ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

ЧУ ДПО "ЦИТ БИС"

Подписано цифровой подписью: ЧУ ДПО "ЦИТ БИС"
DN: email=edu@astralnalog.ru, 1.2.643.3.131.1.1=120C303034303237303936363335, 1.2.643.100.3=120B3030383933313135313432, 1.2.643.100.1=120D31303934303030303031313530, street=ул Циолковского 4 212, c=RU, st=40 Калужская область, l=г Калуга, o=ЧУ ДПО "ЦИТ БИС", title=Директор, givenName=Игорь Ильич, sn=Чернин, cn=ЧУ ДПО "ЦИТ БИС"
Дата: 2022.01.19 10:44:11 +03'00'

УТВЕРЖДАЮ

Директор ЧУ ДПО
«ЦИТ БИС»

_____ И.И. Чернин
«___»_____2018г

Программа
профессиональной переподготовки

«Информационная безопасность. Техническая защита конфиденциальной информации»

г. Калуга

2018 год

1. Общие положения

Настоящая программа профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации» разработана с учетом положений:

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

приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

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

профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 599н;

профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 3 ноября 2016 г. № 608н;

профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;

профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н;

федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1515;

федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1513;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1512;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 16 ноября 2016 г. № 1426;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1509;

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

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

примерной программы профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну», утвержденной ФСТЭК России 30 апреля 2015 г.;

примерной программы профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации», утвержденной ФСТЭК России 28 апреля 2017 г.

2. Цель реализации программы профессиональной переподготовки

Целью реализации программы профессиональной переподготовки является формирование компетенций, необходимых специалистам для выполнения нового вида профессиональной деятельности

«Техническая защита информации» в части защиты конфиденциальной информации.

3. Требования к квалификации поступающего на обучение

К освоению программы профессиональной переподготовки допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук (в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Минобрнауки России).

4. Планируемые результаты обучения

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

5. Условия реализации программы

Лабораторная база учреждения оснащена современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки.

Компьютерные классы оборудованы современной вычислительной техникой для занятий по учебным дисциплинам из расчета одно рабочее место на одного обучающегося при проведении занятий в данных классах.

6. Формы аттестации и оценочные материалы

Форма итоговой аттестации обучающихся, освоивших программу профессиональной переподготовки, экзамен в форме тестирования.

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

Для проведения итоговой аттестации организуется аттестационная комиссия, состав которой утверждается руководителем учреждения.

7. Учебный план программы профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации»

№ п/п	Наименование учебных дисциплин	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и Контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11
1.		454	356	72	74	118	92	16	82	
1.1.	Организационно-правовые основы ТЗКИ	30	18	6	10	2	-	2	10	Зачет
1.2.	Средства и системы обработки информации	62	52	16	4	18	14	2	8	Зачет
1.3.	Способы и средства ТЗКИ от утечки по техническим каналам	80	66	12	14	16	24	2	12	Зачет
1.4.	Меры и средства ТЗКИ от НСД	80	66	10	10	20	26	2	12	Зачет
1.5,	Техническая защита конфиденциальной информации от специальных воздействий	10	6	2	2	2	-	2	2	Зачет
1.6	Организация защиты конфиденциальной информации на объектах информатизации	52	38	6	6	26	-	2	12	Зачет
1.7.	Аттестация объектов информатизации по требованиям безопасности информации	48	36	6	4	14	12	2	10	Зачет
1.8.	Контроль состояния ТЗКИ	92	74	14	24	20	16	2	16	Зачет
2.	Итоговая аттестация	16	4	-	-	-	-	-	12	Экзамен
Итого:		470	360	72	74	118	92	16	94	-

. Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоя-тельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	У чебное время		Учебные занятия по расписанию	Прак тики			
59	8	52/470	470	356	-	82	16	-

8. Календарный учебный график[1]

Срок обучения - 9 недель, 2 месяца.

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

А - аудиторная и самостоятельная работа; И - итоговая аттестация.

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

. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Цели и задачи ТЗКИ	Основные термины и определения в области ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗКИ. Объекты информатизации: классификация и характеристика. Защищаемые информация и информационные ресурсы. Объекты защиты конфиденциальной информации. Государственные информационные ресурсы негосударственные информационные ресурсы находящиеся в ведении органов государственной власти и организаций. Перечень сведений конфиденциального характера, подлежащих защите. Угрозы безопасности конфиденциальной информации. Классификация ТКУИ. Классификация угроз безопасности информации, связанных с НСД. Модель угроз безопасности информации в заданных условиях функционирования объекта зашиты. Методы выявления и оценки возможности реализации угроз безопасности информации
2.	Основы нормативного правового обеспечения ТЗКИ	Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации.

