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=120C3030343032373039363633335, 1.2.643.100.3=120B303038393331313531343 2, 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: 2022.01.18 18:10:10 +03'00'

УТВЕРЖДАЮ

Директор ЧУ ДПО
«ЦИТ БИС»

_____ И.И. Чернин
«___»_____2017г

Программа
профессиональной переподготовки

«Информационная безопасность. Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

г. Калуга

2017 год

1. Общие положения

Настоящая программа профессиональной переподготовки «Информационная безопасность. Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» разработана с учетом положений Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» и 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».

Программа профессиональной переподготовки «Информационная безопасность. Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» разработана в соответствии с «Методическими рекомендациями по разработке программ профессиональной переподготовки 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 г, примерной программой профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну», утвержденной ФСТЭК России, и на основании требований профессиональных стандартов «Специалист по технической защите информации» и «Специалист по защите информации в автоматизированных системах», а также требований к результатам освоения программы бакалавриата ФГОС высшего образования по направлению подготовки 10.03.01 «Информационная безопасность.

2. 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 в части конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Объектами профессиональной деятельности обучающихся по программе профессиональной переподготовки являются:

3. Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение – среднее или высшее профессиональное образование, подтвержденное документом об образовании. Заказчик обучения гарантирует исполнение данного требования.

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

Итоговая аттестация обучающихся, освоивших программу профессиональной переподготовки, проводится в форме, определяемой учреждением, самостоятельно локальным актом.

7. Учебный план программы профессиональной переподготовки «Информационная безопасность»

№ п/п	Наименование учебных дисциплин	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий (количество часов)					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		552	368	86	116	102	64	18	166	-
1.1.	Организационно-правовые основы ТЗКИ	66	40	10	30	—	—	2	24	Зачет
1.2.	Аппаратные средства вычислительной техники	58	40	6	4	20	10	2	16	Зачет
1.3.	Системы и сети передачи информации	40	28	6	4	14	4	2	10	Зачет
1.4.	Способы и средства ТЗКИ от утечки по техническим каналам	78	54	16	10		28	2	22	Зачет
1.5.	Меры и средства ТЗКИ от несанкционированного доступа	62	40	10	8	8	14	2	20	Зачет
1.6.	Техническая защита конфиденциальной информации от специальных воздействий	54	32	6	8	18		2	20	Зачет
1.7.	Организация защиты конфиденциальной информации на объектах информатизации	62	44	12	20	12		2	16	Зачет
1.8.	Аттестация объектов информатизации по требованиям безопасности информации	68	46	8	8	22	8	2	20	Зачет
1.9.	Контроль состояния ТЗКИ	64	44	12	24	8	—	2	18	Зачет
2.	Итоговая аттестация	54	36	-	-	-	-	-	18	Экзамен/ тест
Итого:		606	404	102	116	142	64	18	184	-

Дисциплины раздела 1 обеспечивают уровень знаний, умений навыков, необходимый для профессиональной деятельности всех обучающихся в области ТЗКИ.

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 самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные	Учебное время		Учебные занятия по расписанию	Практики			
84	11	68/612	606	368	-	166	54	6

8. Примерный календарный учебный график[1]

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.

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

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. Угрозы безопасности конфиденциальной информации. Классификация угроз утечки информациипо техническим каналам. 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. Организация научных исследований и разработок в области ТЗКИ
2.	Основы нормативно-правового обеспечения ТЗКИ	Правовые, нормативные и методические документы, национальные и международные стандарты в области защиты информации. Документы в области технического регулирования и стандартизации. Организационно-правовые 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 информации, содержащейся в информационной системе (на объекте информатизации). Перечень сведений конфиденциального характера, подлежащих защите. Класс защищенности автоматизированных (информационных) систем. Требования по защите речевой конфиденциальной информации. Требования по защите конфиденциальной информации, обрабатываемой в автоматизированных (информационных) системах (от утечки по техническим каналам, от НСД и специальных воздействий). Требования международных и национальных стандартов по защите информации. Требования по защите персональных данных

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Цели и задачи технической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну	2	-	-	4	8	14
2.	Основы нормативно-правового обеспечения технической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну	8	-	-	26	16	50

10. Рабочая программа учебной дисциплины «Аппаратные средства вычислительной техники»

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Основы ЭВМ	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). 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. Понятия кодирования и декодирования информации. Системы счисления: позиционные и непозиционные; двоичные, десятичные, шестнадцатеричные. Форматы числовых данных. Представление символьной информации. Международные системы байтового кодирования. Представление графической информации. Растровые и векторные методы представления цветного изображения. Типы компьютерных устройств хранения информации и их носители. Физический и логический уровни организации хранения данных. Взаимосвязь
2.	Вычислительные системы	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. 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 виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Основы ЭВМ	4	16	6	2	8	36
2.	Вычислительные системы	2	4	4	2	8	20

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

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Сети связи	Сети и средства связи. Основные понятия и определения. Сети 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. 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. 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. Услуги телефонной сети общего пользования. Протокол SIP. Мультисервисная сеть связи. Состав оборудования. Цифровые сети интегрального обслуживания (сети ISDN). Широкополосные цифровые сети интегрального обслуживания. Обеспечение защиты средств связи от НСД. Тенденции развития сетей электросвязи

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
2.	Системы передачи информации	Системы передачи информации. Архитектура и 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. 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. Перспективы развития телекоммуникационных систем в России и за рубежом

