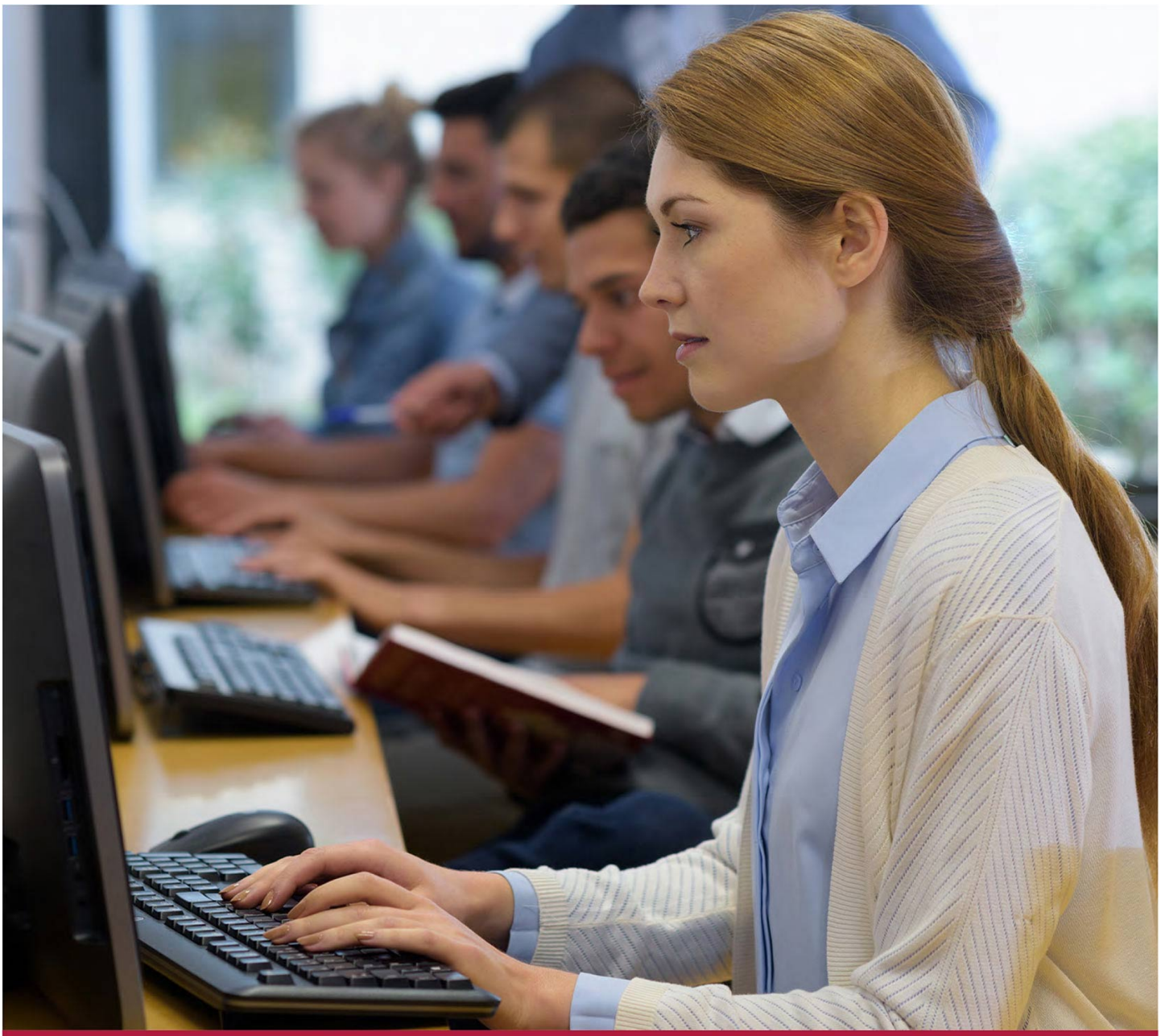
softline учебный центр



Защита информации криптографическими методами

Код курса: SLIT-1032

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

Защита информации криптографическими методами

Код курса: SLIT-1032

Длительность	12 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Секреты и особенности самого востребованного направления информационной безопасности с учетом актуальных нововведений в законодательстве. В данном курсе проводится детальный разбор технологий и методов криптографической защиты информации (электронная подпись, шифрование, хеширование блокчейн и т.д.), а также предоставляется практическое руководство по организации работы с усиленной электронной подписью, машиночитаемыми доверенностями, порядку защиты веб-ресурсов с использованием TLS и другим вопросам. Программа ориентирована на специалистов коммерческих организаций и государственных структур, ответственных за защиту информации и применение электронной подписи, а также на специалистов и экспертов по другим направлениям ИТ и ИБ. В процессе обучения слушателям предоставляется информация с учетом актуальных целей и задач цифровой трансформации. По результату прохождения курса слушатели смогут самостоятельно определять необходимость и порядок использования средств криптографической защиты информации, эффективно выстраивать работу по использованию усиленной электронной подписи: от организации получения квалифицированных сертификатов в ведомственных удостоверяющих центрах (ФНС, Казначейство) до обеспечения комплексной проверки электронной подписи в информационных системах.

Подробная информация

Профиль аудитории:

- специалисты по информационной безопасности;

- сотрудники, ответственные за организацию работы с электронной подписью;

- специалисты по информационным технологиям, ответственные за организацию электронного документооборота, создание информационных систем.

Предварительные требования:

Среднее или высшее образование

По окончании курса слушатели смогут:

- определять необходимость и условия применения средств криптографической защиты информации (проведение классификации, определение типа и характеристик криптографических средств);

- выстраивать работу по получению сертификатов усиленной квалифицированной электронной подписи в удостоверяющих центрах и их использованию в соответствии с нововведениями законодательства;

- обеспечивать корректность создания и проверки электронной подписи электронных документов, документов о полномочиях в информационных системах;

