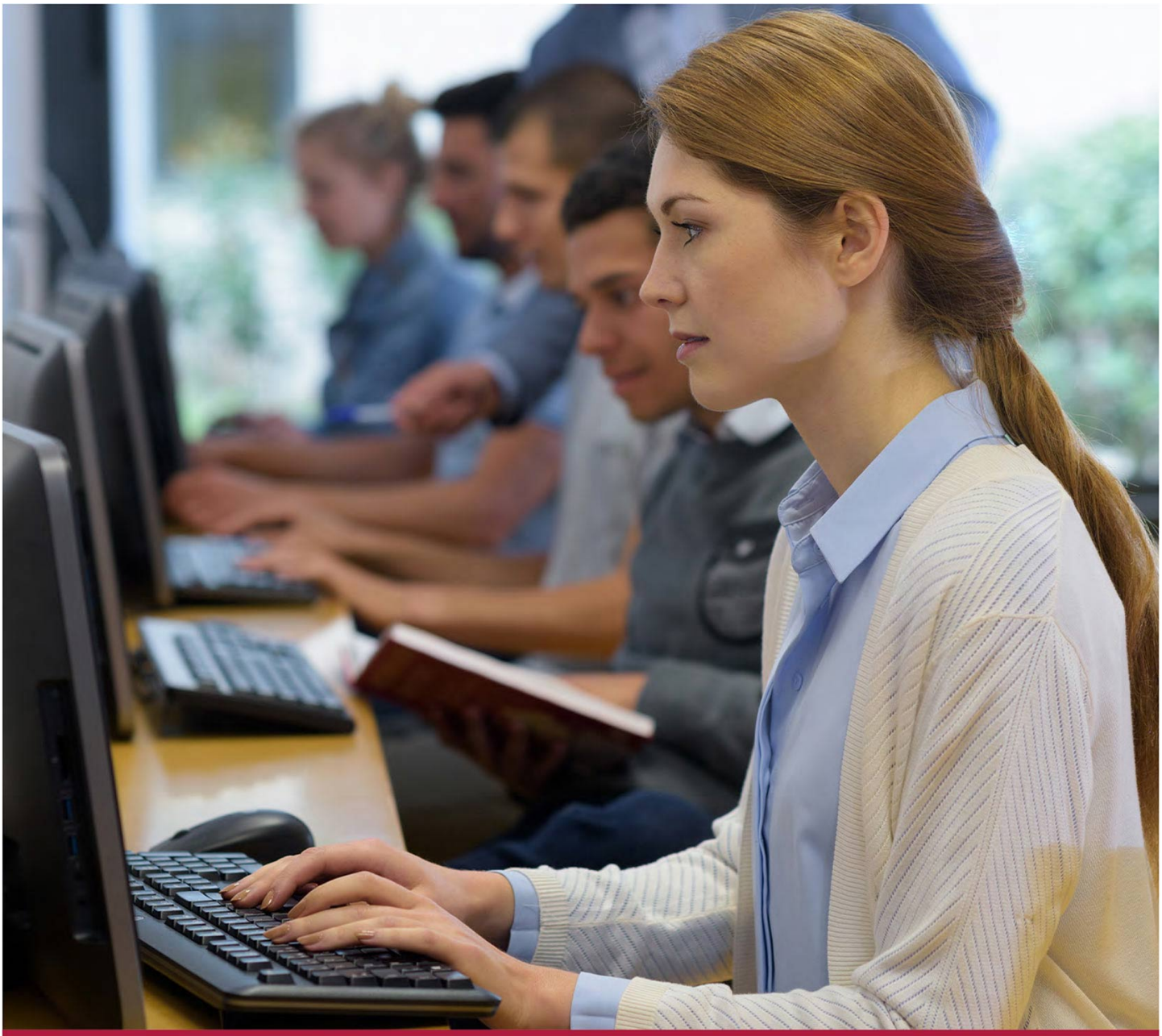
softline®

Учебный центр Softline



Комплексная защита объектов информатизации

Код курса: БПД-КЗОИ-664

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

© Softline 2020

Комплексная защита объектов информатизации

Код курса: БПД-КЗОИ-664

Длительность	664 ак. часа
Формат	Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Программа разработана в соответствии с правовыми и нормативными актами в области ИБ, введенными в действие указами Президента РФ, постановлениями Правительства РФ и организационно-распорядительными документами ФСБ России.

