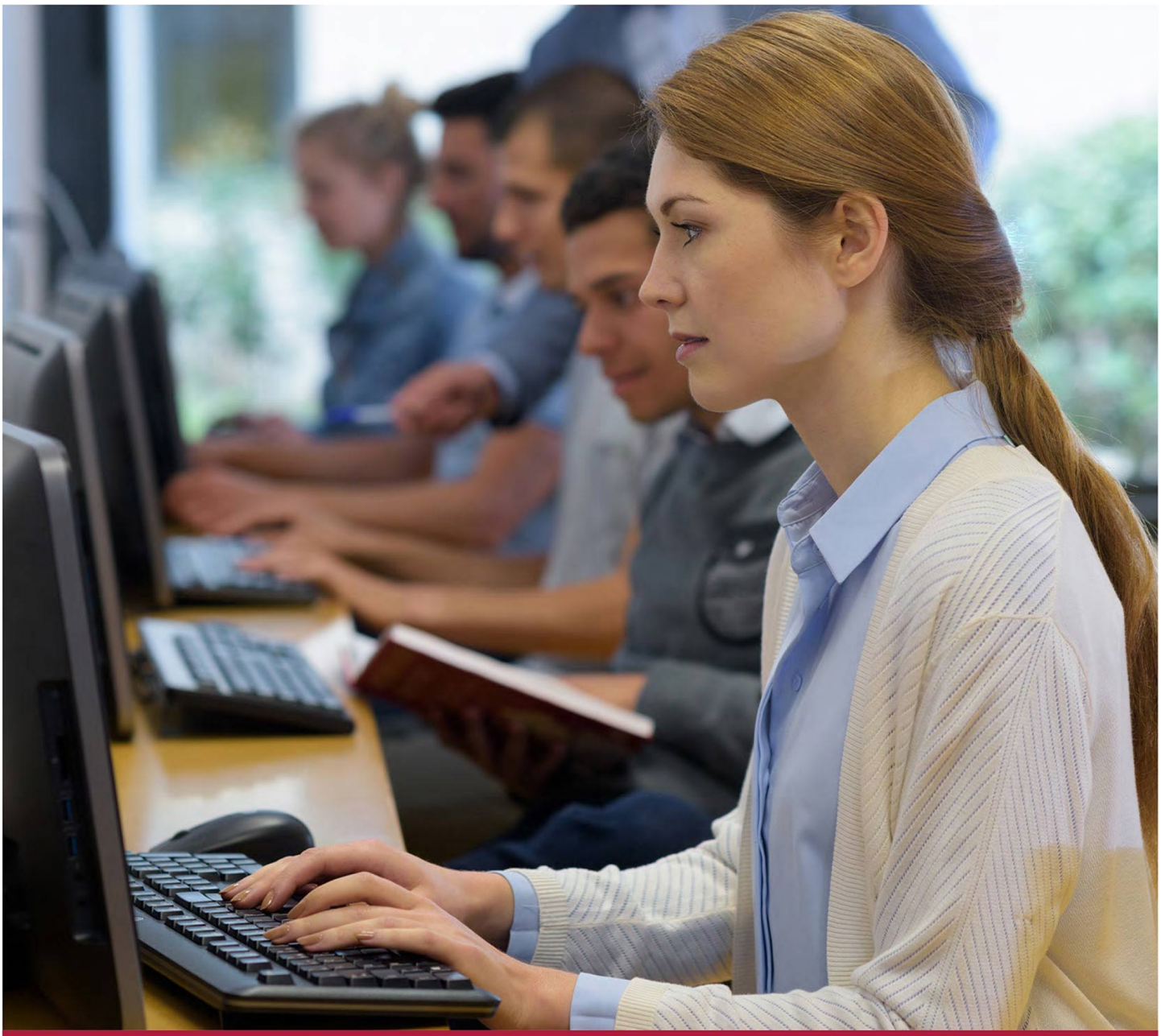
softline учебный центр



Обеспечение безопасности значимых объектов КИИ и АСУТП

Код курса: SLBT-087

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

Обеспечение безопасности значимых объектов КИИ и АСУТП

Код курса: SLBT-087

Длительность	24 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

После принятия Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 27 июля 2017, организациям, ведущим деятельность на территории РФ, стало необходимым привести свои системы защиты информации в соответствие новым требованиям. Трёхдневная программа повышения квалификации «Обеспечение безопасности значимых объектов КИИ и АСУТП» предназначена для подготовки руководителей и специалистов по обеспечению защиты информации в автоматизированных системах управления, информационных системах и информационно-телекоммуникационных сетях в процессе их проектирования и эксплуатации: начальников и специалистов отделов по защите информации, руководителей и специалистов отделов ИТ, АСУ и ИБ, начальников секторов АСУПТ, инженеров по автоматизированным системам управления, инженеров по внедрению АСУТП, начальников служб системной интеграции, начальников отделов информационно-коммуникационных технологий. Результаты обучения: возможность самостоятельно провести категорирование объектов КИИ; подготовить необходимые документы для надзорных органов; выполнить в срок требования законодательства. Курс включает в себя теоретическую и практическую часть и доступен к прослушиванию онлайн и в классах Учебного центра Softline в городах России (Москве, Санкт-Петербурге, Екатеринбурге, Казани, Красноярске, Нижнем Новгороде, Новосибирске, Омске, Ростове-на-Дону и Хабаровске). По окончании обучения выдаётся удостоверение о повышении квалификации и сертификат Учебного центра Softline.

