Негосударственное образовательное частное учреждение
дополнительного профессионального образования
«Межрегиональный учебный центр»

Для служебного пользования
Экз. № 1

СОГЛАСОВАНО
Начальник 1 управления
ФСТЭК России

_____ Н.М.Мартинец

«__» _____ 2018 г.

УТВЕРЖДАЮ
Директор НОЧУ ДПО «МУЦ»

_____ Е.П.Семенова

«__» _____ 2018 г.

Программа
профессиональной переподготовки
«Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

Москва 2017

Оглавление

Общие положения----------3
Цель реализации программы профессиональной переподготовки----------4
Требования к квалификации поступающего на обучение----------7
Планируемые результаты обучения----------7
Условия реализации программы----------12
Формы аттестации и оценочные материалы----------15
Учебный план----------16
Примерный календарный учебный график----------19
Структура и краткое содержание учебного курса----------19
Организационно-правовые основы технической защиты конфиденциальной информации----------24
Аппаратные средства вычислительной техники----------42
Системы и сети передачи информации----------53
Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам----------64
Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа----------76
Техническая защита конфиденциальной информации от специальных воздействий----------90
Организация защиты конфиденциальной информации на объектах информатизации----------100
Аттестация объектов информатизации по требованиям безопасности информации----------116
Контроль состояния технической защиты конфиденциальной информации----------129

1.Общие положения.

Настоящая программа профессиональной переподготовки **«Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»** разработана с учетом требований Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» и в соответствии с «Методическими рекомендациями по разработке программ профессиональной переподготовке и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации», утвержденными ФСТЭК России 4 апреля 2015 года и «Типовой программой профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»», утвержденной ФСТЭК России 30 апреля 2015 года.

Программа профессиональной переподготовки реализуется в **Негосударственном образовательном частном учреждении дополнительного профессионального образования «Межрегиональный учебный центр».**

Разработчик:

1. Завалихина Руслана Султановна кандидат психологических наук-учебного центра.

Программа профессиональной переподготовки обсуждена на заседании методического совета Негосударственного образовательного частного учреждения дополнительного профессионального

образования «Межрегиональный учебный центр». Протокол № 3 от 21.03.2017 года.

В тексте используется следующие сокращенные названия:

1. ТЗКИ – техническая защита конфиденциальной информации;
2. ФСТЭК – Федеральная служба по техническому и экспортному контролю;
3. НСД – несанкционированный доступ;
4. ПО – программное обеспечение;
5. ЭВМ – электронно-вычислительная машина;
6. ВТСС – вспомогательные технические средства и системы;
7. ГОСТ – Государственный стандарт;
8. ТКУИ – технические каналы утечки информации;
9. ДОТ – дистанционные образовательные технологии;
10. ОУ – образовательное учреждение;
11. ПЭМИН – побочное электромагнитное излучение и наводка

1. Цель реализации программы профессиональной переподготовки.

Целью реализации программы профессиональной переподготовки является: формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации.

Специалист, проходящий обучение по программе профессиональной переподготовки **«Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»** готовиться к следующим видам профессиональной деятельности: организационно-управленческой;

проектно-деятельностной;

эксплуатационной.

1. Организационно-управленческий вид профессиональной деятельности включает в себя:

планирование деятельности по обеспечению ТЗКИ (разработка документов, регламентирующих в организации политики по обеспечению ТЗКИ);

организация внедрения и применения политик по обеспечению ТЗКИ в организации;

проведение контроля (мониторинга) и анализа применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

поддержка и совершенствование деятельности по обеспечению ТЗКИ в организации;

2. Проектно-деятельностный вид профессиональной деятельности включает в себя:

определение ТКУИ на объектах информатизации и угроз безопасности информатизации в автоматизированных системах;

формирование требований к обеспечению ТЗКИ на объектах информатизации;

разработка способов и средств для обеспечения ТЗКИ на объектах информатизации;

внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации;

3. Эксплуатационный вид профессиональной деятельности включает в себя;

обеспечение ТЗКИ в ходе эксплуатации объектов информатизации;

обеспечение ТЗКИ при выводе из эксплуатации объектов информатизации.

Объекты профессиональной деятельности:

объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средств их обеспечения, а также помещения, предназначенные для ведения секретных (конфиденциальных) переговоров (выделенные (защищаемые)помещения);

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

способы и средства, используемые для обеспечения технической защиты информации;

система нормативных правовых актов, методических документов и национальных стандартов в области технической защиты информации.

Обучающиеся по программе профессиональной переподготовки готовиться к решению следующих задач профессиональной деятельности:

1. Организационно-управленческие:

планирование деятельности по обеспечению ТЗКИ (разработка документов, регламентирующих в организации политики по обеспечению ТЗКИ);

организация внедрения и применения политик по обеспечению ТЗКИ в организации;

проведение контроля (мониторинга) и анализа применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

поддержка и совершенствование деятельности по обеспечению ТЗКИ в организации;

2. В проектной деятельности:

определение ТКУИ на объектах информатизации и угроз безопасности информатизации в автоматизированных системах;

формирование требований к обеспечению ТЗКИ на объектах информатизации;

разработка способов и средств для обеспечения ТЗКИ на объектах информатизации;

внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации;

3. В эксплуатационной деятельности

обеспечение ТЗКИ в ходе эксплуатации объектов информатизации;

обеспечение ТЗКИ при выводе из эксплуатации объектов информатизации.

2. Требования к квалификации поступающего на обучение.

Уровень образования лица, поступающего на обучение: 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 РФ, в соответствии с ч. 8 ст. 11 Федерального закона от 29.12.2012г №273-ФЗ «Об образовании в Российской Федерации», подтвержденное документом об образовании.

3. Планируемые результаты обучения.

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

а) общепрофессиональных;

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

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

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

б) профессиональных;

в организационно-управленческой деятельности:

способность планировать деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность проводить контроль (мониторинг) и анализ применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ в организации;

в проектной деятельности:

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

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 информатизации;

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

В результате освоения программы профессиональной переподготовки обучающийся должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности.

Перечень знаний, умений и навыков обучающихся формируется на основе нижеприведенного списка с учетом направленности конкретных программ профессиональной переподготовки.

Освоившие программу должны:

а) **знать:**

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

основы построения информационных систем и формирования информационных ресурсов;

виды конфиденциальной информации;

перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации;

физические основы возникновения, классификацию и характеристики ТКУИ;

угрозы безопасности информации;

цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации;

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

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

порядок проведения аттестации объектов информатизации по требованиям безопасности информации;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защиты информации от

несанкционированного доступа (НСД) и по защите информации от специальных воздействий);

общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

требования к средствам ТЗКИ и контроля защищенности информации; средства ТЗКИ и контроля защищенности информации, порядок их применения;

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

программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей;

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;

порядок организации и проведения контроля защищенности информации;

типовую структуру, задачи и полномочия подразделения по ТЗКИ;

требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объекта информатизации;

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:

работать с действующей нормативной правовой и методической базой в области защиты информации;

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

определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации;

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации;

разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в области ТЗКИ;

проводить работы по категорированию, классификации защищенности автоматизированных систем от НСД к информации, аттестации объектов информатизации;

применять подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений требований по ТЗКИ;

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

применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации;

проводить организационные и технические мероприятия по ТЗКИ;

в) владеть навыками:

организации деятельности подразделений и специалистов в области ТЗКИ в органах государственной власти и организациях;

работы с действующей нормативной правовой и методической базой в области защиты информации;

разработки необходимой документации по вопросам организации ТЗКИ в органах государственной власти и организациях;

выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты;

определения задач, способов и средств ТЗКИ и контроля защищенности информации;

использования программных и аппаратных средств ТЗКИ и контроля защищенности информации;

проведения организационных и технических мероприятий по ТЗКИ, контролю защищенности информации;

работы с современными операционными системами;

установки и настройки современных операционных систем с учетом требований по безопасности информации;

установки и настройки современных средств защиты информации, системного и прикладного программного обеспечения с учетом требований по безопасности информации;

разработки, документирования баз данных, компьютерных сетей с учетом требований по безопасности информации;

работы в компьютерных сетях с учетом требований по безопасности информации;

обследования, категорирования и аттестации объектов информатизации по требованиям безопасности информатизации;

применения экспертно-документального и инструментального методов, метода проверки соответствия настройки элементов системы защиты информации требованиям безопасности информации с проведением проверки подсистем защиты информации от НСД, проверки программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации при проведении аттестационных испытаний объектов информатизации по требованиям безопасности информации.

4. Условия реализации программы.

Программа рассчитана на 560 ч. (8 часов в день).

Форма обучения – очно-заочная, дистанционная.

Кабинеты оснащены современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки.

Компьютерный класс оборудован современной вычислительной техникой для занятий по учебным дисциплинам, из расчета одно рабочее место на одного обучающегося, при проведении занятий в данных классах.

Негосударственное образовательное частное учреждение дополнительного профессионального образования «Межрегиональный учебный центр» имеет необходимый комплект лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В рамках программы профессиональной переподготовки предусмотрено проведение практических занятий с участием специалистов высшего уровня квалификации в области технической защиты информации (ТЗИ), представителей российских компаний, государственных организаций.

Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, изданными за последние 10 лет, из расчета не менее одного экземпляра на 4-5 обучающихся.

В фонд дополнительной литературы, помимо учебной, включены официальные, справочно-библиографические и специализированные периодические издания, в том числе, правовые нормативные акты и нормативные методические документы в области информационной безопасности в расчете один-два экземпляра на каждые 20 обучающихся.

Обучающимся обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам по тематике защиты информации.

Передача программы профессиональной переподготовки другой образовательной организации допускается при создании условий и соблюдении требований законодательства Российской Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения федеральных государственных органов, в ведении которых находятся организации, осуществляющие образовательную деятельность.

Внесение изменений в программы профессиональной переподготовки осуществляется в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования и порядком обращения со служебной информацией ограниченного распространения.

