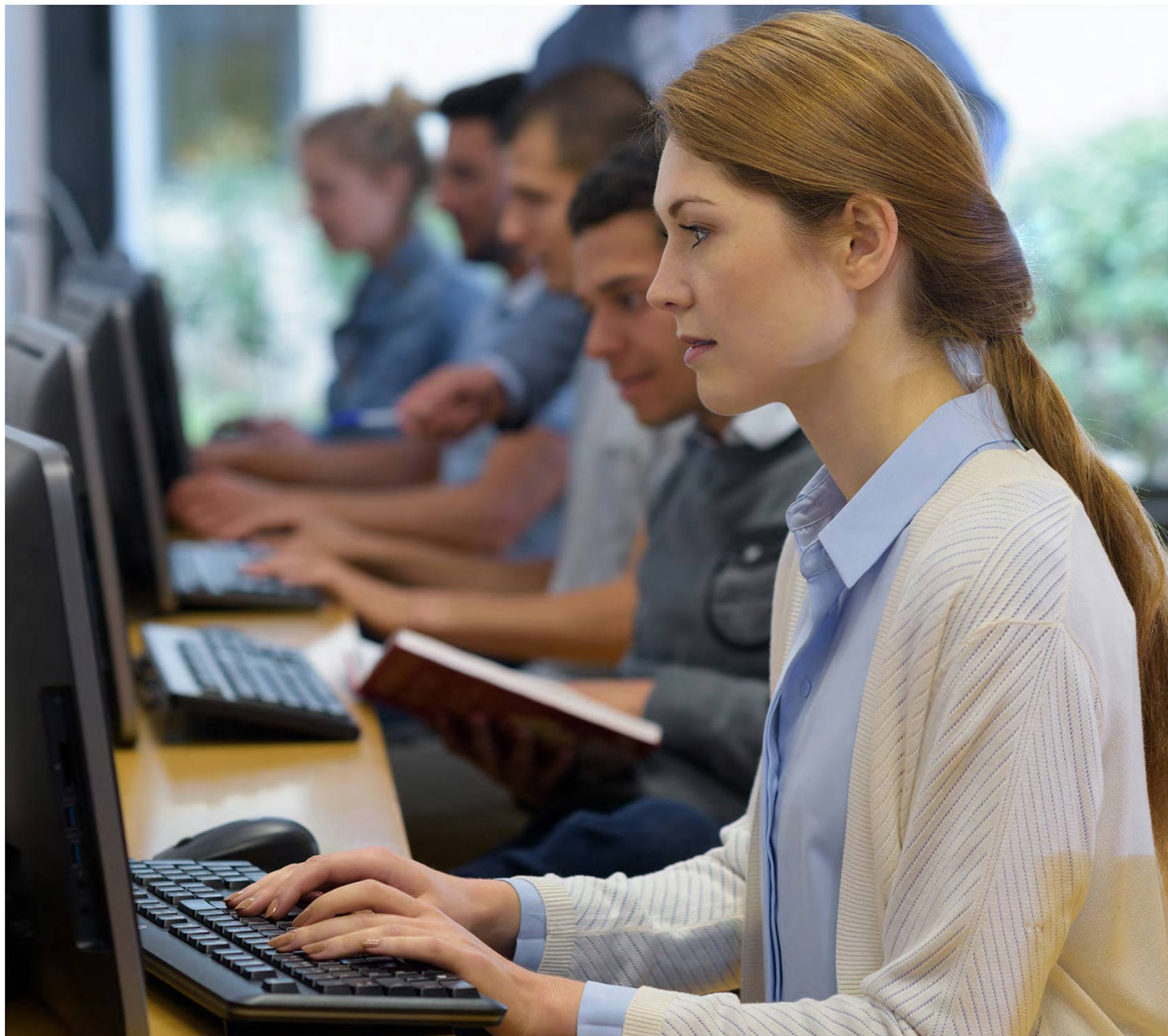




Академия АйТи
a Softline Company



Организация работы органа криптографической защиты

Код курса: СКЗИ

Организация работы органа криптографической защиты

Код курса: СКЗИ

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Внедрение и эксплуатация средств криптографической защиты информации (СКЗИ) требует определенной подготовки, как руководителей организаций, так и специалистов информационной безопасности. И одним из наиболее частых вопросов является «А что должен делать сотрудник, назначаемый руководить работами по вопросам применения СКЗИ, как правильно его назвать, как обучить?». «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», введенная в действие приказом ФАПСИ при Президенте Российской Федерации №152 от 13 июня 2001 г. (агентство упразднено в 2004 г., с передачей функций в части криптографической защиты ФСБ России, далее – Инструкция) указывает, что (статья 6) «для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации организация создает орган криптографической защиты. Органом криптографической защиты может быть организация, структурное подразделение организации - лицензиата ФСБ, обладателя конфиденциальной информации...», а также функции органа криптографической защиты могут быть возложены на физическое лицо. В соответствии со статьей 13 Инструкции, к выполнению обязанностей сотрудников органов криптографической защиты допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ. Предлагаемый курс позволит организации иметь в своем штате подготовленных специалистов и удовлетворить сегодняшние требования ФСБ.

Подробная информация

Профиль аудитории:

- руководители и сотрудники органа криптографической защиты государственных, муниципальных органов и организаций различных правовых форм и форм собственности.

Предварительные требования:

- знать основы информационных технологий;
- иметь навыки работы на персональном компьютере в ОС MS Windows;

- иметь навыки работы в пакете MS Office.

По окончании курса слушатели смогут:

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;

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;

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.

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

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 при хранении в информационной системе.
- Назначение, состав и порядок применения программно-аппаратных средств автоматизации деятельности Удостоверяющих центров.

[Посмотреть расписание курса и записаться на обучение](#)

**Обращайтесь по любым вопросам
к менеджерам Академии АйТи**

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