Подробная информация

Профиль аудитории:

- Руководители и главные специалисты структурных подразделений по защите информации в федеральных органах исполнительной власти, администрациях субъектов Российской Федерации, органах местного самоуправления, организациях и учреждениях;
- Соискатели лицензий ФСБ России, чья деятельность связана с криптографической и технической защитой информации;
- Лицензиаты ФСБ России для продления лицензий;
- Специалисты, планирующие сменить деятельность на работу в сфере информационной безопасности;
- Иные специалисты, деятельность которых связана с обеспечением соответствия режима безопасности информации ограниченного доступа требованиям федеральных регуляторов, нормативно-правовому и организационно-техническому обеспечению информационной безопасности.

Предварительные требования:

- Высшее или среднее профессиональное образование по направлению подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей, либо высшее техническое или среднее профессиональное (техническое) образование с опытом работы не менее 3 лет в сфере обеспечения информационной безопасности.

По окончании курса слушатели смогут:

- Использовать основные естественнонаучные законы, понимать значение информации,

© Softline 2020

применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации;
- Использовать нормативные правовые документы в своей профессиональной деятельности;
- Формировать комплекс мер по информационной безопасности;
- Организовывать и поддерживать выполнение комплекса мер по информационной безопасности;
- Организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;
- Использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
- Определять виды и формы информации, подверженной угрозам;
- Принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;
- Администрировать подсистемы информационной безопасности объекта;
- Участвовать в разработке подсистемы управления информационной безопасностью;
- Оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;
- Использовать инструментальные средства и системы программирования для решения профессиональных задач;
- Проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- Разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- Формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
- Применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;
- Организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, и Федеральной службой по техническому и экспортному контролю.

Программа курса

Блок №1. Техническая защита информации

Модуль № 1. Правовые и организационные основы технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

- Основные понятия в области ТЗИ. Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Концептуальные задачи в области ТЗИ. Государственная система защиты информации Российской Федерации. Законодательные акты, Постановления Правительства, указы Президента Российской Федерации и иные правовые акты. Государственные стандарты, отраслевые стандарты, руководящие и специальные нормативные документы, регулирующие вопросы защиты конфиденциальной информации в Российской Федерации. Международные стандарты в сфере защиты информации. Международные стандарты в сфере защиты информации. Структура системы ТЗИ в субъектах Российской Федерации и направления её деятельности. Органы,

© Softline 2020

обеспечивающие ТЗИ в субъектах Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи и функции Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи и функции управлений ФСТЭК России по федеральным округам.
- Лицензирование деятельности в области технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.
- Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.

Модуль № 2. Выявление угроз безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации.

- Основные определения «угрозы безопасности информации», «источник угрозы», «уязвимость», «утечка», «технический канал утечки информации», «модель угроз», «модель нарушителя».
- Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы обнаружения уязвимостей, оценка вероятности реализации угроз, с использованием обнаруженных уязвимостей. Методы обнаружения уязвимостей, оценка вероятности реализации угроз, с использованием обнаруженных уязвимостей. Методы оценки опасности угроз. Классификация объектов информатизации и информационных ресурсов.
- Методические рекомендации по классификации объектов защиты. Идентификация объектов защиты, наиболее подверженных угрозами. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных типов уязвимостей. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Способы реализации атак с использованием стека протоколов TCP/IP.
- Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации.

