SLBT-087

Обеспечение безопасности значимых объектов КИИ и АСУТП

Содержание

Краткая информация

Длительность:	3 дня (24 ак.ч.)
Категория слушателей	руководители служб и подразделений в сфере информационно-коммуникационных технологий, руководители отделов систем защиты информации, специалисты по защите информации
Форма обучения:	очная или дистанционная

Обзор:

Настоящая программа 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.

Цель обучения:

Программа направлена на:

- формирование и развитие компетенций в области защиты объектов критической информационной инфраструктуры;
- знакомство с правовым регулированием отношений в области обеспечения безопасности КИИ;
- получение навыков анализа структурно-функциональных характеристик ИС, ИТС, АСУ, категорирования объектов КИИ;
- получение навыков работы с подзаконными актами, методическими рекомендациями регулирующих органов;
- формирование навыков разработки организационных и технических мер по обеспечению безопасности значимого объекта;
- получение опыта формирования моделей угроз и выбора мер защиты объекта информатизации.

Планируемые результаты обучения:

В результате освоения программы обучающийся должен:

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.

Содержание обучения:

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

- введение в тему;
- термины и определения;
- основная проблематика;
- устойчивость функционирования объектов КИИ относительно компьютерных атак.

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

- верхнеуровневые концептуальные документы, федеральное законодательство, подзаконные нормативные акты, методические документы, проекты документов ФСТЭК России;
- безопасность критической информационной инфраструктуры РФ;
- утверждение правил категорирования объектов критической информационной инфраструктуры;
- освоение правил категорирования объектов критической информационной инфраструктуры.

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

- утверждение правил категорирования объектов критической информационной инфраструктуры;
- классификация АСУ ТП по Приказу ФСТЭК России №31;
- категорирование объектов критической информационной инфраструктуры;
- разработка формы направления сведений о результатах категорирования;
- использование правил категорирования для выбранной ИС, ИТС, АСУ, заполнение акта категорирования.

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

- обязанности и права субъектов КИИ;
- сопутствующие изменения в законодательстве после принятия 187 ФЗ.

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

- общий порядок организации обеспечения безопасности значимых объектов КИИ;
- требования к силам обеспечения безопасности значимых объектов КИИ;
- требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;
- требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов.

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

- 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»:

- уязвимости информационных систем. Классификация уязвимостей информационных систем;
- информационные системы и объекты информатизации. Угрозы безопасности информации;
- модель угроз;
- создание модели угроз для выбранной ИС, ИТС или АСУ.

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 АСУ ТП в целом с соблюдением последовательности стадий и этапов работ, определенных ГОСТом.

Предварительные требования:

к освоению программы допускаются лица, имеющие:

- 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.