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Сети связи	2	4	4	4	2	16
2.	Системы передачи информации	4	10	-	-	8	22

12. 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	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 и классификация ТКУИ, обрабатываемой техническими средствами. Причины возникновения ПЭМИН СВТ. Характеристики ПЭМИН СВТ в различных режимах работы. Принципы построения средств перехвата ПЭМИН СВТ. Схема ТКУИ, возникающего за счет ПЭМИ СВТ. Зона 2. Причины возникновения электрических ТКУИ, обрабатываемойСВТ. Случайные антенны. 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. Способы перехвата речевой информации из защищаемых помещений по прямому акустическому каналу. Схемы перехвата информации по прямым акустическим каналам утечки информации. Средства акустической разведки с датчиками микрофонного типа. Вибрационный, акустооптический, акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации. Способы перехвата речевой информации из защищаемых помещений по вибрационным каналам. Схемы перехвата речевой конфиденциальной информации. Средства перехвата речевой конфиденциальной информации по вибрационным каналам. Способы перехвата речевой конфиденциальной информации из защищаемых помещений по акустооптическому каналу. Схема перехвата речевой конфиденциальной информации по акустооптическому каналу. Лазерные акустические системы разведки.

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Способы перехвата речевой информации из защищаемых помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектрического каналаутечки речевой конфиденциальной информации. Схема активного акустоэлектрического канала утечки речевой конфиденциальной информации. Причины возникновения акустоэлектромагнитных каналов утечки речевой конфиденциальной информации. Способы перехвата речевой информации из защищаемых помещений по акустоэлектромагнитным каналам. Схема пассивного акустоэлектромагнитного канала утечки речевой конфиденциальной информации. Схема активного акустоэлектромагнитного канала утечки речевой информации.
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам	Классификация способов и средств защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Пассивные способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Активные способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Системы пространственного электромагнитного зашумления. Требования к системе пространственного электромагнитного зашумления. Принципы построения широкополосных генераторов шума. Основные характеристики систем пространственного электромагнитного зашумления. Основные характеристики систем линейного электромагнитного зашумления. Особенности зашумления инженерных коммуникаций. Требования к системе электропитания ОТСС. Требования к заземлению ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. Способы и средства защиты информации от утечки по цепям электропитания и заземления. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ. Принципы построения, основные характеристики и требования по установке помехоподавляющих фильтров
3.	Способы и средства защиты защищаемых помещений от утечки акустической речевой информации по техническим каналам	Классификация способов и средств защиты речевой информации от утечки по техническим каналам. Пассивные способы защиты речевой конфиденциальной информации от утечки по техническим каналам. Активные способы защиты речевой конфиденциальной информации от утечки по техническим каналам. Звуко- и виброизоляция защищаемых помещений, звукопоглощающие материалы. Системы и средства виброакустической защиты. Требования к системе виброакустической защиты. Системы виброакустической защиты, построенные на базе генераторов шума и генераторов-изучателей. Принципы построения генераторов шума, акустических излучателей и виброизлучателей. Особенности установки акустическихизлучателей и виброизлучателей. Средства защиты речевой конфиденциальной

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
		информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС. Пассивные способы защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС (ограничение сигналов малой амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС. Принципы построения средств защиты в ОТСС и ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот. Принципы построения средств защиты в ОТСС и ВТСС, основанных на отключении акустоэлектрических преобразователей. Принципы построения средств защиты в ОТСС и ВТСС, основанных на использовании низкочастотных генераторов шума. 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

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	8	-	12	4	6	30
2.	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам	4	-	8	4	6	22
3.	Способы и средства защиты защищаемых помещений от утечки речевой конфиденциальной информации по техническим каналам	4	-	8	2	10	24

13. 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 безопасностиинформации. 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
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. 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 виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Угрозы безопасности информации, связанные с НСД	2	2	—	-	6	10
2.	Меры и средства защиты информации от НСД	8	6	14	8	14	50

14. 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. 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 виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Информация как объект защиты от специальных воздействий	2	6	—	4	8	20
2.	Меры и средства защиты информации от специальных воздействий	4	12	—	4	12	32

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

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	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).

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
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 виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Планирование работ по технической защите конфиденциальной информации. Стадии создания системы защиты информации объекта информатизации	8	12	-	8	10	38
2.	Реализация требований по технической защите конфиденциальной информации	4	—	—	12	6	22

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

Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
1.	Организационно-правовые основы системы аттестации объектов информатизации по 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
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 объектах информатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации

№ п/п	Наименование раздела учебной дисциплины	Содержание раздела
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 (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

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (темы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Организационно-правовые и методические основы системы аттестации объектов информатизации по требованиям безопасности информации	2	-	-	4	2	8
2.	Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	2	12	-	-	6	20
3.	Порядок проведения аттестации объектов информатизации	4	10	8	4	12	38

17. 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 средствоконтролязащищенности 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

Разделы учебной дисциплины и виды занятий

№ п/п	№ (наименование) раздела (гемы) учебной дисциплины (модуля)	Л	ПЗ	ЛР	С	СР	Всего
1.	Основы организации контроля состояния ТЗКИ	2	—	—	4	2	8
2.	Методы и средства контроля защищенности конфиденциальной информации	8	8	-	16	12	44
3.	Сертификация средств защиты информации по требованиям безопасности информации	2	-	-	4	4	10