Вся программа, а также ее отдельные модули могут реализовываться с применением дистанционных образовательных технологий (ДОТ). При дистанционном обучении режим занятий согласуется с заказчиком обучения (со слушателями). В процессе обучения в зависимости от подготовленности слушателей возможно изменение последовательности изложения тем, но при этом качество освоения учебного материала не должно быть снижено и количество учебных часов должно быть не менее 367 часов. Каждый обучающийся с использованием дистанционных технологий получает доступ в личный кабинет, где он может пользоваться всеми учебными материалами.

Программой предусмотрено проведение:

1) Теоретических занятий;
2) Практических занятий;
3) Промежуточного тестирования;
4) Экзамена;
5) Написание итоговой квалификационной работы

При организации процесса обучения в рамках данной программы предполагается применение информационной технологии обучения.

5. Формы аттестации и оценочные материалы.

Итоговая аттестация обучающихся (за исключением обучающихся из числа государственных гражданских служащих), освоивших программу профессиональной переподготовки, проводится в форме, определяемой организацией, осуществляющей образовательную деятельность, самостоятельно.

Освоение государственными гражданскими служащими программы профессиональной переподготовки завершается итоговой аттестацией в форме экзамена и защиты выпускной квалификационной (аттестационной) работы.

Перечень вопросов, используемых для проведения экзамена, сформирован на основе основных вопросов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным дисциплинам, представленных в рабочих программах учебных дисциплин.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается руководителем организации, осуществляющей образовательную деятельность.

В целях обеспечения объективного определения практической и теоретической подготовленности обучающихся к выполнению профессиональных задач по результатам обучения в состав аттестационной комиссии рекомендуется включать по согласованию представителей ФСТЭК России (управлений ФСТЭК России по федеральным округам).

Промежуточная аттестация проводится в соответствии с уставом ОУ в форме тестирования. Итоговая аттестация проходит в форме защиты квалификационной работы.

После окончания обучения слушателям выдается диплом о профессиональной переподготовки, установленного образца.

6. УЧЕБНЫЙ ПЛАН

по программе профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

Категория обучающихся: специалисты, работающие в области ТЗКИ.

Форма обучения: очная с отрывом от работы или дистанционная (без отрыва от работы).

Продолжительность обучения: 70 дней 560 академических часов.

Режим занятий : не более 5 часов в день с преподавателем и 3 часа самостоятельной работы в день (форма обучения очно-заочная) и 6 часов самостоятельно и 2 часа консультации с преподавателем по скайпу (дистанционная форма обучения).

№ темы	Тема	Всего часов	Теоретические занятия, количество часов	Практические занятия, количество часов	Самостоятельная нагрузка студента
1	**Введение**	1	1	**-**	**-**
1	**Организационно-правовые основы ТЗКИ**	**106**	**70**	**-**	**36**
1.1	Объект информатизации. Классификация объектов защиты	30	20	-	10
1.2	Государственные органы в области защиты информации	12	8	-	4
1.3	Порядок сертификации средств защиты информации	12	8	-	4
1.4	Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP	32	20	-	12
1.5	Требования и рекомендации по защите информации	20	14	-	6
Проверка знаний (зачет)+1 ч					
2	**Аппаратные средства вычислительной техники**	**100**	**56**	**20**	**24**
2.1	Основы ЭВМ	20	12	-	8
2.2	Микропроцессор. Тип и структура	14	2	8	4
№ темы	Тема	Всего часов	Теоретические занятия,	Практические занятия,	Самостоятельная нагрузка студента

			количество часов	количество часов	
2.3	Программное обеспечение. Основные понятия и классификация	22	16	-	6
2.4	Операционные системы	28	24	-	4
2.5	Глобальная компьютерная сеть Интернет	16	2	12	2
Проверка знаний (зачет) +1 ч					
3	**Системы и сети передачи информации**	**80**	**42**	**14**	**24**
3.1	Классификация и состав современных сетей электросвязи	20	12	-	8
3.2	Радиоволны	18	8	6	4
3.3	Технология Ethernet и ее развитие	20	14	-	6
3.4	Компоненты и функции телекоммуникационной системы	14	2	8	4
3.5	Волоконно-оптические системы передачи	8	6	-	2
Проверка знаний (зачет) +1 ч					
4	**Способы и средства ТЗКИ от утечки по техническим каналам**	**100**	**60**	**-**	**40**
4.1	Характеристика технических каналов утечки информации	20	10	-	10
4.2	Закладные устройства и защита информации от них	40	20	-	20
4.3	Средства обнаружения каналов утечки информации	40	30	-	10
Проверка знаний (зачет) +1 ч					
5	**Меры и средства ТЗКИ от несанкционированного доступа**	**31**	**13**	**8**	**10**
Проверка знаний (зачет) +1 ч					
6	**Техническая защита конфиденциальной информации от специальных воздействий**	**27**	**8**	**9**	**10**
Проверка знаний (зачет) +1 ч					
7	**Организация защиты конфиденциальной информации на объектах информатизации**	**31**	**17**	**6**	**8**
№ темы	Тема	Всего часов	Теоретические занятия, количество часов	Практические занятия, количество часов	Самостоятельная нагрузка студента

7.1	Планирование мероприятий по защите конфиденциальной информации	15	7	3	5
7.2	Реализация требований по защите персональных данных	16	10	3	3
Проверка знаний (зачет) +1 ч					
8	**Аттестация объектов информатизации по требованиям безопасности информации**	**34**	**13**	**11**	**10**
Проверка знаний (зачет) +1 ч					
9	**Контроль состояния ТЗКИ**	**32**	**19**	**4**	**9**
9.1	Основы организации контроля состояния ТЗКИ	9	6	-	3
9.2	Методика контроля защищенности автоматизированной системы обработки конфиденциальной информации	10	5	2	3
9.3	Общий порядок сертификации средств защиты информации	13	8	2	3
Проверка знаний (зачет) +1 ч					
Квалификационный экзамен и квалификационная работа +9 ч					
	Итого	**560**	**298**	**72**	**190**

7. Примерный календарный учебный график

Срок обучения - 12 недель, 3 месяца.

Срок обучения по программе профессиональной переподготовки, месяцы	1				2				3			
Срок обучения по программе профессиональной переподготовки, недели	1	2	3	4	5	6	7	8	9	10	11	12
Виды занятий, предусмотренные программой профессиональной переподготовки	А	А	А	А	А	А	А	А	А	А	А	И

А- аудиторная и самостоятельная работа;

И- итоговая аттестация

8. Структура и краткое содержание учебного курса

Введение

Понятие информации, защиты информации, их параметры, характеристики и свойства. Рассмотрение технической защиты информации, ее объекты и принципы.

1 Организационно-правовые основы ТЗКИ.

1.1 Объект информатизации. Классификация объектов защиты.

Изучение таких понятий как - объект информации, объект защиты информации, персональные данные. Также рассматривается классификация автоматизированных систем и классы защищённости совокупности программных и технических элементов систем обработки данных.

1.2 Государственные органы в области защиты информации.

В данной теме дана характеристика государственных органов в области информационной безопасности, таких как:

Комитет Государственной думы по безопасности,

Совет безопасности России,

Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности Российской Федерации (ФСБ России),

Служба внешней разведки Российской Федерации (СВР России),

Министерство обороны Российской Федерации (Минобороны России),

Министерство внутренних дел Российской Федерации (МВД России),

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

1.3 Порядок сертификации средств защиты информации.

В данной теме рассматривается сертификация средств защиты информации, ее участники, процедура осуществления, а также органы системы сертификации.

1.4 Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP.

Изучается такое понятие, как «несанкционированный доступ (НСД) к информации». Рассматриваются основные угрозы НСД и основные классы атак в сетях.

1.5 Требования и рекомендации по защите информации.

В данной теме обучающийся рассматривает основные аспекты документа "Специальные требования и рекомендации по технической защите конфиденциальной информации". В том числе: основные требования и рекомендации по защите служебной тайны и персональных данных; основные рекомендации по защите информации, составляющей коммерческую тайну.

2 Аппаратные средства вычислительной техники.

2.1 Основы ЭВМ.

В этой теме дается характеристика таких понятий, как электронно-вычислительная машина, компьютер и система счисления, а также методы хранения программ и данных на цифровых носителях.

2.2 Микропроцессор. Тип и структура.

Рассмотрение понятия «микропроцессор», его задач, свойств и функций.

2.3 Программное обеспечение. Основные понятия и классификация.

Дается определение основного компонента ПО, характеристики пользователей, задач, приложений и системного программного обеспечения. Описывается процесс создания программ и инструментарий технологии программирования.

2.4 Операционные системы.

В этой теме рассматриваются характеристики операционных систем, способы написания алгоритмов, уровни современных компьютеров, а также основные действия выполнения программ.

2.5 Глобальная компьютерная сеть Интернет.

Определение понятия интернет, рассмотрение различных вариантов подключения к глобальной компьютерной сети, адресации в интернете, системы счисления и маршрутизации данных.

3 Системы и сети передачи информации.

3.1 Классификация и состав современных сетей электросвязи

Характеристика сетей электросвязи, элементов сетей и их свойств, а также классификационных признаков сетей связи.

3.2 Радиоволны.

Рассмотрение колебательных явлений, периода, частоты, амплитуды колебаний. Понятие радиоволн и радиопередачи.

3.3 Технология Ethernet и ее развитие

История становления технологии Ethernet и форматов Ethernet-кадров.

3.4 Компоненты и функции телекоммуникационной системы.

Дается понятие телекоммуникационной системы, ее основных компонентов, функций, а также типов сигналов и каналов связию.

3.5 Волоконно-оптические системы передачи.

Рассматривается основное направление развития телекоммуникационных систем – ВОСП, его состав и преимущества.

4. Способы и средства ТЗКИ от утечки по техническим каналам.

4.1 Характеристика технических каналов утечки информации.

