Частное образовательное учреждение дополнительного профессионального образования «Межрегиональный образовательный центр»

Аннотации

к рабочим программам дисциплин
по программе профессиональной переподготовки «Информационная безопасность. Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

№ п/п	Наименование дисциплины	***Аннотация***
1	Организационно-правовые основы ТЗКИ	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам организационно-правовых основ ТЗКИ. ***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.

		Содержание учебной дисциплины: 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 информации по 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. 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 акустической 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.
2	Аппаратные средства вычислительной техники	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков, связанных с использованием аппаратных средств вычислительной техники. ***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. ***Содержание учебной дисциплины:*** 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 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. 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 (OSI). 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.
3	Системы и сети передачи информации	***Цель учебной дисциплины*** – формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков, связанных с применением систем и сетей передачи 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. ***Содержание учебной дисциплины:*** 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. 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. 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.
4	Способы и средства ТЗКИ от утечки по техническим каналам	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам технической защиты конфиденциальной информации от утечки по техническим каналам. ***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. ***Содержание учебной дисциплины:*** 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 ПЭМИ СВТ. Характеристики ПЭМИ СВТ в различных режимах работы. Принципы построения средств перехвата ПЭМИ СВТ. Схема ТКУИ, возникающего за счет ПЭМИ СВТ. Зона 2. Причины возникновения электрических ТКУИ, обрабатываемой СВТ. Случайные антенны. Характеристики случайных антенн. Зона 1. Схема ТКУИ, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Причины просачивания в линии электропитания и цепи 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 негласного получения информации,

		внедряемых в СВТ. Технические каналы утечки акустической речевой информации. Акустические сигналы. Спектр и типовые уровни речевого сигнала. Классификация технических каналов утечки акустической речевой конфиденциальной информации. Причины возникновения каналов утечки акустической речевой конфиденциальной информации. Способы перехвата акустической 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. Способы перехвата акустической речевой информации из защищаемых помещений по вибрационным каналам. Схемы перехвата акустической речевой конфиденциальной информации. Средства перехвата акустической речевой конфиденциальной информации по вибрационным каналам. Способы перехвата акустической речевой конфиденциальной информации из защищаемых помещений по акустооптическому каналу. Схема перехвата акустической речевой конфиденциальной информации по акустооптическому каналу. Лазерные акустические системы разведки. Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Способы перехвата акустической речевой информации из защищаемых помещений по акустоэлектрическим каналам. Схема пассивного акустоэлектрического канала утечки акустической речевой конфиденциальной информации. Схема активного акустоэлектрического канала утечки акустической речевой конфиденциальной информации. Способы перехвата акустической речевой информации из защищаемых помещений по акустоэлектромагнитным каналам. Схема пассивного акустоэлектромагнитного канала утечки акустической речевой конфиденциальной информации. Схема активного акустоэлектромагнитного канала утечки акустической речевой информации. Способы перехвата информации за счет «высокочастотного облучения», «высокочастотного навязывания» и «высокочастотной прокачки». Классификация способов и средств защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Способы и средства пассивной защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Способы и средства активной защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Экранирование технических средств и 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 электрического 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. Классификация способов и средств защиты акустической речевой информации от утечки по техническим каналам. Способы пассивной защиты акустической речевой конфиденциальной информации от утечки по техническим каналам. Способы активной защиты акустической речевой конфиденциальной информации от утечки по техническим каналам. Звуко- и виброизоляция защищаемых помещений, звукопоглощающие материалы. Требования к системе виброакустической защиты. Системы и средства виброакустической защиты. Системы виброакустической защиты, построенные на базе генераторов шума и генераторов-излучателей. Принципы построения генераторов шума, акустических излучателей и виброизлучателей. Особенности установки акустических излучателей и виброизлучателей. Средства защиты акустической речевой информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС. Способы пассивной защиты акустической речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС (ограничение сигналов по амплитуде, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Способы активной защиты акустической речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ОТСС и ВТСС. Принципы построения средств защиты в ОТСС и ВТСС, основанных на использовании ограничителей 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 негласного получения акустической речевой конфиденциальной информации, порядок их установки и настройки. Общий порядок разработки и производства средств защиты акустической речевой конфиденциальной информации.

5	Меры и средства ТЗКИ от утечки по техническим каналам	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам защиты конфиденциальной информации от НСД. ***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 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. ***Содержание учебной дисциплины:*** 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.
6	Техническая защита конфиденциальной информации от специальных воздействий	***Цель учебной дисциплины*** - формирование (совершенствование и(или) получение специалистами дополнительных). знаний, умений и навыков по вопросам технической защиты конфиденциальной информации от специальных воздействий. ***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; 6) 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 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 для обеспечения информатизации 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. ***Содержание учебной дисциплины:*** Информация как объект защиты от специальных электромагнитных воздействий. Технические воздействий 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. 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.
7	Организация защиты конфиденциальной информации на объектах информатизации	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам организации защиты конфиденциальной информации на объектах информатизации. ***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; 6) 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. ***Содержание учебной дисциплины:*** 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 требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации. 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.
8	Аттестация объектов информатизации по требованиям безопасности информации	***Цель учебной дисциплины*** - формирование (совершенствование и (или) получение специалистами дополнительных) знаний, умений и навыков по вопросам аттестации 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 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. ***Содержание учебной дисциплины:*** 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 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. 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.
9	Контроль состояния ТЗКИ	***Цель учебной дисциплины*** - формирование (совершенствование и(или) получение специалистами дополнительных). знаний, умений и навыков по вопросам контроля

		состояния ТЗКИ. ***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; 6) 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. ***Содержание учебной дисциплины:*** 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 ТЗКИ. 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. 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.
10	Итоговая аттестация	***Экзамен***

Директор В.Ю. Филоненко

ЧОУ ДПО "МОЦ"

Подписан цифровой подписью: ЧОУ ДПО "МОЦ"
DN: OID.1.2.643.100.4=4826049695, СНИЛС=03551729247, ОГРН=1064823007919, ИНН=482601419024, E=vfilonenko@list.ru, C=RU, S=48 Липецкая область, L=ГОРОД ЛИПЕЦК, STREET=",НИЖНЯЯ ЛОГОВАЯ УЛИЦА,ДОМ 2,,ПОМЕЩЕНИЕ 9", O="ЧОУ ДПО ""МОЦ""", CN="ЧОУ ДПО ""МОЦ""", T=Директор, G=ВИКТОР ЮРЬЕВИЧ, SN=ФИЛОНЕНКО
Основание: Я являюсь автором этого документа
Расположение:
Дата: 2022.09.21 11:19:35+03'00'
Foxit PDF Reader Версия: 12.0.0