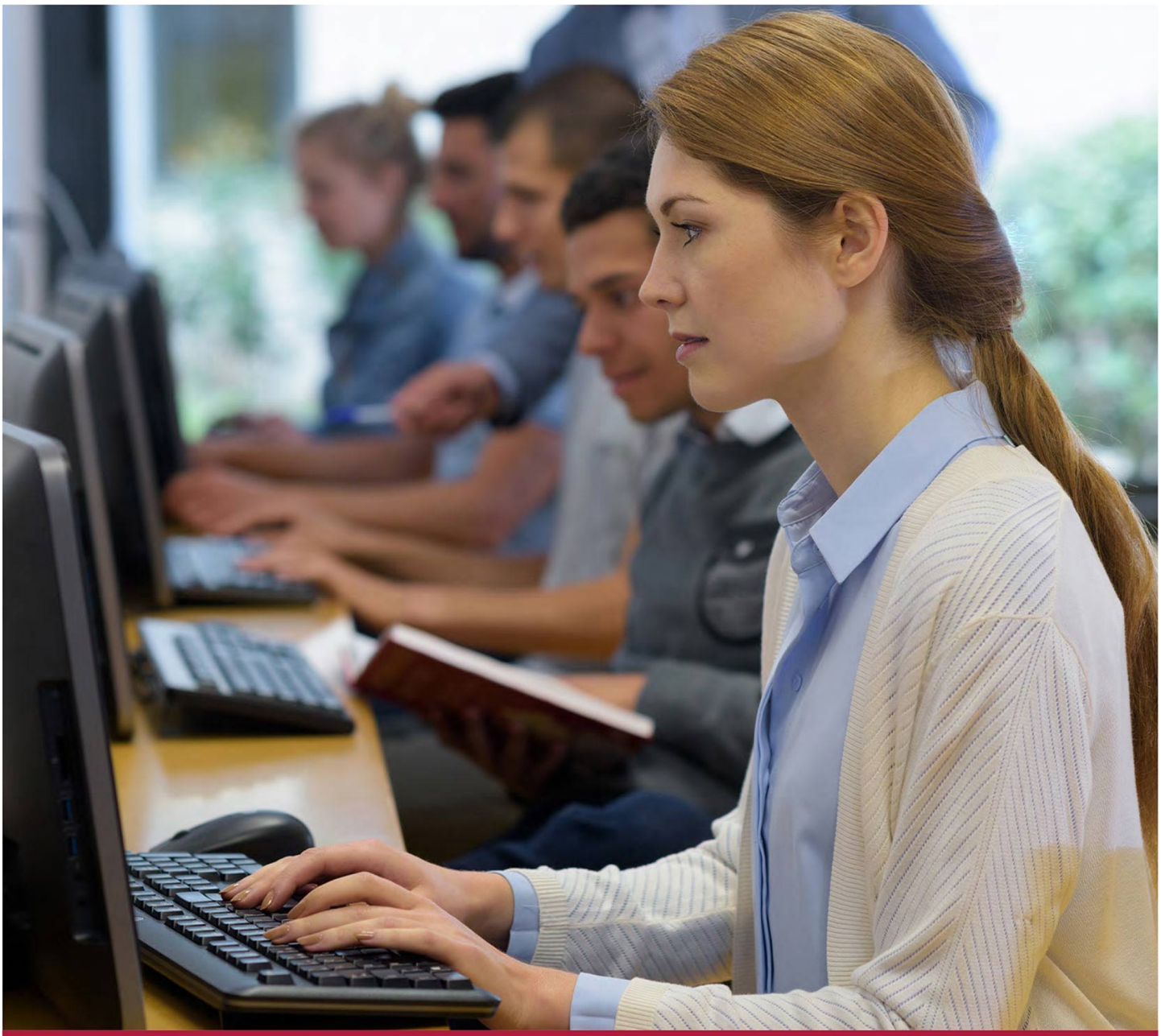
Академия АйТи
a Softline Company



Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и некриптографическими методами

Код курса: ИБ642

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

Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими и некриптографическими методами