В данной теме изучаются каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. А также характеристика технических каналов утечки информации - электромагнитные, электрические, параметрические и вибрационные.

4.2 Закладные устройства и защита информации от них

Рассмотрение конструктивных особенностей, характеристик и схемных решений построения закладных устройств, а также мероприятий по недопущению установки закладных устройств.

4.3 Средства обнаружения каналов утечки информации.

Раскрываются такие понятия как, радиочастотомеры, радиоусилители, радиозакладки, детектор и индикатор излучения. Также приводятся иллюстрации внешнего вида радиочастотомеров, индикаторов электромагнитного излучения и переносимых сканирующих приемников.

5. Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа.

Дается понятие компьютерного преступника, рассматриваются признаки компьютерных преступлений, цели информационной безопасности, а также меры защиты информационной безопасности.

6. Техническая защита конфиденциальной информации от специальных воздействий.

Рассматриваются такие понятия как, техническая защита конфиденциальной информации от специальных воздействий, преднамеренное силовое электромагнитное воздействие на информацию, защита информации от [иностранной] разведки. А также направления защиты конфиденциальной информации.

7. Организация защиты конфиденциальной информации на объектах информатизации.

7.1 Планирование мероприятий по защите конфиденциальной информации.

В данной теме определяются основные цели планирования мероприятий по защите информации, и рассматривается структура и основное содержание плана мероприятий по защите конфиденциальной информации.

7.2 Реализация требований по защите персональных данных

Учащийся рассматривает последствия невыполнения требований законодательства, изучает понятие «информационные системы персональных данных» и их требования в законодательстве.

8. Аттестация объектов информатизации по требованиям безопасности информации.

Рассматривается аттестация объектов информатизации, требования к аттестации и перечни ее работ, а также структура системы аттестации.

9. Контроль состояния ТЗКИ.

9.1 Основы организации контроля состояния ТЗКИ.

Дается понятие контроля, основных объектов, форм и методов контроля состояния ТЗКИ, а также суть проверки, алгоритм ее подготовки и проведения.

9.2 Методика контроля защищенности автоматизированной системы обработки конфиденциальной информации.

В данной теме рассматриваются принципы защиты от НСД, внутренние и внешние факторы угроз НСД.

9.3 Общий порядок сертификации средств защиты информации.

Дается определение таких понятий, как сертификация, сертификат соответствия, участники сертификации. Также изучаются органы системы сертификации – центральные и федеральные.

9. РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «Организационно-правовые основы технической защиты конфиденциальной информации»

Цель учебной дисциплины - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности **«Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»** и приобретения новой квалификации. Получение дополнительных знаний, умений и навыков по вопросам организационно-правовых основ технической защиты конфиденциальной информации.

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: «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий»,. «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации» и «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

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

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

б) профессиональных:

в организационно-управленческой деятельности:

способность планировать деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

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.

В результате освоения дисциплины обучающийся 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.

Обучающийся должен знать:

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

основы построения информационных систем и формирования информационных ресурсов;

виды конфиденциальной информации;

перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации;

цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации;

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

физические основы возникновения, классификацию и характеристики ТКУИ;

угрозы безопасности информации;

общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

уметь:

работать с действующей нормативной правовой и методической базой в области защиты информации;

разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в области ТЗКИ;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

организации деятельности подразделений и специалистов в области ТЗКИ в органах государственной власти и организациях;

разработки необходимой документации по вопросам организации ТЗКИ в органах государственной власти и организациях.

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 106 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**70**
лекции (Л)	30
практические занятия (ПЗ)	-
семинары (С)	40
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего), в том числе:	**36**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	34
Вид промежуточной аттестации (зачет)	2
Итого:	**106**

Содержание разделов учебной дисциплины.

1.1 Объект информатизации. Классификация объектов защиты

Изучение таких понятий как - объект информации, объект защиты информации, персональные данные. Также рассматривается классификация автоматизированных систем и классы защищённости совокупности программных и технических элементов систем обработки данных.

1.2 Государственные органы в области защиты информации

В данной теме дана характеристика государственных органов в области информационной безопасности, таких как:

Комитет Государственной думы по безопасности,

Совет безопасности России,

Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности Российской Федерации (ФСБ России),

Служба внешней разведки Российской Федерации (СВР России),

Министерство обороны Российской Федерации (Минобороны России),

Министерство внутренних дел Российской Федерации (МВД России),

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

1.3 Порядок сертификации средств защиты информации

В данной теме рассматривается сертификация средств защиты информации, ее участники, процедура осуществления, а также органы системы сертификации.

1.4 Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP

Изучается такое понятие, как «несанкционированный доступ (НСД) к информации». Рассматриваются основные угрозы НСД и основные классы атак в сетях.

1.5 Требования и рекомендации по защите информации

В данной теме обучающийся рассматривает основные аспекты документа "Специальные требования и рекомендации по технической защите конфиденциальной информации". В том числе: основные требования и рекомендации по защите служебной тайны и персональных данных; основные рекомендации по защите информации, составляющей коммерческую тайну

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	2
1.	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	+	+
2.	Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа	+	+
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 технической защиты конфиденциальной информации	+	+

Лабораторный практикум.

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

Практические занятия (семинары)

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1		Информация как объект защиты. Цели и задачи ТЗКИ.	4
2.	2		Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации.	4
3.	2		Нормативные правовые акты и методические документы ФСТЭК России в области защиты информации.	4
4.	3		Система международных и национальных стандартов в области защиты информации	4
5.	3		Организационно-правовые основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации	4
6.	3		Система сертификации средств защиты информации	8
7.	4		Требования по защите речевой конфиденциальной информации.	4
8.	4		Требования по защите конфиденциальной информации, обрабатываемой в автоматизированных системах (от утечки по техническим каналам и от НСД и специальных воздействий).	4
9	5		Требования по защите персональных данных	4

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) данной дисциплиной не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) 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. - 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. - 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.: Издательский центр «Академия», 2008. -256 с.

4. Семкин С.Н., Семкин А.Н. Основы правового обеспечения защиты информации: Учебное пособие для вузов. - М.: «Горячая линия - Телеком», 2008;

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

б) дополнительная литература:

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

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 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

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

9. 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».

10. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. №171.

11. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

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

13. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

14. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

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

16. 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.

17. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

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

19. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

20. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

21. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

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

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

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 антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.

25. 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.

26. 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.

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

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

29. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.

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

31. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992.

32. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

33. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода.

34. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

35. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

36. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1997.

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

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

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

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

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

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

43. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.

44. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013.

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

46. ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.

47. 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.

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

49. 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.

50. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/1EC 15408-2:2008). Росстандарт, 2013.

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

52. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2012.

53. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.

54. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.

55. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.

56. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.

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

58. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

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

60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

61. 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.

62. 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.

Программное обеспечение для изучения данной дисциплины: не требуется.

Необходимые базы данных, информационно-справочные и поисковые системы: правовые справочно-поисковые системы («Гарант», «Консультант Плюс»), www.fstec.ru;www.gost.ru/wps/portal/tk362.

Материально-техническое обеспечение учебной дисциплины.

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

мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

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 защиты информации, 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 обучающихся.

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 обучающиеся 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 защиты информации; работать с правовыми базами данных, базами данных, а также формируются навыки реализации в органах государственной власти и организациях требований нормативных и методических документов, а также действующего законодательства по вопросам защиты конфиденциальной информации.

Для обучающихся дистанционной формой обучения предусмотрены видеотрансляции занятий и консультации с преподавателями по скайпу.

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70% учебного времени.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

Вопросы для подготовки к зачету.

1. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации.
2. Цели и задачи ТЗКИ.
3. Объекты информатизации: классификация и характеристика.
4. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

5. Классификация угроз утечки информации по техническим каналам.

6. Классификация угроз безопасности информации, связанных с НСД.

7. Правовые, нормативные и методические документы, национальные стандарты и международные стандарты в области защиты информации.

8. Организационно-правовые основы лицензирования деятельности в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации по требованиям безопасности информации.

9. Требования по защите конфиденциальной речевой информации.

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

11. Требования по защите персональных данных.

10. РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «Аппаратные средства вычислительной техники»

Цель учебной дисциплины - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам аппаратных средств вычислительной техники».

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: «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации» и «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

Процесс освоения учебной дисциплины направлен на получение (формирование) обучающимися таких компетенций, как: Процесс освоения учебной дисциплины направлен на получение (формирование) обучающимися 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 организационно-управленческой деятельности:

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

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 обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

В результате освоения дисциплины обучающийся 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.

Обучающийся должен знать:

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

принципы построения и функционирования, примеры реализации современных 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;

уметь:

определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации;

владеть навыками:

работы с современными операционными системами;

установки и настройки современных операционных систем с учетом требований по безопасности информации;

разработки, документирования баз данных, компьютерных сетей с учетом требований по безопасности информации;

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 100 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**76**
лекции (Л)	36
практические занятия (ПЗ)	24
семинары (С)	8
лабораторные работы (ЛР)	8
Самостоятельная работа (СР, всего), в том числе:	**24**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	22
Вид промежуточной аттестации (зачет)	2
Итого:	**100**

Содержание разделов учебной дисциплины.

1. Основы ЭВМ

В этой теме дается характеристика таких понятий, как электронно-вычислительная машина, компьютер и система счисления, а также методы хранения программ и данных на цифровых носителях.

1.1 Сущность программного управления компьютером. Структурная схема микропроцессорной системы. Функциональная схема арифметико-логического устройства. Укрупненная функциональная схема устройства управления. Микропроцессорная память. Интерфейсная часть микропроцессора. Загрузка компьютера(инициализация).

1.2 Классификация и назначение различных видов программного обеспечения. Системное и прикладное программное обеспечение. Операционные системы: Windows, Unix, Linux. Разновидности драйверов, программ-оболочек, утилит. Основные виды и назначение прикладного программного обеспечения. Инструментарий технологии программирования. Средства разработки программного обеспечения. Сетевое программное обеспечение.