- организовывать мероприятия по эксплуатации средств криптографической защиты информации в соответствии с требованиями регуляторов

- применять в работе практические советы по эффективному использованию мер криптографической защиты информации

Программа курса

Модуль 1. Как работает криптография и почему её нельзя заменить

1. Роль и место криптографии в современном ИТ и цифровой трансформации
2. Классификация криптографических алгоритмов
3. Нормативное регулирование использования криптографии и электронной подписи (обзор и ориентация в законах и ведомственных документах)
4. Определение практических сценариев и задач применения криптографии
5. Инфраструктура использования электронной подписи и криптографии в России (инструменты, регуляторы, участники взаимодействия)
6. Зарубежная криптография (где и когда используется)

Модуль 2. Практическое применение криптографических инструментов

1. Перечень задач, требующих применение криптографии
2. Обзор криптографических технологий (VPN, блокчейн, хеширование, шифрование), сравнительная характеристика, критерии выбора)
3. Электронная подпись (получение и использование ключей, организация взаимодействия в ведомственными удостоверяющими центрами (ФНС, Федеральное казначейство)
4. Электронные доверенности (порядок создания, хранения, проверки)
5. TLS шифрование, TLS ГОСТ шифрование (виды алгоритмов, особенности и порядок использования, настройки и выявления уязвимостей)
6. Моделирование угроз безопасности и типа нарушителя, классификация криптографических средств
7. Организация учета криптографических средств

Модуль 3. Углубленное изучение технологии усиленной электронной подписи

1. Организация инфраструктуры создания и проверки электронной подписи (особенности встраивания функционала электронной подписи в информационные системы)
2. Сервисы создания электронной подписи (облачная, мобильная электронная подпись,

встраивание средства электронной подписи и т.д.)
3. Сервисы проверки электронной подписи (системы централизованной проверки, доверенная третья сторона)
4. Форматы электронной подписи длительного хранения (электронные архивы, штампы времени, метки статуса действительности сертификатов)
5. Актуальные тренды развития криптографии и электронной подписи (квантовая, постквантовая криптография, актуальные проекты органов власти и т.д.)
6. Результирующий обзор полученных знаний и ориентация в поиске полезной информации

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!

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 **18 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 Касперского, 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.