Код курса: ИБ642

Длительность	642 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Уникальная программа для специалистов по защите информации Программа позволит освоить полный спектр современных методик и инструментов защиты информации. Она охватывает важнейшие направления от базовой теории некриптографических мер защиты до продвинутых техник криптографии и кибербезопасности. Вы получите глубокие знания и практические навыки в управлении защитой информации, обеспечивающие готовность эффективно решать любые задачи в области защиты конфиденциальных данных и важнейших инфраструктурных объектов. Благодаря программе вы приобретете уникальные компетенции, которые откроют перед вами двери новых карьерных возможностей. Преимущества программы: согласована со ФСТЭК, ФСБ, УМО по ИБ России включает сильный модуль по криптографии с опытными экспертами содержит обучающие блоки от вендоров. По итогам выпускники получат три документа: диплом о переподготовке, сертификаты “Код безопасности” и “КриптоПро” практикоориентированный подход позволит сразу применять полученные знания на практике удобный график позволяет совмещать обучение с основным видом деятельности на видеолекциях у вас будет возможность задать вопросы экспертам в режиме реального времени Программа профессиональной переподготовки разработана на основании: Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»; приказа Министерства науки и высшего образования Российской Федерации от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»; профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 9 августа 2022 г. № 474н; профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 525н; профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 533н; федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427; федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного

приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 № 1455; федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459; федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1458; федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г № 1457. согласована со ФСТЭК РФ, ФСБ и УМО по ИБ России

Подробная информация

Цель: Целью реализации программы профессиональной переподготовки является формирование компетенций, необходимых специалистам для выполнения нового вида профессиональной деятельности «Информационная безопасность» в части защиты конфиденциальной информации.

Профиль аудитории:

- руководители и (или) лица, уполномоченные руководить работами по лицензируемому виду деятельности в области ТЗКИ
- инженерно-технические работники организаций соискателей лицензии и лицензиатов в области ТЗКИ
- индивидуальные предприниматели, являющиеся соискателями лицензии и лицензиатами в области ТЗКИ
- руководители и (или) лица, уполномоченные руководить работами, утвержденными Постановлением Правительства РФ от 16 апреля 2012 г. №313
- инженерно-технические работники, выполняющие работы, утвержденные Постановлением Правительства РФ от 16 апреля 2012 г. 313

Предварительные требования:

- уровень образования лица, поступающего на обучение – высшее образование, подтвержденное документом об образовании

По окончании курса слушатели будут уметь:

- применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ
- разрабатывать необходимые документы в интересах проведения работ по ТЗКИ
- определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий
- формировать требования по ТЗКИ
- определять требования к средствам ТЗКИ на объектах информатизации
- организовывать и проводить работы по ТЗКИ

- организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля
- применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации
- проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний
- разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации
- осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных
- проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации
- устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации
- разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган
- применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области криптографической защиты информации
- применять документы национальной системы стандартизации Российской Федерации в области криптографической защиты информации, государственных стандартов в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям безопасности информации
- определять возможные угрозы безопасности информации и типовые криптоатаки злоумышленников
- формировать требования по криптографической защите информации
- организовывать и проводить работы по криптографической защите информации
- проводить инструктажи и повышать осведомленность сотрудников организации по вопросам применения СКЗИ
- администрировать штатные СКЗИ (средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы)
- выбирать, обосновывать и применять современные информационно-коммуникационные технологии и программные средства, реализующие криптографические методы и алгоритмы для решения задач проектно-технологического и организационно-управленческого типа
- планировать работы по установке, настройке, обслуживанию и проверке работоспособности программных и программно-аппаратных СКЗИ
- применять нормативные документы, регулирующие применение программно-аппаратных средств защиты информации
- обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях
- оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах и компьютерных сетях
- выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях (ПАК «КриптоПро УЦ», АПКШ «Континент»)

- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях (ПАК «КриптоПро УЦ», АПКШ «Континент»)
- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях (ПАК «КриптоПро УЦ», АПКШ «Континент»)
- предоставлять услуги по шифрованию и имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств

Программа курса

Модуль 1 «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

Тема 1. Организационно-правовые основы ТЗКИ

Тема 2. Средства и системы обработки информации

Тема 3. Способы и средства ТЗКИ от утечки по техническим каналам

Тема 4. Меры и средства технической защиты конфиденциальной информации от НСД

Тема 5. Техническая защита конфиденциальной информации от специальных воздействий

Тема 6. Организация защиты конфиденциальной информации на объектах информатизации

Тема 7. Аттестация объектов информатизации по требованиям безопасности информации

Тема 8. Контроль состояния технической защиты конфиденциальной информации

Модуль 2 «Защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, криптографическими средствами»

Тема 1. Введение в дискретную математику

Тема 2. Нормативно-правовые основы защиты информации с использованием СКЗИ в Российской Федерации

Тема 3. Основные понятия криптографии

Тема 4. Криптографические системы с симметричным ключом

Тема 5. Криптографические системы с открытым ключом. Электронная подпись

Тема 6. Хэш-функции. Обеспечение контроля целостности сообщений

Тема 7. Инфраструктура открытых ключей PKI

Тема 8. Криптографические протоколы

Тема 9. Обеспечение безопасности информации с использованием СКЗИ

Итоговая аттестация.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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