1.3 Понятия кодирования и декодирования информации. Системы счисления: позиционные и непозиционные; двоичные, десятичные, шестнадцатеричные. Форматы числовых данных. Представление символьной информации.

1.4 Международные системы байтового кодирования. Представление графической информации. Растровые и векторные методы представления цветного изображения.

1.5 Типы компьютерных устройств хранения информации и их носители. Физический и логический уровни организации хранения данных. Взаимосвязь физического и логического уровней организации хранения данных. Файловые системы: FAT, NTFS и др. Физическая сущность форматирования носителей информации, создания и удаления файлов, папок (каталогов). Организация хранения данных на компакт-дисках, Flash- памяти

2. Микропроцессор. Тип и структура

Рассмотрение понятия «микропроцессор», его задач, свойств и функций.

3. Программное обеспечение. Основные понятия и классификация.

Дается определение основного компонента ПО, характеристики пользователей, задач, приложений и системного программного обеспечения. Описывается процесс создания программ и инструментарий технологии программирования.

4. Операционные системы.

В этой теме рассматриваются характеристики операционных систем, способы написания алгоритмов, уровни современных компьютеров, а также основные действия выполнения программ.

Использование компьютеров в системе обработки информации. Автоматизированные рабочие места и рабочие станции, серверы и специализированные компьютеры. Универсальные и специальные вычислительные комплексы высокой производительности. Архитектура специализированных вычислительных комплексов, их возможности и перспективы развития.

5. Глобальная компьютерная сеть Интернет

Определение понятия интернет, рассмотрение различных вариантов подключения к глобальной компьютерной сети, адресации в интернете, системы счисления и маршрутизации данных.

Локальные и глобальные компьютерные сети. Способы объединения компьютеров в сетевых технологиях. Понятие топологии компьютерной сети. Принципы передачи данных в компьютерных сетях. Модель взаимодействия открытых систем (OS1). Программное обеспечение, поддерживающее работу сети. Технические устройства, выполняющие функции сопряжения ЭВМ с каналами связи: сетевая плата (сетевой адаптер), мультиплексор передачи данных, концентратор, повторитель, модем. Оборудование, предназначенное для объединения локальных

вычислительных сетей: мост, маршрутизатор (роутер), шлюз. Технология управления взаимодействием в сети: клиент-сервер.

Обобщенная структура и функции глобальных компьютерных сетей. Подключение к сети Internet. Основные услуги и сервисы сети Internet. Распространенные приемы поиска и получения информации, обмена сообщениями по электронной почте. Технология IntraNet.

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	2
1.	Системы и сети передачи информации		+
2.	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	+	
3.	Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа	+	+
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 технической защиты конфиденциальной информации	+	+

Лабораторный практикум.

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Кол-во часов
1.	1	Представление информации и основы работы компьютера	4
2.	2	Исследование технических устройств, выполняющих функции сопряжения ЭВМ с каналами связи: сетевая плата (сетевой адаптер), мультиплексор передачи данных, концентратор, повторитель, модем	4

Практические занятия (семинары).

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1	—	Принцип программного управления компьютером	4
2.	1	Представление данных в ЭВМ	-	4
3.	1	Системное и прикладное программное обеспечение	-	4
4.	1	Способы представления информации в компьютере и методы их реализации		4
6.	1	Типы компьютерных Устройств хранения информации и их носители		4
7.	2		Использование компьютеров в системе обработки информации	4
8.	2	Модель взаимодействия открытых систем (OSI)	—	4

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) данной дисциплиной не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) основная литература:

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

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

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

б) дополнительная литература:

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

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

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

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

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

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

Материально-техническое обеспечение учебной дисциплины.

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

мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

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 защиты информации, 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 обучающихся.

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 обучающиеся 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 защиты информации; работать с правовыми базами данных, базами данных, а также формируются навыки реализации в органах государственной власти и организациях требований нормативных и методических документов, а также действующего законодательства по вопросам защиты конфиденциальной информации.

Для обучающихся дистанционной формой обучения предусмотрены видио трансляции занятий и консультации с преподавателями по скайпу.

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70%.

Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся.

Вопросы к зачету:

1. Сущность программного управления компьютером.
2. Классификация и назначение различных видов программного обеспечения.
3. Основные виды и назначение прикладного программного обеспечения.
4. Понятия кодирования и декодирования информации.
5. Системы счисления: позиционные и непозиционные; двоичные, десятичные, шестнадцатеричные.
6. Международные системы байтового кодирования.
7. Растровые и векторные методы представления цветного изображения.
8. Типы компьютерных устройств хранения информации и их носители.
9. Физическая сущность форматирования носителей информации, создания и удаления файлов, папок (каталогов).
10. Автоматизированные рабочие места и рабочие станции, серверы и специализированные компьютеры.
11. Архитектура специализированных вычислительных комплексов. Их возможности и перспективы развития.
12. Способы объединения компьютеров в сетевых технологиях.
13. Технические устройства, выполняющие функции сопряжения ЭВМ с каналами связи: сетевая плата (сетевой адаптер), мультиплексор передачи данных, концентратор, повторитель, модем.
14. Оборудование, предназначенное для объединения локальных вычислительных сетей: мост, маршрутизатор (роутер), шлюз.
15. Обобщенная структура и функции глобальных компьютерных сетей.
16. Распространенные приемы поиска и получения информации, обмена сообщениями по электронной почте.
17. Технология IntraNet.

11.Рабочая программа учебной дисциплины «Системы и сети передачи информации»

Цель учебной дисциплины: - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков, связанных с применением систем и сетей передачи информации.

Место учебной дисциплины в структуре программы профессиональной переподготовки.

Учебная дисциплина входит в программу профессиональной переподготовки, при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебной дисциплины: «Аппаратные средства вычислительной техники».

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

Требования к результатам освоения учебной дисциплины.

Процесс освоения учебной дисциплины направлен на получение (формирование) обучающимися 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 организационно-управленческой деятельности:

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

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 обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

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

программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей;

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

уметь:

работать с действующей нормативной правовой и методической базой в области защиты информации;

определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации;

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

владеть навыками:

установки и настройки современных средств защиты информации, системного и прикладного программного обеспечения с учетом требований по безопасности информации;

работы в компьютерных сетях с учетом требований по безопасности информации.

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 80 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**56**
лекции (Л)	24
практические занятия (ПЗ)	16
семинары (С)	8
лабораторные работы (ЛР)	8
Самостоятельная работа (СР, всего), в том числе:	**24**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	22
Вид промежуточной аттестации (зачет)	2
Итого:	**80**

Содержание разделов учебной дисциплины.

1. **Классификация и состав современных сетей электросвязи.**

Характеристика сетей электросвязи, элементов сетей и их свойств, а также классификационных признаков сетей связи. Сети и средства связи. Основные понятия и определения. Сетей электросвязи. Классификация сетей электросвязи. Архитектура сетей связи: структурные элементы сети, режим коммутации каналов, принципы построения телефонной сети общего пользования. Сигналы и их характеристики. Методы преобразования сигналов. Методы модуляции и манипуляции сигналов. Импульсно-кодовая модуляция сигналов. Цифровые сигналы. Дискретизация аналогового сигнала. Квантование сигнала. Кодирование сигнала. Методы кодирования сигналов.

2. **Радиоволны**

Рассмотрение колебательных явлений, периода, частоты, амплитуды колебаний. Понятие радиоволн и радиопередачи. Основы распространения радиоволн. Антенно-фидерные устройства. Радиопередающие и радиоприемные устройства. Основные характеристики, функциональные схемы и работа радиопередающих и радиоприемных устройств. Каналы и

тракты звукового вещания. Системы цифрового вещания. Системы проводного вещания. Радиорелейные линии и спутниковые системы связи. Принципы построения и функционирования радиорелейных линий и спутниковых систем связи.

3. Технология Ethernet и ее развитие.

История становления технологии Ethernet и форматов Ethernet-кадров. Технология Ethernet: протоколы локальных сетей, форматы кадров, методы доступа и разделения среды, высокоскоростной Ethernet. Организация и сервис виртуальных частных сетей (VPN).Структура сети GSM. Подсистема базовой станции, регистры HLR и VLR, центр коммутации подвижной связи, центр аутентификации и регистр идентификации оборудования. Сети стандартов 3G, 4G, LTE.

Архитектура сетей подвижной связи. Основные сетевые компоненты. 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.

4. Компоненты и функции телекоммуникационной системы.

Услуги телефонной сети общего пользования. Дается понятие телекоммуникационной системы, ее основных компонентов, функций, а также типов сигналов и каналов связи. Протокол SIP. Мультисервисная сеть связи. Состав оборудования. Цифровые сети интегрального обслуживания (сети SDN). Широкополосные цифровые сети интегрального обслуживания. Обеспечение защиты средств связи от НСД. Тенденции развития сетей электросвязи классификация телекоммуникационных систем. Телекоммуникационные системы. Понятие о цифровых системах передачи информации. Формирование группового сигнала. Синхронизация и регенерация (восстановление) цифровых сигналов. Цифровые иерархии.

Синхронная цифровая иерархия. Асинхронный режим передачи. Сигналы PDH и SDH. Принципы построения, европейский и североамериканский стандарты Hiperlan, WiFi, WiMax. Перспективы развития телекоммуникационных систем в России и за рубежом.

5. Волоконно-оптические системы передачи.

Классификация и архитектура волоконно-оптических систем передачи, способы организации двухсторонней связи, способы уплотнения оптических кабелей. Оптический линейный тракт: передатчики, приемники, источники излучения, модуляторы, усилители оптического излучения. Рассматривается основное направление развития телекоммуникационных систем – ВОСП, его состав и преимущества.

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	2
1.	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	+	+
2.	Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа	+	+
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 технической защиты конфиденциальной информации	+	+

Примечания:
«+»- раздел обеспечивает изучение данной учебной дисциплины; «-» - раздел не обеспечивает изучение данной учебной дисциплины.

Лабораторный практикум.

