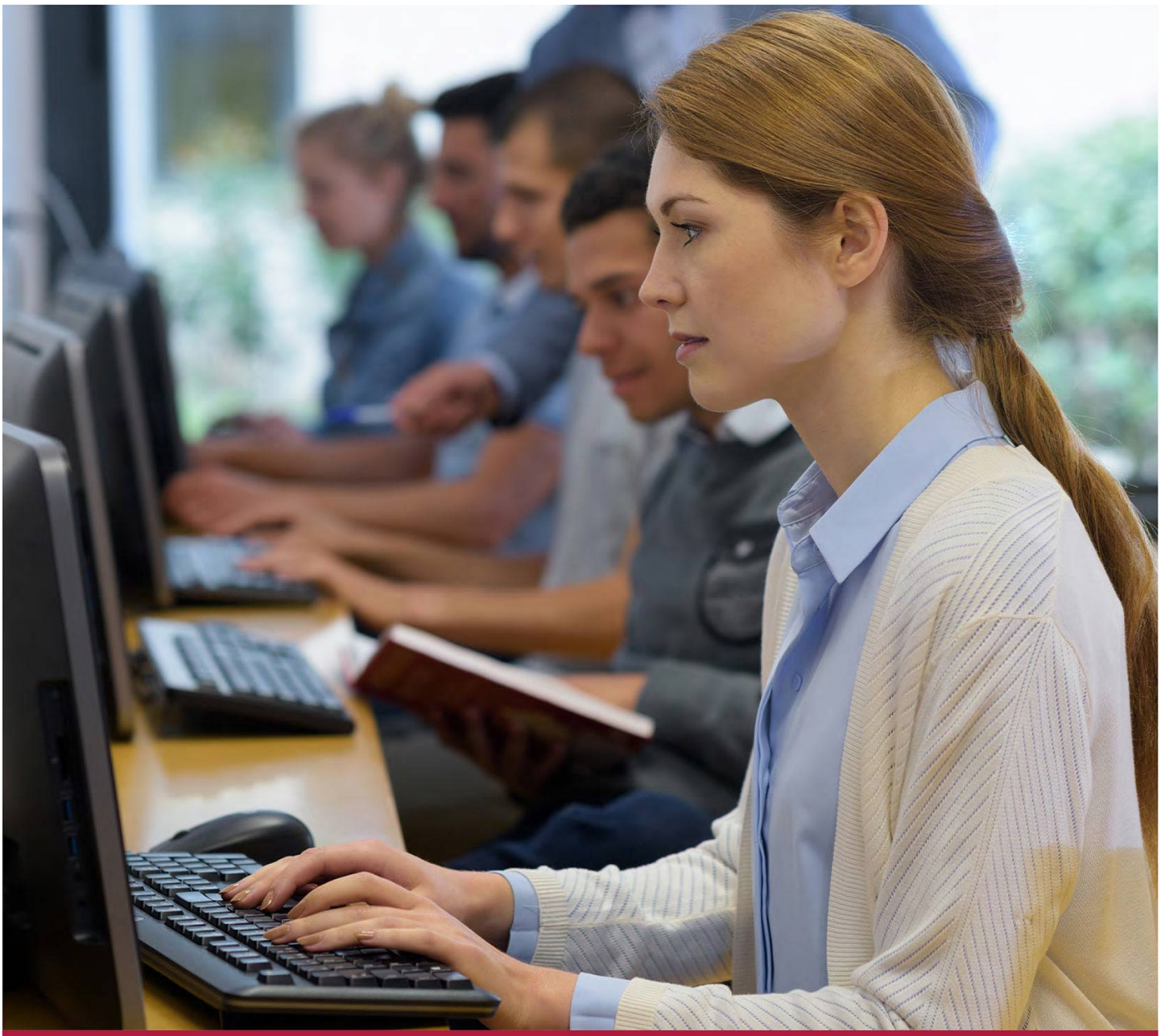
Академия АйТи
a Softline Company



Криптографическая защита информации

Код курса: ИБ011

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Криптографическая защита информации

Код курса: ИБ011

Длительность	104 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Одним из наиболее действенных способов обеспечения конфиденциальности и подлинности информации при ее хранении и передаче по каналам связи, а зачастую и единственным, является применение шифровальных (криптографических) средств (средств криптографической защиты информации). Внедрение и эксплуатация средств криптографической защиты информации требует определенной подготовки, как руководителей организаций, так и специалистов ИТ и информационной безопасности. Более того, в соответствии с пунктом 1 статьи 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) отнесена к лицензируемым видам деятельности. Перечнем федеральных органов исполнительной власти, осуществляющих лицензирование, утвержденным Постановлением Правительства РФ от 21 ноября 2011 г. № 957 определено, что лицензирование выше поименованного вида деятельности осуществляет Федеральная служба безопасности России. При предоставлении государственной услуги по осуществлению лицензирования выше поименованного вида деятельности ФСБ России руководствуется «Положением о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», введенным в действие

Постановлением Правительства РФ от 16 апреля 2012 г. № 313. Учебная программа настоящего курса согласована с уполномоченными должностными лицами ФСБ России и удовлетворяет требованиям Постановления Правительства РФ от 16 апреля 2012 г. № 313, предъявляемым к соискателям лицензии (или лицензиатам), выполняющих работы и оказывающих услуги, перечисленные в пунктах 21-24 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (приложение к «Положению о лицензировании деятельности по....»).

