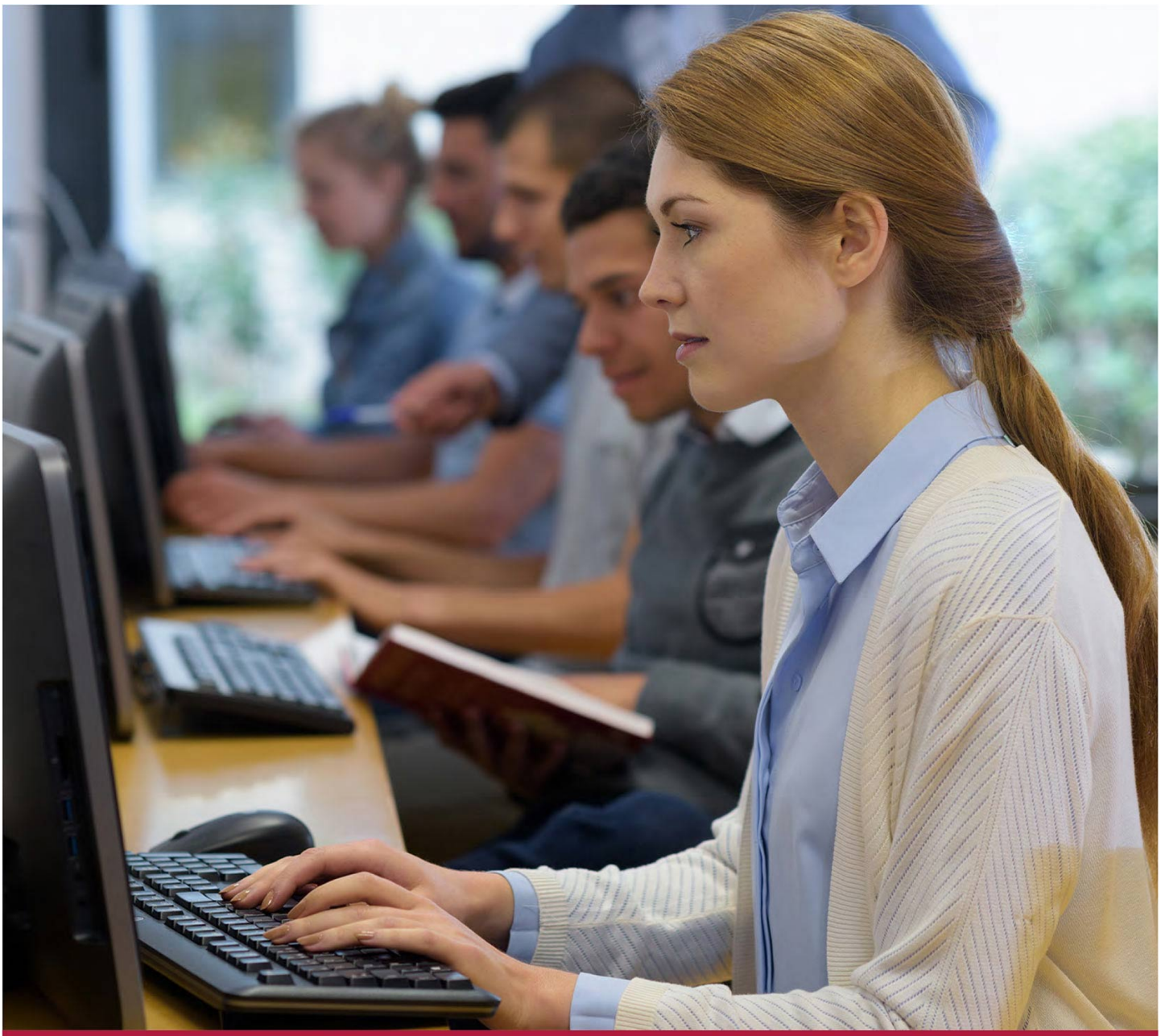
softline учебный центр



Система управления информационной безопасностью

Код курса: СУИБ

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

Система управления информационной безопасностью

Код курса: СУИБ

Длительность	40 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Система управления информационной безопасностью.

Подробная информация

Профиль аудитории:

- Руководители и специалисты в области защиты информации.

Предварительные требования:

- Базовые знания об эксплуатации средств вычислительной техники;
- Навыки работы с прикладным программным обеспечением;
- Умение работать с источниками информации.

По окончании курса слушатели смогут:

Уметь:

- Использовать рисковую методологию управления защитой информации в автоматизированной системе;
- Разрабатывать модели угроз безопасности информации в организации;
- Разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;
- Определять степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер взаимодействия работников между собой;
- Классифицировать информационные активы предприятия/организации;
- Оценивать и классифицировать угрозы безопасности;
- Выбирать модель управления рисками в соответствии с технико-экономическими особенностями функционирования информационных систем;
- Формировать перечень мероприятий по предотвращению угроз безопасности данным, обрабатываемым в информационных системах;
- Разрабатывать проекты внутренних нормативных актов, регламентирующих действия по

защите информации ограниченного доступа;
- Реализовывать меры по предотвращению и расследованию инцидентов информационной безопасности;

Знать:

- Терминологию в области информационной безопасности
- Требования законодательства в сфере информационной безопасности;
- Основные угрозы сетевой безопасности;
- Основные требования к информационной безопасности в организации;
- Методы защиты информации от утечки по техническим каналам;
- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- Организационные меры по защите информации;
- Последствия от нарушения свойств безопасности информации.