[1] Календарный учебный график разрабатывается учреждением для каждого заказчика.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		Система стандартов в области защиты информации. Стандарты Единой системы конструкторской документации (ЕСКД), Единой системы технологической документации (ЕСТД) и Единой системы программной документации (ЕСПД). Основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации. Требования по защите конфиденциальной информации на объекте информатизации (от утечки по техническим каналам, от НСД и специальных воздействий). Особенности защиты персональных данных. Требования международных и национальных стандартов по защите информации

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ИЗ	ЛР	С	СР	Всего
1.	Цели и задачи ТЗКИ	2	-	-	2	4	8
2.	Основы нормативного правового обеспечения ТЗКИ	4	2	-	8	6	20

10. Рабочая программа учебной дисциплины

«Средства и системы обработки информации»

. Содержание разделов учебной дисциплины

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

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

. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ИЗ	ЛР	С	СР	Всего
1.	Технические средства обработки информации	6	8	4	-	2	20
2.	Информационные технологии	4	-	4	2	2	12
3.	Вычислительные сети, сети и системы передачи информации	6	10	6	2	4	28

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

Содержание разделов учебной дисциплины

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

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		Прямой акустический канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата информации по прямому акустическому каналу. Средства перехвата акустической речевой информации, использующие микрофоны воздушной проводимости. Вибрационный канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата акустической речевой информации по вибрационному каналу. Средства перехвата акустической речевой информации, использующие вибропреобразователи. Оптико-электронный канал утечки акустической речевой информации из защищаемых помещений. Схема перехвата акустической речевой информации по оптико-электронному каналу. Средства перехвата акустической речевой информации, использующие «лазерные микрофоны». Акустоэлектрический канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектрического канала утечки акустической речевой информации. Схема активного акустоэлектрического канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектрического преобразования речевого сигнала. Акустоэлектромагнигный канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектромагнитного канала утечки акустической речевой информации. Схема активного акустоэлектромагнитного канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектромагнитного преобразования речевого сигнала. Каналы утечки акустической речевой информации, использующие высокочастотные генераторы

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок	Классификация способов и средств защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Способы и средства пассивной защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Экранирование технических средств и их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Поглощение электромагнитных волн. Безэховые камеры, поглощающие чехлы и накидки. Способы и средства активной защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Системы пространственного электромагнитного зашумления. Требования к системе пространственного электромагнитного зашумления. Основные характеристики систем пространственного электромагнитного зашумления. Системы линейного электрического зашумления. Требования к системе линейного электрического зашумления. Основные характеристики систем линейного электрического зашумления. Особенности зашумления инженерных коммуникаций. Требования к системам электроснабжения и заземления ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. Способы и средства защиты информации от утечки по цепям электроснабжения и заземления. Установка, монтаж, настройка, испытания, ремонт и техническое обслуживание средств защиты информации от утечки за счет Г1ЭМИН. Устранение неисправностей и организация ремонта средств защиты информации от утечки за счет ПЭМИН

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
3.	Способы и средства защиты акустической речевой информации от утечки по техническим каналам	Классификация способов и средств защиты акустической речевой информации от утечки по техническим каналам. Способы и средства пассивной акустической речевой информации от утечки по техническим каналам. Звукоизоляция и экранирование защищаемых помещений, звукопоглощающие материалы. Способы и средства пассивной акустической речевой информации от утечки по акустоэлектрическим каналам, каналам ВЧ-навязывания и ВЧ-прокачки (ограничение сигналов по амплитуде, установка НЧ-фильтров в соединительных линиях ВТСС, отключение акустоэлектрических преобразователей сигналов). Способы и средства активной защиты акустической речевой информации от утечки по техническим каналам. Акустическая и виброакустическая маскировка. Требования к системе виброакустической защиты. Системы и средства виброакустической защиты. Особенности установки акустических излучателей и виброизлучателей. Способы и средства активной защиты акустической речевой информации от утечки по акустоэлекгрическому каналу, каналам ВЧ-навязывания и ВЧ-прокачки. Специальные технические средства подавления электронных устройств негласного получения акустической речевой информации, порядок их установки и настройки. Установка, монтаж, настройка, испытание, ремонт и техническое обслуживание средств защиты акустической речевой информации от утечки по техническим каналам. Устранение неисправностей и организация ремонта средств защиты акустической речевой информации от утечки по техническим каналам