Модуль № 3. Основные механизмы защиты, организационные меры, технические и программные средства защиты информации от несанкционированного доступа

- Основные механизмы защиты информации. Идентификация и аутентификация. Криптография и шифрование. Методы разграничения доступа. Регистрация и учет. Межсетевое экранирование.
- Общая характеристика существующих технических и программных средств защиты информации от несанкционированного доступа. Основные классы устройств.
- Основные меры и средства защиты информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Основные меры и средства защиты информации в локальных вычислительных сетях. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Основные классы средств защиты информации при межсетевом взаимодействии. Типы средств межсетевого экранирования, основные возможности, способы размещения средств межсетевого экранирования в

 © Softline 2020

локальной вычислительной сети.
- Средства обнаружения вторжений, возможности, типы. Средства анализа защищенности. Средства мониторинга, управления и реагирования на инциденты информационной безопасности. Защита информации при работе с системами управления базами данных. Средства защиты от воздействия вредоносных программ, основные типы, их недостатки и преимущества. Средства защиты информации в виртуальных средах. Документационное обеспечение использования технических средств защиты информации. Состав и содержание документов.
- Защита информации, передаваемой по информационно-телекоммуникационным каналам связи с использованием средств криптографической защиты. Симметричные и ассиметричные криптосистемы, недостатки и преимущества. Основные алгоритмы. Хэш-функция. Технологии электронной подписи. Инфраструктура открытых ключей. Типы сертифицированных средств криптографической защиты информации. Организационные особенности защиты информации с использованием средств криптографической защиты информации, необходимые мероприятия. Требования к организационно-штатному обеспечению. Перечень необходимых организационно-распорядительных документов.

Модуль № 4. Основные организационные меры и технические средства защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации и в защищаемых помещениях от утечки по техническим каналам.

- Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации и защищаемых помещений. Классификация ТКУИ. Характеристики информационных сигналов, определяющие степень их опасности. Методы и средства выявления ТКУИ на типовом объекте информатизации и в защищаемых помещениях.
- Утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН), физические основы возникновения, структура каналов, способы измерения и контроля. Основные требования и рекомендации по защите информации от утечек за счет ПЭМИН.
- Каналы утечки речевой информации. Акустический и виброакустический каналы. Особенности распространения звуковых колебаний в различных средах. Утечка речевой информации по проводным коммуникациям, акустоэлектрические преобразования, активные и пассивные методы съема информации, механизмы реализации. Съем речевой информации за счет использования оптико-электронных излучений, механизмы реализации. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
- Способы оценки защищенности информации от утечки по ТКУИ. Принципы оценки, проведения замеров и расчетов. Содержание и порядок организации и проведения специальных исследований технических средств обработки информации. Оценка защищённости помещений от утечки речевой информации по акустическому и виброакустическому каналам и по каналу электроакустических преобразований во вспомогательных технических средствах и системах.
- Оценка защищённости информации, обрабатываемой основными
- техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.
- Состав контрольно-измерительного оборудования для проведения оценки защищенности объекта информатизации.
- Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

© Softline 2020

Модуль № 5. Нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений.