Подробная информация

После изучения курса слушатель будет:

Знать:

- основные положения нормативно-правовых документов по обеспечению информационной безопасности;
- основные положения нормативно-правовых документов по обеспечению юридической значимости электронного документооборота;
- основные требования нормативно-методических документов ФСБ России по организации и обеспечению функционирования шифровальных (криптографических) средств;
- основные положения о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами;
- методы и способы криптографической защиты информации;
- принципы функционирования инфраструктуры открытых ключей;
- рекомендации и основные мероприятия по организации и обеспечению функционирования шифровальных (криптографических) средств;
- основы работы с сертифицированными средствами криптографической защиты информации.

Уметь:

- определять необходимость применения шифровальных (криптографических) средств в системе защиты информации организации (предприятия);
- оценивать и выбирать шифровальные (криптографические) средства, которые могут быть использованы при создании (дооборудовании) и дальнейшей эксплуатации информационных систем;
- определять комплекс мероприятий по организации и обеспечению функционирования шифровальных (криптографических) средств;
- разрабатывать организационно-распорядительные документы, необходимые для эксплуатации шифровальных (криптографических) средств;
- устанавливать, настраивать и эксплуатировать сертифицированные шифровальные (криптографические) средства.

Владеть:

- навыками работы с правовыми базами данных;
- навыками разработки необходимых документов в интересах организации работ по защите информации ограниченного доступа с использованием шифровальных (криптографических) средств;
- навыками применения сертифицированных шифровальных (криптографических) средств.

Успешное окончание обучения по программе данного курса позволит специалистам:

- определять и обосновывать необходимость применения средств криптографической защиты информации;
- аргументированно выбирать средства криптографической защиты информации, удовлетворяющие потребностям организации – обладателя информации;
- правильно организовать эксплуатацию средств криптографической информации;
- самостоятельно разрабатывать требуемую организационно-распорядительную документацию;
- успешно эксплуатировать шифровальные (криптографические) средства;
- повысить свою привлекательность перед работодателем, в т.ч. лицензиатом ФСБ России.

Необходимая подготовка

знать основы информационных технологий;

иметь навыки работы на персональном компьютере в ОС MS Windows XP или выше;

иметь навыки работы в пакете MS Office 2010 или выше.

Цель курса

Формирование знаний и навыков, необходимых для обеспечения информационной безопасности с использованием шифровальных (криптографических) средств в информационных системах.

Программа курса

Модуль 1. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств

Введение. Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности.

Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.

Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств.

Модуль 2. Теоретические основы использования шифровальных (криптографических) средств

Методы и способы криптографической защиты информации.

Инфраструктура открытых ключей (ИОК/PKI).

Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.

Практическая работа: Изучение базовых криптографических операций.

Практическая работа: Изучение основных криптографических алгоритмов.

Модуль 3. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа

Порядок обращения с СКЗИ и криптоключами к ним.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами.

Модуль 4. Практическое применение сертифицированных шифровальных (криптографических) средств

Назначение, состав и порядок применения аппаратных ключей в качестве функциональных ключевых носителей.

Назначение и порядок применения СКЗИ, реализующих базовый функционал по криптографической защите информации ограниченного доступа.

Назначение и порядок применения СКЗИ, используемых для обеспечения безопасности информации ограниченного доступа при передаче по каналам связи.

Назначение и порядок применения СКЗИ для обеспечения защиты информации ограниченного доступа от несанкционированного доступа (НСД) при хранении в информационной системе.

Назначение, состав и порядок применения программно-аппаратных средств автоматизации деятельности Удостоверяющих центров.

Практическая работа: Работа с локальным хранилищем сертификатов в ОС MS Windows.

Практическая работа: Порядок использования функциональных ключевых носителей на примере eToken.

Практическая работа: Практическое применение цифровых сертификатов.

Практическая работа: Установка, настройка СКЗИ «КриптоПро CSP». Работа с контейнерами закрытого ключа и сертификатами пользователя.

Практическая работа: Практическое применение «КриптоПро CSP» и сертификатов для защиты сообщений электронной почты.

Практическая работа: Защита информации при ее хранении в ИС с использованием ПО «Secret Disk 4».

Практическая работа: Защита информации при ее хранении в корпоративной ИС с использованием ПО «Secret Disk Server NG».

Практическая работа: Защита информации при передаче по каналам связи с использованием ПО

«КриптоПро IPSec».

Практическая работа: Установка и настройка ПАК «Удостоверяющий центр КриптоПро УЦ».

Практическая работа: Практическая реализация регламентных процедур с использованием АРМ администратора ЦР.

Практическая работа: Реализация процедур Технического регламента Удостоверяющего центра.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru