САНКТ-ПЕТЕРБУРГСКАЯ АКАДЕМИЯ БЕЗОПАСНОСТИ

АНО ДПО «Санкт-Петербургская академия безопасности»
194044, г. Санкт-Петербург, Лесной пр., д. 20, корп. 15
Тел.: (812) 603-28-74 e-mail: info@nsab.ru, http://www.nsab.ru/

Программа повышения квалификации

«Основные аспекты обеспечения безопасности критической информационной инфраструктуры»

Продолжительность: 5 дней (72 академических часа, из них 40 часов – аудиторные занятия, 32 часа – самостоятельная подготовка по выданным учебным материалам).

Категории слушателей - руководители и специалисты различных категорий, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры.

Содержание программы

Тема 1. Основы обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ)

1. Правовые основы обеспечения безопасности КИИ Российской Федерации (3 ак. часа).

1.1. Нормативно-правовые акты и методические документы в области безопасности КИИ.
1.2. Права и обязанности субъектов КИИ.
1.3. Государственный контроль в области обеспечения безопасности значимых объектов КИИ.
1.4. Документы в области технического регулирования и стандартизации.
1.5. Ответственность за нарушение мер, правил и требований по обеспечению безопасности КИИ.

2. Угрозы безопасности информации, обрабатываемой на объектах КИИ (3 ак. часа).

2.1. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ.
2.2. Модель угроз безопасности информации значимого объекта КИИ.
2.3. Модель нарушителя безопасности КИИ.

3. Методика определения актуальных угроз безопасности КИИ (2 ак. часа).

3.1. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.
3.2. Методы определения возможных способов реализации угроз безопасности информации и последствий от их реализации.
3.3. Разработка модели угроз безопасности информации значимого объекта КИИ.

Тема 2. Организация работ по обеспечению безопасности значимого объекта КИИ

4. Категорирование объектов КИИ (3 ак. часа).

4.1. Правила и порядок категорирования объектов КИИ (ПП РФ от 08.02.2018 №127).
4.2. Порядок определения объектов, подлежащих категорированию.
4.3. Порядок определения значимости объектов КИИ.

5. Разработка документов в рамках категорирования объектов КИИ (1 ак. час).

5.1. Формирование акта комиссии по категорированию значимого объекта КИИ (ПП от 08.02.2018 № 127).
5.2. Подготовка сведений о результатах категорирования значимого объекта КИИ для направления в ФСТЭК России (Приказ ФСТЭК от 22.12.2017 № 236).

6. **Требования по обеспечению безопасности значимых объектов КИИ (3 ак. часа).**

6.1. Система безопасности значимого объекта КИИ (Приказ ФСТЭК от 21.12.2017 № 235).

6.2. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.

6.3. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ.

7. **Стадии (этапы) работ по созданию систем безопасности (4 ак. часа).**

7.1. Обеспечение безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов КИИ в соответствии с Приказом ФСТЭК от 25.12.2017 № 239.

7.2. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.

8. **Разработка технического задания (разделов ТЗ) на создание системы безопасности значимого объекта КИИ (1 ак. час)**

8.1. Основные разделы ТЗ.

8.2. Практикум по заполнению ТЗ.

9. **Правовая основа создания и функционирования ГосСОПКА, структура, субъекты взаимоотношений (4 ак. часа).**

9.1. Структура ГосСОПКА и субъекты взаимоотношений.

9.2. Нормативная документация, регламентирующая сферу ГосСОПКА.

9.3. Требования к субъектам ГосСОПКА.

9.4. Порядок создания ведомственных и корпоративных центров ГосСОПКА.

9.5. Порядок взаимодействия с НКЦКИ.

Тема 3. Основные средства, предназначенные для обнаружения, предупреждения, ликвидации компьютерных атак и реагирования на компьютерные инциденты

10. **Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ (8 ак. часов).**

10.1. Анализ угроз программно-математических воздействий.

10.2. Виды систем обнаружения вторжений.

10.3. Демонстрация возможностей средств, предназначенных для обнаружения, предупреждения и ликвидации компьютерных атак.

10.4. Обзор основных средств защиты, необходимых для выполнения требований по обеспечению безопасности значимых объектов КИИ.

11. **Порядок приемки системы защиты информации (2 ак. часа).**

11.1. Разработка программы и методик испытаний СЗИ на соответствие требованиям по безопасности

11.2. Приемочные испытания значимого объекта КИИ и его системы безопасности.

Тема 4. Контроль за обеспечением безопасности значимого объекта КИИ

12. **Контроль за обеспечением безопасности значимого объекта КИИ (3 ак. часа).**

12.1. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

12.2. Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ.

13. **Документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ (1 ак. час).**
    13.1. Состав комплекта документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.
    13.2. Разработка документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

14. **Итоговая аттестация (2 ак. часа).**

При успешном прохождении итоговой аттестации по данной программе слушателям выдается **Удостоверение о повышении квалификации.**