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Кол-во часов
1.	1	Исследование сигналов и их характеристик	8

Практические занятия (семинары).

№ п/п	Тематика практических занятий (семинаров)		Кол-во часов
	тематика практических занятий	тематика семинаров	
1.		Основные характеристики сигналов электросвязи, спектры и виды модуляции	4
2.	-	Основы распространения радиоволн	4
3.	Телекоммуникационное оборудование	-	4
4.	Адресная схема протокола, маршрутизация, маска подсети, расширенный сетевой префикс		4
5.	Характеристики цифровых систем передачи		4
6	Анализ основных характеристик и возможностей телекоммуникационных систем и сетей связи		4

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) основная литература:

1. Системы и сети передачи информации: учеб, пособие / Л.В. Воробьев, А.В. Давыдов, Л.П. Щербина. - М.: Академия, 2009. - 329 с.

2.Системы и сети передачи информации: учебник / А.А. Чертков. - СПб.: Санкт-Петербургский государственный университет водных коммуникаций, 2012.

3.Компьютерные сети. Протоколы, технологии, принципы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. - 4-е изд. - Спб.: Питер, 2010;

б) дополнительная литература:

1.Сети нового поколения - NGN: учеб, пособие для вузов / В.И. Битнер, Ц.Ц. Михайлова. - М.: Горячая линия - Телеком», 2011.

2.Сетевые операционные системы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. - 2-е изд. - СПб.: Питер, 2009.

3.Телекоммуникационные технологии: введение в технологии GSM: учеб, пособие для вузов / С.Б. Макаров, Н.В. Певцов, Е.А. Попов, М.А. Сиверс. - М.: Издательский дом «Академия», 2008.

4.Основы инфокоммуникационных технологий, учеб, пособие для вузов / В.В. Величко, Г.П. Катунин, В.П. Шувалов; под ред. В.П. Шувалова. - М.: Горячая линия - Телеком, 2009;

5.Федеральный закон № 126-ФЗ от 7 июля 2003 г. «О связи».

6.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»;

программное обеспечение:

1. Системное и прикладное программное обеспечение; операционные системы: Windows 9X/2000/XP/Vista, Adobe Audition 1.5;

2. Базы данных, информационно-справочные и поисковые системы: www.pravo.gov.ru,www.fstec.ru,www.gost.ru/wps/portal/tk362/; правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (с приводом лазерных дисков типа DVD-RW, звуковым сопровождением и т.п.);

Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным персональным компьютером (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

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 основой в изучении сетей связи и систем передачи информации.

Практическая часть учебной дисциплины отрабатывается на практических занятиях и в ходе лабораторных работ. На практических занятиях развиваются умения применять подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений требований по ТЗИ; создавать защищенные каналы между взаимодействующими объектами с использованием выделенных каналов связи.

В ходе проведения 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; разработки,

документирования баз данных, компьютерных сетей с учетом требований по безопасности информации.

Лабораторные работы и практические занятия по демонстрации сетей связи и систем передачи информации, способов их использования в процессе эксплуатации объектов информатизации проводятся в классе, оборудованном под радиополигон. Занятия проводятся на четырех-восьми рабочих местах (количество рабочих мест зависит от количества обучающихся 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 обучающиеся получают консультации у преподавателей.

На изучение теоретических вопросов учебной дисциплины отводится 30 % учебного времени, практических - 70%.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 примерных вопросов, выносимых для контроля знаний обучающихся:

1. Классификация сетей электросвязи.
2. Методы преобразования сигналов.
3. Основы распространения радиоволн.
5. Системы цифрового и проводного вещания.

6. Системы телевизионного вещания.

7. Принципы построения и функционирования радиорелейных линий и спутниковых систем связи.

8. Понятие о цифровых системах передачи информации.

9. Архитектура сетей связи: структурные элементы сети, режим коммутации каналов, принципы построения телефонной сети общего пользования.

10. Архитектура сетей передачи данных: структурные элементы сети, режим коммутации пакетов, принципы маршрутизации.

11. Стандарты Hiperlan, WiFi, WiMax.

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

Цель учебной дисциплины: - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам технической защиты конфиденциальной информации от утечки по техническим каналам.

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: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации». Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются для изучения последующих учебных дисциплин программы профессиональной переподготовки: «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации» и «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

в проектной деятельности:

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

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 обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен: знать:

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

физические основы возникновения, классификацию и характеристики ТКУИ;

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

общие требования по ТЗКИ (по защите информации от ее утечки по техническим каналам), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (по защите информации от утечки по техническим каналам);

требования к средствам ТЗКИ;

средства ТЗИ, возможности и порядок применения, перспективы развития;

уметь:

определять возможные ТКУИ;

работать с действующей нормативной правовой и методической базой в области защиты информации;

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ;

применять штатные средства ТЗКИ и контроля защищенности информации;

проводить организационные и технические мероприятия по ТЗКИ;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты;

определения задач, способов и средств ТЗКИ и контроля защищенности информации;

использования программных и аппаратных средств ТЗКИ.

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 100 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**60**
лекции (Л)	16
практические занятия (ПЗ)	-
семинары (С)	24
лабораторные работы (ЛР)	20
Самостоятельная работа (СР, всего), в том числе:	**40**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	38
Вид промежуточной аттестации (зачет)	2
Итого:	**100**

Содержание учебной дисциплины.

1. Характеристика технических каналов утечки информации.

В данной теме изучаются каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. А также характеристика технических каналов утечки информации - электромагнитные, электрические, параметрические и вибрационные. Термины и определения в области защиты информации 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. Классификация ТКУИ, обрабатываемой техническими средствами. Физические основы возникновения ТКУИ. Общая характеристика классификация ТКУИ, Характеристики случайных антенн. Причины возникновения наводок информативных сигналов в случайных антеннах. Зона 1. Схема ТКУИ, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах.

Причины просачивания в линии электропитания и цепях заземления СВТ. Схемы ТКУИ, возникающих за счет просачивания информативных сигналов в линии электропитания и цепи заземления СВТ. Специально создаваемые ТКУИ, обрабатываемой СВТ. Классификация электронных устройств перехвата информации, внедряемых в СВТ.

Технические каналы утечки речевой конфиденциальной информации. Акустические сигналы. Спектр и типовые уровни речевого сигнала. Классификация технических каналов утечки речевой конфиденциальной информации. Прямые акустические каналы утечки речевой информации.

2. Закладные устройства и защита информации от них.

Рассмотрение конструктивных особенностей, характеристик и схемных решений построения закладных устройств, а также мероприятий по недопущению установки закладных устройств. Специальные технические средства подавления электронных устройств перехвата речевой конфиденциальной информации, порядок их установки и настройки. Общий порядок разработки и производства средств защиты речевой конфиденциальной информации

3. Средства обнаружения каналов утечки информации.

Раскрываются такие понятия как, радиочастотомеры, радиоусилители, радиозакладки, детектор и индикатор излучения. Также приводятся иллюстрации внешнего вида радиочастотомеров, индикаторов электромагнитного излучения и переносимых сканирующих приемников.

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	2	3
1.	Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа	+	+	+
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 технической защиты конфиденциальной информации	+	+	+

Лабораторный практикум

№ п/п	Наименование лабораторной работы	Кол-во часов
1.	Исследование ПЭМИН СВТ	4
2.	Исследование акустических и вибрационных каналов утечки информации.	4
3.	Исследование акустоэлектрических каналов утечки информации	4
4.	Исследование характеристик системы вибрационной защиты. Установка и настройка системы вибрационной защиты	4
5.	Исследование характеристик средств защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам	4

Практические занятия (семинары).

№ п/п	Тематика практических занятий (семинаров)		Кол-во часов
	тематика практических занятий	тематика семинаров	
1.		Технические каналы утечки информации, обрабатываемой СВТ	4
		Технические каналы утечки речевой конфиденциальной информации	8
		Способы и средства защиты информации от утечки по техническим каналам	8
		Способы и средства защиты защищаемых помещений от утечки речевой информации по техническим каналам	4

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) основная литература:

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

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.

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

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

б) дополнительная литература:

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

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

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

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

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.

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

7. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

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

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

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

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

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

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

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. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

16. 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.

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

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru;www.gost.ru/wps/portal/tk362.

Материально-техническое обеспечение учебной дисциплины.

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

мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

Лаборатория оснащена анализаторами спектра с демодуляторами и с интерфейсом анализатора спектра с компьютером (GPIB, USB), набором антенн электрических и магнитных антенн, эквивалентом сети, генераторами пространственного и линейного зашумления, а также специализированным программным обеспечением для проведения специальных исследований СВТ, комплектом аппаратуры для проведения акустических и вибрационных измерений, комплектом средств ТЗИ для демонстрации способов защиты информации от утечки по техническим каналам.

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 обучающихся.

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 обучающиеся получают консультации у преподавателей.

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70% учебного времени.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

1. Способы перехвата речевой информации из защищаемых помещений по прямому акустическому каналу.
2. Способы перехвата речевой информации из защищаемых помещений по акустовибрационным каналам.
3. Способы перехвата речевой информации из защищаемых помещений по акустооптическому каналу.
4. Способы перехвата речевой информации из защищаемых помещений по акустоэлектрическим каналам.
5. Классификация способов и средств защиты конфиденциальной информации от утечки по техническим каналам.
6. Пассивные способы и средства защиты конфиденциальной информации от утечки по техническим каналам.

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

8. Основные характеристики систем линейного электромагнитного зашумления.

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

10. Классификация способов и средств защиты речевой конфиденциальной информации по техническим каналам.

11. Пассивные способы защиты речевой конфиденциальной информации от утечки по техническим каналам.

12. Активные способы защиты речевой конфиденциальной информации от утечки по техническим каналам.

13. Системы и средства виброакустической маскировки.

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

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

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

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

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

Цель учебной дисциплины: - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам защиты конфиденциальной информации от НСД.

