяющих центров (ПАК «КриптоПро УЦ»). Назначение, состав и порядок использования СКЗИ (ПК ViPNet Client (Windows, Linux, Android), ПК ViPNet Coordinator VA), применяемых для обеспечения безопасности передачи по каналам связи информации ограниченного доступа. Назначение и порядок использования СКЗИ (ПО КриптоАРМ, ПК ViPNet PKI Client), применяемых для обеспечения защиты от несанкционированного доступа (НСД) к информации ограниченного доступа

25.5.2. Разделы учебной дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) учебных дисциплин (модулей)	№№ разделов данной учебной дисциплины, необходимых для изучения обеспечиваемых (последующих) учебных дисциплин
		1
1.	Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации	+
2.	Основные понятия криптографии	+
3.	Криптографические системы с симметричным ключом	+
4.	Криптографические системы с открытым ключом. Электронная подпись	+
5.	Хэш-функции. Обеспечение контроля целостности сообщений	+
6.	Инфраструктура Открытых Ключей (PKI)	+
7.	Криптографические протоколы	+

Примечания:

«+» - раздел обеспечивает изучение данной учебной дисциплины;

«-» - раздел не обеспечивает изучение данной учебной дисциплины.

25.5.3. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Обеспечение безопасности информации с использованием СКЗИ	8	26	27	-	2	63

25.6. Лабораторный практикум

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Количество времени, отводимого на проведение лабораторной работы (час.)
1.	9	Установка и настройка КриптоПро CSP (Windows, Linux). Установка и настройка ViPNet CSP. Установка, настройка ПК ViPNet Client (Windows, Linux, Android), работа с Деловой Почтой. Установка, настройка ПК ViPNet Coordinator VA, создание защищенного канала связи	27

25.7. Семинары

В процессе изучения учебной дисциплины семинары не предусмотрены.

25.8. Практические занятия

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий	Количество времени, отводимого на проведение практического занятия (час.)
1.	9	Инфраструктура открытых ключей (PKI). Создание, применение электронной подписи. Работа с различными типами ключевых носителей с помощью КриптоПро CSP, ViPNet CSP. Процедура подписания и проверки подлинности электронной подписи с помощью ПО КриптоАРМ и ПК ViPNet PKI Client. Процедура шифрования и расшифровки с помощью ПО КриптоАРМ и ПК ViPNet PKI Client	26

25.9. Учебно-методическое и информационное обеспечение учебной дисциплины:

Основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005 г.

2. Алабина Ю.Ф., Чаплыгин В.Е., Чефранова А.О. Удостоверяющий центр ViPNet: учебно – методическое пособие. М.: 11 – формат, 2017 г. - 256 с.

3. Аристархов И.В., Баушев С.В., Гаценко О.Ю., Горбачев И.Е., Камышев С.Н., Кузьмин А.С., Максимов С.В., Маршалко Г.Б., Нездоровин Н.В., Сабанов А.Г., Самонов А.В., Синев С.Г. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику. Учебное пособие. СПб.: БХВ –Петербург, 2016 г. - 304 с.

4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2006 г.

5. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб.: ИЦ «Интермедия», 2019 г. - 384 с. - ISBN 978-5-4383-0135-6.

6. Введение в криптографию / Под общ. ред. В.В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012 г. - 348 с.

7. Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011 г.

8. Горбатов В.С., Полянская О.Ю. Инфраструктура открытых ключей: Учебное пособие. М.: Интернет – Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2013 г. - 368 с.

9. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Академия, 2009 г.

10. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр Академия, 2005 г. - 144 с.

11. Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации. Учебник для академического бакалавриата. - М.: Юрайт, 2017 г.

12. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. - М.: КУДИЦ-ОБРАЗ, 2002 г.

13. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005 г.

14. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003 г.

15. Иванов О.В., Чугринов А.В., Захаров Л.Н., Зырянов А.В., Калинин С.В., Солтанов А.Г. «Построение юридически значимого электронного документооборота на основе инфраструктуры открытых ключей». — М.: РФК-Имидж Лаб, 2008 г. — 224 с.: ил.

16. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. - М.: Горячая линия- Телеком, 2012 г. — 141 с.

17. Кэрриэ Б. Криминалистический анализ файловых систем. - М.: Питер, 2007 г.

18. Лось А.Б., Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022 г. — 473 с. - ISBN 978-5-534-12474-3.

19. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г.

20. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:

МЦНМО, 2006 г.