- Цели и задачи организации ТЗИ на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений. Общий порядок организации ТЗИ на действующих объектах информатизации. Составление перечня сведений конфиденциального характера. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Методика принятия управленческих решений по организации защиты информации. Принципы построения комплексной системы защиты информации.
- Порядок разработки и согласования проектов ТТЗ на проведение научно-исследовательских и опытно-конструкторских работ в интересах создания систем защиты информации на объектах информатизации.
- Необходимое нормативное и информационное обеспечение ТЗИ на объектах информатизации. Система требований по ТЗИ на объектах информатизации и процедура обоснования указанных требований. Порядок разработки и согласования требований по ТЗИ. Оценка достаточности и обоснованности запланированных мероприятий по ТЗИ.
- Основные требования и рекомендации по защите сведений, связанных с профессиональной деятельностью, доступ к которым ограничен в соответствии с законодательством Российской Федерации. Основные рекомендации по защите информации, составляющей коммерческую тайну.
- Структура подразделений, ответственных за реализацию ТЗИ на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений. Принципы построения системы ТЗИ. Функции, задачи, права и обязанности подразделений, ответственных за реализацию ТЗИ. Документационное обеспечение ТЗИ, структура разрабатываемых внутренних нормативных документов, регламентирующих вопросы ТЗИ. Виды разрабатываемых документов, содержание, правила составления. Жизненный цикл документов. Повышение осведомленности в вопросах ТЗИ. Основные роли, задействованные в обеспечении защиты информации, их обязанности и ответственность.
- Порядок разработки и согласования проектов планов и ТТЗ по выполнению работ по строительству, реконструкции и техническому переоснащению объектов информатизации, оценка обоснованности запланированных мероприятий по ТЗИ. Порядок разработки и согласования требований по ТЗИ для этапа строительства, реконструкции и технического переоснащения объектов информатизации.
- Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Модуль №6. Оценка состояния технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений

- Цели проведения оценки состояния ТЗИ на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений субъектов Российской Федерации. Показатели и критерии оценки состояния ТЗИ. Требования к показателям и процедуре оценки состояния ТЗИ. Методические рекомендации по сбору исходной информации для проведения оценок состояния ТЗИ и обобщения этой информации.

© Softline 2020

Методики определения показателей оценки состояния ТЗИ.
- Цели, принципы и задачи развития системы ТЗИ в субъекте Российской Федерации. Определение приоритетных мероприятий по повышению эффективности ТЗИ и обеспечение деятельности системы ТЗИ в субъекте Российской Федерации.

Блок № 2. Защита информации с использованием шифровальных (криптографических) средств

Модуль № 1. Криптографические методы защиты информации

- История криптографии. Три основных способа защиты информации. Четыре этапа криптографии. Актуальные задачи криптографии. Криптосистемы (симметричные, ассиметричные). Понятие имитозащиты и имитовставки. Чем занимается криптография. Что такое криптоанализ. Основы криптоанализа. Методы криптоанализа. Статистический криптоанализ. Алгебраический криптоанализ. Дифференциальный (или разностный) криптоанализ. Линейный криптоанализ. Удостоверяющий центр.

Модуль № 2. Основные понятия, термины и определения

- Криптология, как наука. Терминология. Две части криптологии. Основные понятия в области СКЗИ. Смежные дисциплины. Математические методы сжатия информации – преобразование информации за счет уменьшения избыточности. Кодирование информации — процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки. Наивная криптография. Формальная криптография. Научная криптография. Компьютерная криптография. Современная криптография.

Модуль № 3. Законодательная, нормативная и специальная методическая база использования шифровальных (криптографических) средств.

- Нормативно-методическое обеспечение защиты информации средствами криптографических средств защиты. Государственная система защиты информации Российской Федерации в рамках регулирования правил применения технических средств шифрования. Законодательные акты, Постановления Правительства, указы Президента Российской Федерации и иные правовые акты, регулирующие деятельность, связанную с применением, разработкой, внедрением и иных работ со СКЗИ. Государственные. международные стандарты, отраслевые стандарты, руководящие и специальные нормативные документы регулирующие вопросы, вопросы применения СКЗИ в Российской Федерации
- Органы, обеспечивающие криптографическую защиту информации в субъектах Российской Федерации, их задачи и распределение полномочий. Задачи и функции Федеральной службы безопасности.
- Лицензирование деятельности в области криптографической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну. Сертификация средств криптографической защиты информации.

Модуль № 4. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.

- Требования к электронной подписи. Свойства электронной подписи, которыми она должна обладать. Способы организации электронной подписи.
- Электронная подпись на базе RSA. Стандарт электронной подписи на базе DSA. ГОСТ 34.10-94

© Softline 2020

Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма."

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

© Softline 2020

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **17 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперсокого, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла и презентации

© Softline 2020