Место учебной дисциплины в структуре программы профессиональной переподготовки

Учебная дисциплина входит в программу профессиональной переподготовки при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам». 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» и «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ от НСД (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации от НСД в организации;

в проектной деятельности:

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

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

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

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ от НСД в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ от НСД при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

угрозы безопасности информации;

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

организацию и содержание проведения работ по ТЗКИ состав и содержание необходимых документов (по защите информации от НСД);

общие требования по ТЗКИ (по защите информации от НСД), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации;

требования к средствам ТЗКИ от НСД;

средства ТЗКИ от НСД, возможности и порядок применения;

программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей;

подсистемы разграничения доступа, подсистемы обнаружения атак, несанкционированных, непреднамеренных и преднамеренных воздействий, контроля целостности информации;

уметь:

определять угрозы безопасности информации в результате НСД; работать с действующей нормативной правовой и методической базой в области защиты информации;

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ;

применять штатные средства ТЗКИ от НСД и контроля защищенности информации от НСД;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

определения угроз безопасности информации, связанных с НСД, применительно к конкретным объектам;

проведения организационных и технических мероприятий по ТЗКИ от НСД;

определения задач, способов и средств ТЗКИ от НСД; использования программных и аппаратных средств ТЗКИ от НСД.

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 31 час.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**22**
лекции (Л)	4
практические занятия (ПЗ)	6
семинары (С)	6
лабораторные работы (ЛР)	6
Самостоятельная работа (СР, всего), в том числе:	**9**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	7
Вид промежуточной аттестации (зачет)	2
Итого:	**31**

Содержание учебной дисциплины.

Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа. Дается понятие компьютерного преступника, рассматриваются признаки компьютерных преступлений, цели информационной безопасности, а также меры защиты информационной безопасности. Понятие и общая классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации.

Уязвимости информационных систем, используемые для реализации угроз безопасности информации. Модель вероятного нарушителя в заданных условиях функционирования объекта защиты. Характеристика типовых сетевых атак в информационных системах. Угрозы применения вредоносных программ. Методы анализа угроз безопасности информации 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 защиты информации от НСД. Системы обнаружения вторжений, требования к ним и технологии применения. Средства антивирусной защиты, требования к ним и технологии применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации.

Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения. Межсетевые экраны, требования к ним и технологии применения. Установка и настройка программных и программно¬аппаратных средств защиты информации от НСД. Общий порядок разработки и производства 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.

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	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 технической защиты конфиденциальной информации	+	+

Примечания: «+»- раздел обеспечивает изучение данной учебной дисциплины; «-»- раздел не обеспечивает изучение данной учебной дисциплины.

Лабораторный практикум.

№ п/п	Наименование лабораторной работы	Кол-во часов
1.	Установка и настройка антивирусных программ	2
2.	Установка средств сетевой безопасности и их настройка по классу защищенности	2
3.	Контроль сетевой безопасности (системы обнаружения вторжений и Анализа защищенности, сетевые сканеры)	2

Практические занятия (семинары).

№ п/п	Тематика практических занятий (семинаров)		Кол-во часов
	тематика практических занятий	тематика семинаров	
1.	Разработка модели угроз безопасности информации		2
2.		Классификация способов обеспечения информационной безопасности (управление доступом; регистрация и учет; обеспечение целостности; антивирусная защита; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений.	2
3.		Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей технических средств, программного обеспечения и средств защиты информации информационных систем	2
4.		Защита информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации	2
5.	Установка, настройка и эксплуатация систем (средств)защиты информации от НСД		2
6.	Порядок проведения работ, выполняемых при осуществлении контроля защищенности информации от НСД		2

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) основная литература.

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

2. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2012. - 352 с.

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

б) дополнительная литература:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2012. - 416 с.

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

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. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

6. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.

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

8. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992.

9. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия

недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

10. 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 недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

11. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

12. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

13. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1997.

14. 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.

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 доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

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 контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

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

18. Временное положение по организации разработки, изготовлении и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утверждено Гостехкомиссией России, 1992.

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

20. 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.

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

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

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

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

25. ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.

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

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

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

Материально-техническое обеспечение учебной дисциплины.

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

мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

Лаборатория оснащена учебными лабораторными комплексами для обеспечения исследований специального программного обеспечения и аппаратного средства защиты конфиденциальной информации в составе:

средства защиты информации от НСД;

программно-аппаратный комплекс доверенной нагрузки;

антивирусные пакеты;

межсетевые экраны;

средство создания модели разграничения доступа;

программа контроля полномочий доступа к информационным ресурсам;

программа фиксации и контроля исходного состояния программного комплекса;

программа поиска и гарантированного уничтожения на дисках;

системы обнаружения вторжений и анализа защищенности;

сканеры безопасности;

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 защиты информации, 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 обучающихся.

Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к групповым и семинарским занятиям. В ходе самостоятельной работы обучающиеся получают консультации у преподавателей.

Практическая часть учебной дисциплины отрабатывается на практических 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 ТЗКИ.

Практические занятия по демонстрации средств ТЗКИ, 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 четырех-восьми рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе) под руководством преподавателя.

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70% учебного времени.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

1. Понятия и общая классификация угроз безопасности информации, связанных с НСД.
2. Угрозы утечки информации по нетрадиционным информационным каналам.
3. Методы анализа угроз безопасности информации.
4. Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.
5. Обеспечение защиты информации от НСД при выходе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.
6. Требования по защите информации от НСД.

7. Требования к мерам защиты информации от НСД, реализуемым в информационной системе. Меры защиты информации от НСД.

8. Средства защиты информации от НСД.

9. Общий порядок разработки и производства средств защиты информации от НСД.

10. Классификация методов контроля защищенности информации от НСД и их характеристика.

11. Сканеры безопасности и их характеристика.

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

13. Классы защищенности автоматизированных систем в зависимости от степени секретности информации.

14. Способы и комплекс средств защиты информации, обрабатываемой средствами вычислительной техники и автоматизированным системам.

15. Способы контроля целостности программного обеспечения и аппаратных средств.

16. Программные и аппаратные средства защиты информации от программно-математического воздействия.

17. Средства обеспечения целостности составных частей компьютера.

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

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

Цель учебной дисциплины: формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам ТЗКИ от специальных воздействий.

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: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются для изучения последующих учебных дисциплин программы профессиональной переподготовки: «Организация защиты конфиденциальной информации на объектах информатизации», «Аттестация объектов информатизации по требованиям безопасности информации» и «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие з организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ от специальных воздействий в организации;

в проектной деятельности:

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

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

способность организовывать внедрение способов и средств для обеспечения ТЗКИ от специальных воздействий на объектах

информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

способность обеспечивать ТЗКИ от специальных воздействий в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ от специальных воздействий при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

угрозы безопасности информации при специальных воздействиях на нее; организацию и содержание проведения работ по ТЗКИ от специальных воздействий, состав и содержание необходимых документов;

требования к средствам ТЗКИ от специальных воздействий и контроля защищенности информации;

уметь:

работать с действующей нормативной правовой и методической базой в области технической защиты информации от специальных воздействий;

определять возможные угрозы безопасности информации в результате специальных воздействий;

применять средства защиты информации от специальных воздействий;

владеть навыками:

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

определения угроз безопасности информации применительно к конкретным объектам защиты;

проведения организационных и технических, мероприятий по ТЗКИ от специальных воздействий, контролю защищенности информации, оценки состояния ТЗКИ от специальных воздействий.

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 27 часов.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**20**
лекции (Л)	4
практические занятия (ПЗ)	12
семинары (С)	4
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего), в том числе:	**5**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	3
Вид промежуточной аттестации (зачет)	2
Итого:	**27**

Содержание учебной дисциплины.

Рассматриваются такие понятия как, техническая защита конфиденциальной информации от специальных воздействий, преднамеренное силовое электромагнитное воздействие на информацию, защита информации от [иностранной] разведки. А также направления защиты конфиденциальной информации.

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. Угрозы безопасности информации от специальных электромагнитных воздействий. Модели угроз. Механизм влияния электромагнитных и электрических воздействий на технические средства обработки информации
2.	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. Меры и средства защиты конфиденциальной информации от специальных электромагнитных и электрических воздействий

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	2
1.	Организация защиты конфиденциальной информации на объектах информатизации	+	+
2.	Аттестация объектов информатизации по требованиям безопасности информации	+	+
3.	Контроль состояния технической защиты конфиденциальной информации	+	+

Примечания:
«+»- раздел обеспечивает изучение данной учебной дисциплины; «-»- раздел не обеспечивает изучение данной учебной дисциплины.

Лабораторный практикум.

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

Практические занятия (семинары)

п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1		Физическиепроцессы, Возникающие при Воздействии мощными Электрическими и Магнитными полями и токами на технические средства обработки информации	2
2.	1	Угрозы безопасности информации от специальных электромагнитных воздействий		2
3.	1	Организация и содержание работ по защите		2
		информации от преднамеренных силовых электромагнитных воздействий		2
			Меры и средства защиты конфиденциальной информации от специальных электромагнитных и электрических воздействий	2
		Экранирующие материалы и покрытия. Экранирование электростатических, электродинамических полей и низкочастотных магнитных полей. Конструкции экранирующих корпусов и их элементы		2
		Экранирующие системы зданий и помещений. Вводно-защитные устройства для зданий и помещений		2
		Фильтры, разрядники и поглощающие устройства для защиты технических средств обработки информации от электрических воздействий		2

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) 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.

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

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

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

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

б) дополнительная литература:

1. Мощные сверхкороткоимпульсные 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.

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

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

4. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

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

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

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

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

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

10. 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.

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

12. Базы данных, информационно-справочные и поисковые системы: www.pravo.gov.ru,www.fstec.ru,www.gost.ru/wps/portal/tk362/; правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

Материально-техническое обеспечение учебной дисциплины

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

В лаборатории присутствует специализированное оборудование, содержащее образцы различных материалов с экранирующими и поглощающими свойствами для защиты информации от электромагнитных 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.