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Технические каналы утечки информации	4	4	8	6	4	26
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	4	6	6	4	4	26
3.	Способы и средства защиты акустической речевой информации от утечки по техническим каналам	4	6	6	4	4	26

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

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Угрозы безопасности информации, связанные с НСД	Понятие и общая классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS)
2.	Меры и средства защиты информации от НСД	Общая характеристика и классификация мер и средств защиты информации от НСД. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Средства защиты информации от НСД. Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения. Общий порядок разработки и производства средств защиты информации от НСД. Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	Г13	ЛР	С	СР	Всего
1.	Угрозы безопасности информации, связанные с НСД	4	4	-	4	2	14
2.	Меры и средства защиты информации от НСД	6	16	26	6	10	64

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

Содержание разделов учебной дисциплины

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

. Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины(модуля)	Л	ИЗ	ЛР	С	СР	Всего
1.	Информация как объект защиты от специальных воздействий	2	2	-	2	2	8

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

. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Организация защиты конфиденциальной информации на объектах информатизации	Организация работ по созданию и эксплуатации объектов информатизации и их систем защиты информации. Положение о порядке организации и проведения работ по защите конфиденциальной информации. Перечень сведений конфиденциального характера, подлежащих защите. Планирование работ по ТЗКИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ
2.	Реализация требований по ТЗКИ	Реализация требований по защите акустической речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам. Реализация требований по защите информации от НСД и специальных воздействий на эксплуатируемом (функционирующем) объекте информатизации. Реализация требований по защите информации от НСД и специальных воздействий при создании нового объекта информатизации в защищенном исполнении. Особенности реализации требований по защите персональных данных
3.	Проектирование систем защиты конфиденциальной информации	Создание и функционирование систем защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания систем защиты конфиденциальной информации. Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении. Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		объекта информатизации). Разработка эксплуатационной документации на систему защиты информации

Разделы учебной дисциплины и виды занятий

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

15. Рабочая программа учебной дисциплины

«Аттестация объектов информатизации по требованиям безопасности информации»

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции). Задачи, функции, права и обязанности органов по аттестации. Требования к органам по аттестации объектов информатизации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации
2.	Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия). Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации. Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно-документальный метод; измерение и оценка уровней ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их выполнением; попытки «взлома систем защиты информации»). Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	2	-	-	2	2	6
2.	Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	4	14	12	2	8	40

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

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Основы организации контроля состояния ТЗКИ	Основные задачи контроля состояния ТЗКИ. Классификация видов контроля состояния ТЗКИ. Система документов по контролю состояния ТЗКИ. Вопросы, подлежащие проверке при контроле состояния ТЗКИ. Организационный и технический контроль состояния ТЗКИ
2.	Методы и средства контроля защищенности конфиденциальной информации	Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам. Методы и средства контроля защищенности конфиденциальной информации от НСД. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
3.	Мониторинг информационной безопасности средств и систем информатизации	Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации. Состав и структура системы мониторинга. Основные принципы системы мониторинга информационной безопасности средств и систем информатизации. Обнаружение и идентификация инцидентов безопасности информации, а также событий, приводящих к возникновению инцидентов. Анализ инцидентов безопасности информации, в гом числе определение источников и причин возникновения инцидентов, а также оценку их последствий. Планирование мер по устранению инцидентов безопасности информации, в том числе по восстановлению систем информатизации, их сегментов и средств, входящих в их состав, в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Планирование мер по предотвращению повторного возникновения инцидентов безопасности информации. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации. Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации. Анализ и оценка функционирования систем защиты информации систем информатизации, включая выявление, анализ и устранение недостатков в функционировании систем защиты информации систем информатизации. Периодический анализ изменения угроз безопасности информации в средствах и системах информатизации, возникающих в ходе их эксплуатации. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработку предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ по оценке эффективности систем защиты информации систем информатизации

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Основы организации контроля состояния тзки	2	-	-	6	2	10
2.	Методы и средства контроля защищенности конфиденциальной информации	8	14	-	12	10	44
3.	Мониторинг информационной безопасности средств и систем информатизации	4	6	16	6	4	36