Подробная информация

Профиль аудитории:

- Руководители и специалисты по обеспечению защиты информации в автоматизированных системах управления, информационных системах и информационно-телекоммуникационных сетях в процессе их проектирования и эксплуатации.

Предварительные требования:

- Высшее или среднее техническое образование;
- Опыт работы в сфере обеспечения технической защиты информации не менее 1 года;
- Базовые знания общей правовой и нормативной базы в области обеспечения безопасности;

- Знание принципов и правил криптографической защиты информации.

По окончании курса слушатели смогут:

Уметь:

- Контролировать безотказное функционирование технических средств защиты информации;
- Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты;
- Исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем;
- Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности;
- Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем;

Знать:

- Принципы построения и функционирования систем и сетей передачи информации;
- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
- Основные меры по защите информации в автоматизированных системах;
- Технические средства контроля эффективности мер защиты информации;
- Нормативные правовые акты в области защиты информации;
- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- Национальные, межгосударственные и международные стандарты в области защиты информации;
- Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем.

Программа курса

Модуль 1. «Введение в тему КИИ. Термины и определения. Основная проблематика».

- Введение в тематику защиты значимых объектов критической информационной инфраструктуры.
- Рекомендуемые к использованию в отрасли термины и определения. Понятие критической информационной инфраструктуры.
- Обсуждение актуальности тематики устойчивости функционирования объектов КИИ (ИС, ИТС, АСУ), относительно компьютерных атак.

Модуль 2. «Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры».

- Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Описание документов, которыми следует

руководствоваться при обеспечении безопасности объектов КИИ.
- Принципы обеспечения безопасности критической информационной инфраструктуры. Система безопасности значимого объекта КИИ.
- Оценка безопасности критической информационной инфраструктуры.
- Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Модуль 3. «Классификация АСУТП: требования, параметры, сроки. Категорирование объектов критической информационной инфраструктуры».

- Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.
- Оценка последствий возможных аварий. Паспорт безопасности опасного производственного объекта. Декларация промышленной безопасности.
- Показатели критериев значимости объектов КИИ РФ и их значения. Сведения об объекте критической информационной инфраструктуры. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры.
- Возможные последствия в случае возникновения компьютерных инцидентов.
- Организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры.

Модуль 4. «Права и обязанности субъектов критической информационной инфраструктуры.

- Обязанности и права субъектов КИИ. Надзорная деятельность.
- Изменения в уголовном кодексе РФ и перечне сведений, составляющих гос. тайну.

Модуль 5. «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры».

- Организация общего порядка обеспечения безопасности значимых объектов КИИ.
- Установка требований к силам обеспечения безопасности значимых объектов КИИ.
- Обсуждение требований к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, требований к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов, требований по обеспечению безопасности значимых объектов КИИ РФ.

Модуль 6. «Разработка организационных и технических мер (рекомендации и требования ФСТЭК и ФСБ)».

- Безопасность значимых объектов обеспечивается в соответствии со статьей 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение (при ее наличии).
- Проектирование подсистемы безопасности значимого объекта.
- Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).

Модуль 7. «Разработка модели угроз».

- Классификация уязвимостей информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей ИС. Общие требования к структуре описания уязвимости. Методика оценки уязвимостей.
- Причины возникновения угроз безопасности информации.
- Основные признаки классификации угроз безопасности информации. Систематический подход к определению угроз.

Модуль 8. «Выбор мер защиты объекта информатизации».

- Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора конкретных средств защиты информации для реализации организационных и технических мер.

Модуль 9. «Формирование технического проекта. Разработка эксплуатационной документации».

- Разработка АСУТП в целом, в том числе технического проекта, должна соответствовать общим требованиям, установленным ГОСТ 24.104 (АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ. Общие требования), а также требованиям, содержащимся в техническом задании на ее создание ГОСТ 34.602 (Техническое задание на создание автоматизированной системы). Последовательность стадий и этапов работ, связанных с определением целесообразности создания и собственно созданием АСУТП, определена в ГОСТ 34.601 (Автоматизированные системы стадии создания).
- Функционирование систем безопасности в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов критической информационной инфраструктуры, разрабатываемыми субъектами критической информационной инфраструктуры.
- ОРД по безопасности значимых объектов. Определяющие порядок и правила обеспечения безопасности значимых объектов КИИ.
- ОРД по безопасности значимых объектов. Определяющие порядок и правила функционирования системы безопасности значимых объектов (СБЗО) критической информационной инфраструктуры (КИИ).

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.