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 обучающихся.

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 обучающиеся 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.

На изучение теоретических вопросов учебной дисциплины отводится 30 % учебного времени, практических - 70%.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы

обучающихся 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 примерных вопросов, выносимых для контроля знаний обучающихся:

1. Информация как объект защиты от специальных электромагнитных воздействий.
2. Технические средства обработки информации как объекты защиты от специальных электромагнитных и электрических воздействий.
3. Перечень угроз безопасности информации от специальных электромагнитных и электрических воздействий.
4. Механизм влияния электромагнитных и электрических воздействий на технические средства обработки информации.
5. Организация и содержание работ по защите информации от преднамеренных силовых электромагнитных воздействий.
6. Принципы использования экранирующих и поглощающих свойств различных материалов для защиты информации от электромагнитных воздействий.
7. Принципы использования фильтрующих и поглощающих устройств и материалов для защиты информации от электрических воздействий.
8. Средства обнаружения преднамеренных силовых электромагнитных воздействий.

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

Цель учебной дисциплины: формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам организации защиты конфиденциальной информации на объектах информатизации.

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: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий» и «Организация защиты конфиденциальной информации на объектах информатизации».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются для изучения последующей учебной дисциплины программы профессиональной переподготовки «Аттестация объектов информатизации по требованиям безопасности информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ в организации; в проектной деятельности;

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

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 обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;

способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

Комплекс знаний, умений и навыков, получаемых обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

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

цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации;

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

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации;

порядок проведения аттестации объектов информатизации по требованиям безопасности информации;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий);

общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

средства ТЗКИ и контроля защищенности информации, порядок их применения;

программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей;

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

типовую структуру, задачи и полномочия подразделения по ТЗИ;

уметь:

работать с действующей нормативной правовой и методической базой в области защиты информации;

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

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации;

применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты;

определения задач, способов и средств ТЗКИ и контроля защищенности информации;

использования программных и аппаратных средств ТЗКИ и контроля защищенности информации;

проведения организационных и технических мероприятий по ТЗКИ, контролю защищенности информации, оценки состояния ТЗИ;

Объем учебной дисциплины и виды учебной работы.

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 31 час.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**20**
лекции (Л)	8
практические занятия (ПЗ)	8
семинары (С)	6
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего), в том числе:	**9**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	7
Вид промежуточной аттестации (зачет)	2
Итого:	**31**

Содержание учебной дисциплины

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
т	Планирование работ по технической защите конфиденциальной информации. Стадии создания системы защиты информации объекта информатизации	Планирование работ по ТЗКИ. Сущность, цели и задачи планирования. 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 учреждений и предприятий. Стадии и этапы создания системы защиты конфиденциальной информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требования безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации
2.	Реализация требований по технической защите конфиденциальной информации	Реализация требований по защите 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 НСД и специальных воздействий при создании нового объекта информатизации в защищенном исполнении. Особенности реализации требований по защите персональных данных

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	2
1.	Аттестация объектов информатизации по требованиям безопасности информации	+	+
2.	Контроль состояния технической защиты конфиденциал ьной информации	+	+

Примечания: «+» - раздел обеспечивает изучение данной учебной дисциплины; «—» - раздел не обеспечивает изучение данной учебной дисциплины.

Лабораторный практикум.

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

Практические занятия (семинары)

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1		Порядок планирования и организации работ в интересах обеспечения ТЗИ на защищаемых объектах информатизации	2
2.	1		Стадии создания системы защиты информации объекта информатизации	2
3.	1	Разработка руководства по защите информации	—	4
6.	2		Особенности реализации требований по защите информации от НСД на эксплуатируемом (функционирующем) объекте информатизации.	2
7.	2	Особенности реализации требований по защите информации от НСД при создании нового объекта информатизации в защищенном исполнении.		2
8.	2	Особенности реализации требований по защите персональных данных		2

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) **основная литература:**

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

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

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

б) **дополнительная литература**:

1. Гзегжда Д.П. Основы безопасности информационных систем - М.: «Горячая линия - Телеком», 2000.

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

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

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. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

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

11. 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.

12. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

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

14. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

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

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

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

18. 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.

19. 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.

20. 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.

21. 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 недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

22. 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

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

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

25. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Госстандарт, 2014.

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

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

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

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

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

31. 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.

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

33. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.

34. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013.

35. 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.

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

37. 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.

38. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

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

40. ГОСТ Р ИСО/МЭК 18028-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности. Ростехрегулирование, 2008.

41. 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.

42. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2012.

43. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 2700 Т.2005). Ростехрегулирование, 2006.

44. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.

45. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности.

Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.

46. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Росстандарт, 2011.

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

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

49. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

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

51. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

52. 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.

53. 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.

54. Базы данных, информационно-справочные и поисковые системы: www.fstec.ru;www.gost.ru/wps/portal/tk362.

Материально-техническое обеспечение учебной дисциплины.

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

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 обучающихся.

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 обучающиеся 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.

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70%.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

1. Планирование работ по ТЗКИ.
2. Порядок планирования и организация работ в интересах обеспечения ТЗКИ на защищаемых объектах информатизации.
3. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.
4. Создание и функционирование системы защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.
5. Стадии создания системы защиты конфиденциальной информации объекта информатизации.
6. Разработка эксплуатационной документации на систему защиты информации.
7. Особенности реализации требований по защите речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам.

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

9. Особенности реализации требований по защите информации от НСД при создании нового объекта информатизации в защищенном исполнении.

10. Особенности реализации требований по защите персональных данных

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

Цель учебной дисциплины: - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам аттестации объектов информатизации по требованиям безопасности информации.

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: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий» и «Организация защиты конфиденциальной информации на объектах информатизации».

Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются для изучения последующей учебной дисциплины программы профессиональной переподготовки «Контроль состояния технической защиты конфиденциальной информации».

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность проводить контроль (мониторинг) и анализ применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

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 обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

физические основы возникновения, классификацию и характеристики ТКУИ;

угрозы безопасности информации;

требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объекта информатизации;

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;

общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

уметь:

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

работать с действующей нормативной правовой и методической базой в области защиты информации;

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации;

применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты;

обследования, категорирования и аттестации объектов информатизации по требованиям безопасности информатизации;

применения экспертно-документального и инструментального методов, метода проверки соответствия настройки элементов системы защиты информации требованиям безопасности информации с проведением проверки подсистем защиты информации от НСД, проверки программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации при проведении аттестационных испытаний объектов информатизации по требованиям безопасности информации.

Объем учебной дисциплины и виды учебной работы

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 34 часа.

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**26**
лекции (Л)	4
практические занятия (ПЗ)	10
семинары (С)	8
лабораторные работы (ЛР)	4
Самостоятельная работа (СР, всего), в том числе:	**8**
курсовой проект (работа)	-
расчетно-графические работы	-
реферат	-
Другие виды самостоятельной работы	6
Вид промежуточной аттестации (зачет)	2
Итого:	**34**

Содержание учебной дисциплины.

Рассматривается аттестация объектов информатизации, требования к аттестации и перечни ее работ, а также структура системы аттестации.

Содержание разделов учебной дисциплины.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.		средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации
2.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная). Участники аттестации и их полномочия (компетенции). Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектахинформатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации
3.	Порядок проведения аттестации объектов информатизации	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 (экспертнодокументальный метод; 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

Лабораторный практикум.

№ п/п	№ раздела учебной дисциплины	Наименование лабораторной работы	Кол-во часов
1.	3	Анализ возможных каналов утечки речевой информации. Выбор (уточнение) точек возможного ведения разведки (точек контроля показателя защищенности) применительно к условиям объекта информатизации. Выбор (уточнение) точек контроля показателя защищенности применительно к условиям объекта информатизации	2
2.	3	Специальные исследования СВТ, расчет показателей защищенности (Зона 2). Оформление протоколов стендовых специальных исследований и предписания на эксплуатацию СВТ	2

Практические занятия (семинары).

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1		Нормативная правовая и методическая база системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации потребованиям безопасности информации	4
2.	2	Организация аттестации защищаемого помещения по требованиям безопасности информации		4
3.	2	Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД		2
4.	3	Методы аттестационных испытаний	—	2
5.	3	Проверка подсистем защиты информации от НСД	-	2
6.	3		Состав и содержание документов, Разрабатываемых для проведения аттестации и по результатам аттестации объекта информатизации. Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия	4

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А, Основы информационной безопасности: учеб, пособие - М.: «Горячая линия - Телеком», 2005.

2. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, С.В. Дворянкин, А.П. Дураковский, Р.С. Енгалычев, Т.А. Кондратьева, В.С. Лаврентьев, В.А. Петров, В.Р. Петров; под общей редакцией Ю.Н. Лаврухина. - М.: НИЯУ МИФИ, 2014.-560 с.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: «Горячая линия - Телеком», 2011;

б) дополнительная литература:

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

2. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: «Гелиос-АРВ», 2003.

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

4. Хорев А. А. Аттестация объектов информатизации и выделенных помещений. - Статья опубликована в журнале «Специальная техника». - 2006, №4

5. Будников С.А, Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное -Издательство им. Е.А.Болховитинова, Воронеж, 2011.

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

7. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

8. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

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

10. Базы данных, информационно-справочные и поисковые системы: www.fstec.ru;www.gost.ru/wps/portal/tk362.

Программное обеспечение:

специализированное, предусмотренное лабораторным практикумом

Материально-техническое обеспечение учебной дисциплины.

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

Для изучения учебной дисциплины имеются 3 учебные лаборатории:

«Контроль защищенности локальных вычислительных сетей от несанкционированного доступа»; «Защита информации от утечки по

техническим каналам»; «Защита речевой информации от утечки за счет недостаточной звуковой и виброизоляции помещений».