Программа курса

Модуль 1. Стандарты в области управления информационной безопасностью.

- Основы информационной безопасности
- BS 7799 -1 «Практические правила управления информационной безопасностью».
- BS 7799 -2 «СУИБ. Спецификация и руководство по применению».
- ISO 27001, ISO 27002, ISO 27005
- Взаимосвязь организационных стандартов
- Как устанавливать требования защиты
- Критические факторы успеха

Модуль 2. Корпоративные архитектуры

- Пирамида корпоративной архитектуры и ее компоненты
- Пошаговое расширение модели деятельности в стандартах ISO

Модуль 3. Идентификация активов

- Номенклатура и типология документов компании
- Главный актив – информация
- Характеристики и идентификация активов

Модуль 4. Описание бизнес-процессов

- Ключевые понятия
- Пошаговое моделирование бизнес-процессов
- Декомпозиция. Вложенные бизнес-процессы и алгоритмы
- Реестр информационных активов

Модуль 5. Идентификация требований безопасности

- Категории требований безопасности.

- Реестр требований безопасности:
  - Законодательные требования
  - Нормативные требования
  - Контрактные обязательства
  - Требования бизнеса

Модуль 6. Определение ценности активов

- Типовая последовательность определения ценности активов
- Структурирование активов по диапазонам ценности
- Критерии оценки ущерба
- Оценки прямого финансового ущерба
- Таблица ценности активов

Модуль 7. Анализ угроз и уязвимостей

- Зачем нужно моделирование угроз?
- Анализ угроз и уязвимостей:
  - Физические угрозы
  - Нецелевое использование оборудования и сети Интернет сотрудниками
  - Угрозы утечки конфиденциальной информации
  - Угрозы утечки информации по техническим каналам
  - Угрозы несанкционированного доступа
  - Угрозы недоступности ИТ сервисов и разрушения (утраты) информационных активов
  - Угрозы нарушения целостности и несанкционированной модификации данных
  - Угрозы антропогенных и природных катастроф
  - Юридические угрозы

Модуль 8. Профиль и жизненный цикл угрозы. Классификация угроз безопасности.

- Структура угроз
- Понятие профиля и жизненного цикла угрозы
- Описание угроз безопасности
- Способы и принципы классификации угроз
- Примеры декомпозиции / классификации
- Каталоги угроз и контрмер

Модуль 9. Угрозы утечки информации по техническим каналам.

- ТКУИ (технический канал утечки информации), приводящие к возникновению угроз безопасности
- Общая классификация ТКУИ

Модуль 10. Угрозы несанкционированного доступа к информации и характеристика угроз непосредственного доступа в операционную среду

- Способы реализации угроз НСД
- Угрозы непосредственного доступа
- Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия

- Сетевые угрозы, уязвимости и атаки, связанные с эксплуатацией межсетевых экранов
- Возможные последствия реализации угроз
- Этапы реализации угрозы НСД

Модуль 11. Характеристика угроз программно-математических воздействий и нетрадиционных информационных каналов

- Виды вредоносных программ
- Классификация угроз
- Классификация программных вирусов и сетевых червей.
- Пути проникновения

Модуль 12. Нетрадиционные каналы доступа к информации

- Методы формирования нетрадиционных каналов
- Стеганография
- Метод наименее значащих битов
- Общая характеристика результатов утечки информации и НСД

Модуль 13. Уязвимости информационной безопасности

- Уязвимости представляют собой слабости защиты
- Организационные уязвимости
- Источники идентификации потенциальных организационных уязвимостей
- Анализ данных организационных уязвимостей
- Целесообразность использования механизмов контроля
- Оценочная таблица механизмов контроля
- Отчет о несоответствиях

Модуль 14. Оценка угроз и уязвимостей

- Оценка вероятности реализации угроз
- Оценка уровня уязвимостей
- Результаты оценки угроз и уязвимостей
- Опросные листы для оценки угроз

Модуль 15. Определение величины риска и обработка рисков информационной безопасности

- Реестр информационных рисков
- Качественная и количественная оценка риска
- Отчет об оценке рисков
- Процесс обработки рисков
- Способы обработки риска
- Критерии принятия рисков
- Уменьшение риска
- Передача риска
- Избежание риска

Модуль 16. Оценка возврата инвестиций в информационную безопасность и принятие решения по обработке риска. Декларация о применимости механизмов контроля

- Коэффициент возврата инвестиций (ROI)
- Примеры расчета коэффициент возврата инвестиций (ROI)
- «Калькуляторы» рисков
- Принятие решения по обработке риска
- Форма представления руководству организации информации
- План обработки рисков
- Приоритетные меры по обработке рисков
- Декларация о применимости
- Документирование СУИР
- Начальные условия для внедрения СУИР
- Организационная структура управления рисками
- Обучение членов экспертной группы
- Реализация пилотного проекта по оценке рисков
- Жизненный цикл управления рисками

Модуль 17. Аудит информационной безопасности.

- Основы аудита информационной безопасности, состав и роли участников
- Основные этапы проведения аудита ИБ

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.