21. Проскурин В.Г. Защита программ и данных. Учебное пособие для вузов. М.: Академия, 2012 г.

22. Проскурин, В.Г. Защита в операционных системах. – М.: Академия, 2012 г.

23. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. – М.: Горячая линия–Телеком, 2010 г.

24. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008 г.

25. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003 г. - 192 с.

26. Федотов Н.Н. Форензика - компьютерная криминалистика. М.: Юридический мир, 2007 г.

27. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2022 г. — 209 с. - ISBN 978-5-9916-7088-3.

28. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2022 г. — 245 с. — ISBN 978-5-9916-7090-6.

29. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 г.

30. Шнаер Б. «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002 г.

Список дополнительной литературы приведен в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

Программное обеспечение: не требуется.

Базы данных, информационно-справочные и поисковые системы указаны в дисциплине «Нормативные правовые основы защиты информации с использованием криптографических средств в Российской Федерации», п.17.9.

25.10. Материально-техническое обеспечение учебной дисциплины

Лекционные и самостоятельные занятия проводятся в специализированном компьютерном классе (аудитории), аттестованном в установленном порядке, оснащенном автоматизированными рабочими местами, аттестованными по требованиям безопасности

информации. Рабочие места (пользовательские терминалы) слушателей объединены в локальную вычислительную сеть, имеется подключение к сети Internet. Рабочие места оснащены современным оборудованием, стендами, приборами, сертифицированными программными и аппаратными средствами защиты информации, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки. Рабочее место преподавателя оснащено компьютером (сервером), мультимедийным проектором, экраном, доской.

При изучении учебной дисциплины используются специализированные учебные лабораторные комплексы для ознакомления студентов с:

методической документацией к изучаемым СКЗИ;

процедурой установки и настройки СКЗИ согласно технической документацией;

процедурой настройки работы СКЗИ с отчуждаемыми ключевыми носителями;

процедурой генерации ключей электронной подписи с помощью различных СКЗИ;

процедурой подписания электронных документов электронной подписью, проверки электронной подписи на документах, шифрования и расшифрования зашифрованных электронных документов.

Специализированный компьютерный класс (аудитория) оснащается необходимым комплектом лицензионного программного обеспечения, сертифицированными программными и программно-аппаратными средствами защиты информации, в том числе отечественного производства (состав определяется в рабочих программах разделов модуля и подлежит обновлению при необходимости), реализующие базовый функционал СКЗИ в том числе в УЦ, VPN-сетях, при архивировании и защите от НСД на рабочих станциях и серверах, защите данных в компьютерных сетях.

Для проведения занятий необходимо иметь:

рабочую станцию с предустановленной операционной системой Windows или Linux;

предустановленные на рабочей станции средства виртуализации;

лицензии на программные СКЗИ;

программно-аппаратные СКЗИ;

набор виртуальных рабочих станций с операционной системой Windows и Linux.

25.11. Методические рекомендации по организации изучения учебной дисциплины

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по основам обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств в

информационных системах.

Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам учебной дисциплины, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости слушателей.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах:

систематическая отработка лекционного материала;

подготовка к групповым и семинарским занятиям.

В ходе самостоятельной работы слушатели получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях формируются навыки использования программных и аппаратных средств СКЗИ.

Практические занятия демонстрации методов и средств подписания и шифрования электронных документов, построения защищенных виртуальных частных сетей проводятся в специализированных лабораториях (компьютерном классе с предварительной установкой необходимого программного обеспечения). Занятия проводятся на двух-пяти рабочих местах количество рабочих мест (зависит от количества слушателей в учебной группе). За каждым рабочим местом закреплен преподаватель, развернуто программное обеспечение, необходимое для проведения практических и лабораторных работ.

25.12. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы слушателей и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний слушателей:

Опишите порядок учета СКЗИ.

Перечислите требования к форме квалифицированного сертификата ЭП юридического лица.

Перечислите требования к форме квалифицированного сертификата ЭП физического

лица.

Перечислите все классы средств электронной подписи.

Перечислите способы защиты информации от несанкционированного доступа, в том числе с помощью СКЗИ (не менее трех).

Орган криптографической защиты и его функции.

Функции криптопровайдеров.

Состав и функции каждого компонента ПАК «КриптоПро УЦ».

Опишите основные способы хранения ключевой информации для ViPNet Client для Windows.

Способы хранения электронной подписи в электронном документе.