Специализированные лаборатории оснащены полным комплексом программно-технических средств, соответствующих реальному оборудованию, необходимому для проведения лабораторных работ, необходимым количеством тест-объектов, эквивалентов строительных и иных конструкций, позволяющих полностью имитировать реальные ситуации при выполнении аттестационных испытаний объектов информатизации.

Цикл занятий по исследованию защищенности от утечки информации по техническим каналам в защищаемых помещениях и автоматизированных системах целесообразно проводить в специализированной лаборатории «Защита информации от утечки по техническим каналам».

Цикл занятий по исследованиям защищенности речевой конфиденциальной информации от утечки по вибро-акустическим каналам целесообразно проводить в специализированной лаборатории «Защита речевой информации от утечки за счет недостаточной звуковой и виброизоляции помещений».

Цикл занятий по контролю защищенности и моделированию системы защиты информации автоматизированных систем в части защиты от НСД целесообразно проводить в специализированной лаборатории «Контроль защищенности локальных вычислительных сетей от НСД».

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 должна излагаться проблемным методом с привлечением обучающихся 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 обучающихся.

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 обучающиеся 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 по требованиям безопасности информации, обнаружению ТКУИ 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 обучающихся в учебной группе).

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70%.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

1. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.
2. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).
3. Участники аттестации и их полномочия (компетенции).
4. Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий.
5. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.
6. Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации.
7. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации.
8. Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации.
9. Экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний.

10. Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.

11. Проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации.

12. Проверка подсистем защиты информации от НСД, контроль целостности применяемых средств защиты информации от НСД, в том числе с использованием специальных средств контроля защищенности информации.

13. Проверка программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации.

14. 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.

15. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций.

16. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации.

17. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации.

17. Рабочая программа учебной дисциплины «Контроль состояния технической защиты конфиденциальной информации»

Цель учебной дисциплины - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» и приобретения новой квалификации. Совершенствование знаний, умений и навыков специалистов или получение ими дополнительных знаний, умений и навыков по вопросам контроля состояния ТЗКИ.

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: «Организационно-правовые основы технической защиты конфиденциальной информации», «Аппаратные средства вычислительной техники», «Системы и сети передачи информации», «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам», «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа», «Техническая защита конфиденциальной информации от специальных воздействий», «Организация защиты конфиденциальной информации на объектах информатизации» и «Аттестация объектов информатизации по требованиям безопасности информации».

Данная учебная дисциплина является итоговой учебной дисциплиной программы профессиональной переподготовки.

Требования к результатам освоения учебной дисциплины.

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

а) общепрофессиональных:

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

способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в 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 деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность проводить контроль (мониторинг) и анализ применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ в организации;

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 обучающимся в результате изучения учебной дисциплины, должен формироваться из приведенного ниже списка.

Обучающийся должен знать:

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

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

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;

организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий);

общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

требования к средствам ТЗКИ и контроля защищенности информации; средства ТЗКИ и контроля защищенности информации, возможности и порядок применения, перспективы развития;

типовую структуру, задачи и полномочия подразделения по ТЗКИ;

уметь:

работать с действующей нормативной правовой и методической базой в области защиты информации;

разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации;

применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области защиты информации;

выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты;

определения задач, способов и средств ТЗКИ и контроля защищенности информации;

использования программных и аппаратных средств ТЗКИ и контроля защищенности информации.

Объем учебной дисциплины и виды учебной работы составляет

Общий объем времени, отводимого для освоения учебной дисциплины, составляет 32 часа

Вид учебной работы	Всего часов
Аудиторные занятия (всего), в том числе:	**22**
лекции (Л)	6
практические занятия (ПЗ)	10
семинары (С)	6
лабораторные работы (ЛР)	-
Самостоятельная работа (СР, всего), в том числе:	**10**
курсовой проект (работа)	—
расчетно-графические работы	—
реферат	—
Другие виды самостоятельной работы	8
Вид промежуточной аттестации (зачет)	2
Итого:	**32**

Содержание учебной дисциплины

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 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.	Сертификация средств защиты информации по требованиям безопасности информации	Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля защищенности информации, программных, аппаратных средств защиты информации, программных средств контроля защищенности информации. Особенности сертификации средств защиты информации от утечки по техническим каналам. Особенности сертификации средств защиты информации от НСД

Лабораторный практикум

В процессе изучения учебной дисциплины лабораторный практикум не предусмотрен.

Практические занятия (семинары)

№ п/п	№ раздела учебной дисциплины	Тематика практических занятий (семинаров)		Кол-во часов
		тематика практических занятий	тематика семинаров	
1.	1		Организация и порядок проведения контроля состояния ТЗКИ	2
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	Проведение контроля защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов		2
5.	2	Методика инструментального контроля выполнения норм показателя защищенности речевой конфиденциальной информации		2
6.	2	Методы и средства контроля защищенности речевой конфиденциальной информации от утечки по техническим каналам		2
7.	2	Проведение контроля защищенности речевой конфиденциальной информации от утечки по техническим каналам с использованием программно-аппаратных комплексов		2
8.	2	Методы и средства контроля защищенности конфиденциальной информации от НСД		2

Примерная тематика курсовых проектов (работ):

выполнение курсовых проектов (работ) не предусмотрено.

Учебно-методическое и информационное обеспечение учебной дисциплины:

а) 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.

2. Хорев А.А. Организация контроля эффективности противодействия техническим средствам разведки и защиты информации: учебное пособие. - М.: Министерство обороны Российской Федерации, 2006.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: «Горячая линия - Телеком», 2011.

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

5. Тупота В.И., Петигин А.Ф. Контроль защищенности средств вычислительной техники от утечки информации за счет побочных электромагнитных излучений. Учебное пособие. - Воронеж, 2010;

б) дополнительная литература:

1. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: учебное пособие для вузов. - М.: «Радио и связь», 2000.

2. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. - М.: МО РФ, 1998.

3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие. М.: Гостехкомиссия России, 1998.

4. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник. - М.: «МИФИ», 1997.

5. ЗегждаД.П., Ивашко А.М. Основы безопасности информационных систем - М.: «Горячая линия - Телеком», 2000.

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. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

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 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2.

15. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

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

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

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

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

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

21. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования. Ростехрегулирование, 2007.

22. 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.

23. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Госстандарт, 2012.

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

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). Госстандарт, 2013.

26. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

информационной безопасности. Общий обзор и терминология. Госстандарт, 2012.

27. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.

28. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Госстандарт, 2012.

29. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Росстандарт, 2011.

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

31. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Ростехрегулирование, 2008.

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

33. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

34. 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.

35. 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.

36. Базы данных, информационно-справочные и поисковые системы: www.fstec.ru;www.gost.ru/wps/portal/tk362.

Программное обеспечение:

средства разграничения доступа к компонентам вычислительных сетей; средства разграничения доступа к данным; средства поиска разрушающих программных воздействий (антивирусные программы); средства анализа трафика вычислительных сетей; средства анализа структуры вычислительных сетей;

Материально-техническое обеспечение учебной дисциплины.

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (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 (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).

Для проведения практических занятий оборудованы специализированные учебные лаборатории, оснащенные 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 и защиты информации от утечки по каналам ПЭМИН.

Для проведения занятий имеется: локальная вычислительная сеть; аппаратные средства разграничения доступа к информации, хранимой в ПЭВМ; имитатор радиосигналов; цифровой анализатор спектра; средства контроля защищенности по акустическому каналу; средства контроля ПЭМИН.

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 технической защиты информации, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости обучающихся.

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 обучающиеся 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 по требованиям безопасности информации, обнаружению

ТКУИ 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 обучающихся в учебной группе).

На изучение теоретических вопросов учебной дисциплины отводится 30% учебного времени, практических - 70%.

Формы аттестации и оценочные материалы.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся 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 обучающихся:

1. Основные задачи контроля состояния ТЗКИ.
2. Нормативные и методические документы по контролю состояния ТЗКИ.
3. Вопросы, подлежащие проверке при контроле состояния ТЗКИ.
4. Организация и порядок проведения контроля состояния ТЗКИ.
5. Оценка защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ГТЭМИН.
6. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
7. Проведение контроля защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов.
8. Методика инструментального контроля выполнения норм показателя защищенности речевой конфиденциальной информации.

9. Оценка защищенности речевой конфиденциальной информации от утечки по техническим каналам.

10. Методы и средства контроля защищенности речевой конфиденциальной информации от утечки по техническим каналам.

11. Проведение контроля защищенности речевой конфиденциальной информации от утечки по техническим каналам с использованием программноаппаратных комплексов.

12. Методы контроля защищенности конфиденциальной информации от НСД.

13. Средства контроля защищенности конфиденциальной информации от НСД.

14. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов.

15. Основные этапы и задачи сертификационных испытаний.

16. Основные схемы сертификации.

17. Требования к содержанию программ и методик сертификационных испытаний. Основные разделы программ и методик сертификационных испытаний.

18. Особенности сертификационных испытаний средств защиты информации от НСД.

19. Особенности сертификационных испытаний средств защиты информации по ТКУИ.

Примерная тематика итоговой квалификационной работы

1. Комплексный подход к построению технической защиты информации на объекте информатизации.

2. Основные положения и принципы построения технической защиты информации.

3. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.

4. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации по техническим каналам.

5. Условия и факторы, способствующие утечке информации по техническим каналам, методы и способы противодействия утечке информации.

6. Методы защиты радиосигналов от перехвата техническими средствами разведок.

7. Технические средства контроля эффективности защиты информации на примере вербального объекта информации.

8. Разработка предложений по защите корпоративной сети на основе межсетевого экранирования.

9. Анализ способов оценки защищенности автоматизированных систем в соответствии с документами ФСТЭК России.

10. Сравнительный анализ систем обнаружения и предотвращения компьютерных атак.

11. Моделирование процессов защиты в локальной вычислительной сети организации с внешним доступом в сеть Интернет.

12. Разработка предложений по контент- анализу данных социальных сетей.

13. Оценка защищенности межсетевых экранов в соответствии с документами ФСТЭК России.