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

Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

Продолжительность: 10 дней (108 академических часов, из них 72 часа – аудиторные занятия, 36 часов – самостоятельная подготовка по выданным учебным материалам).

Категории слушателей:

– руководители и специалисты различных категорий, ответственные за обеспечение безопасности значимых объектов КИИ.

Программа повышения квалификации разработана в соответствии с:

- Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденными ФСТЭК России 16 апреля 2018 года;
- примерной программой повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, утвержденной заместителем директора ФСТЭК России 30 ноября 2018 года.

Программа повышения квалификации согласована ФСТЭК России.

Содержание программы

Тема 1. Основы обеспечения безопасности значимых объектов критической информационной инфраструктуры

1. Правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации (4 ак. ч.).

1.1. Нормативно-правовые акты и методические документы в области безопасности критической информационной инфраструктуры (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.
1.6. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ Российской Федерации (семинар).

2. Угрозы безопасности информации, обрабатываемой на объектах КИИ (8 ак. ч.).

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.
2.4. Определение актуальных угроз безопасности информации **(семинар).**
2.5. Порядок угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.
2.6. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации **(практическое занятие).**
2.7. Порядок разработки модели угроз безопасности информации значимого объекта КИИ.
2.8. Разработка модели угроз безопасности информации значимого объекта КИИ **(практическое занятие).**

Тема 2. Организация работ по обеспечению безопасности значимого объекта КИИ

3. Категорирование объектов КИИ (6 ак. ч.).

3.1. Правила и порядок категорирования объектов КИИ (ПП РФ от 08.02.2018 №127).
3.2. Порядок определения объектов, подлежащих категорированию.
3.3. Порядок определения значимости объектов КИИ.
3.4. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности **(практическое занятие).**
3.5. Определение значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов **(практическое занятие).**
3.6. Формирование акта комиссии по категорированию значимого объекта КИИ **(практ. занятие).**
3.7. Подготовка сведений о результатах категорирования значимого объекта КИИ **(практ. занятие).**

4. Требования по обеспечению безопасности значимых объектов КИИ (8 ак. ч.).

4.1. Установление требований по обеспечению безопасности значимого объекта КИИ.
4.2. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.
4.3. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности значимого объекта КИИ.
4.4. Организационные и технические меры, для обеспечения безопасности значимых объектов КИИ **(семинар).**
4.5. Способы и средства защиты информации **(семинар).**
4.6. Разработка плана мероприятий по обеспечению безопасности значимого объекта КИИ **(практическое занятие).**
4.7. Разработка правил и порядка реализации отдельных мер по обеспечению безопасности значимых объектов КИИ **(практическое занятие).**
4.8. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ **(практическое занятие).**
4.9. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ **(практическое занятие).**
4.10. Разработка программы и методик испытаний средств защиты информации на соответствие требованиям по безопасности **(практическое занятие).**

5. Система безопасности значимого объекта КИИ (4 ак. ч.).

5.1. Цели и задачи системы безопасности значимого объекта КИИ.
5.2. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования.
5.3. Требования к силам обеспечения безопасности значимых объектов КИИ.
5.4. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ.
5.5. Структура системы безопасности значимого объекта КИИ.
5.6. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования.
5.7. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации **(семинар).**
5.8. Обеспечение функционирования системы безопасности значимого объекта КИИ **(семинар)**.

6. Стадии (этапы) работ по созданию систем безопасности (8 ак. ч.).

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

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

6.3. Организационно-распорядительные и эксплуатационные документы, разрабатываемые на значимый объект КИИ и его систему безопасности **(семинар) (1 ак. ч.).**

6.4. Разработка технического задания (разделов технического задания) на создание системы безопасности значимого объекта КИИ **(практическое занятие) (1 ак. ч.).**

6.5. Разработка эксплуатационной, организационно-распорядительной документации на значимый объект КИИ и его систему безопасности **(практическое занятие) (1 ак. ч.).**

6.6. Приемочные испытания значимого объекта КИИ и его системы безопасности **(практическое занятие) (1 ак. ч.).**

7. Правовая основа создания и функционирования ГосСОПКА, структура, субъекты взаимоотношений (4 ак. ч.).

7.1. Структура ГосСОПКА и субъекты взаимоотношений.

7.2. Нормативная документация, регламентирующая сферу ГосСОПКА.

7.3. Требования к субъектам ГосСОПКА.

7.4. Порядок создания ведомственных и корпоративных центров ГосСОПКА.

7.5. Порядок взаимодействия с НКЦКИ.

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

8. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ (16 ак. ч.).

8.1. Анализ угроз программно-математических воздействий (2 ак.ч).

8.2. Виды систем обнаружения вторжений (2 ак.ч.).

8.3. Демонстрация возможностей средств, предназначенных для обнаружения, предупреждения и ликвидации компьютерных атак (4 ак. ч.).

8.4. Обзор основных средств защиты, необходимых для выполнения требований по обеспечению безопасности значимых объектов КИИ (6 ак. ч.)

8.4.1. Обзор основных средств защиты (4 ак.ч.)

8.4.1.1. Обзор средств защиты информации применяемых при построении системы безопасности значимого объекта КИИ.

8.4.1.2. Практические рекомендации по реализации требований обеспечения безопасности значимого объекта КИИ в части эксплуатации средств защиты информации.

8.4.2. Обзор основных средств мониторинга (2 ак.ч.)

8.4.2.1. Обзор основных средств мониторинга, необходимых для выполнения требований по обеспечению безопасности значимых объектов КИИ.

8.4.2.2. Практические рекомендации по реализации требований обеспечения безопасности значимого объекта КИИ в части эксплуатации средств мониторинга.

8.5. Опыт построения центров ГосСОПКА (2 ак. ч.).

9. Порядок приемки системы защиты информации (4 ак. ч.).

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

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

Тема 4. Контроль за обеспечением безопасности значимого объекта КИИ

10. Контроль за обеспечением безопасности значимого объекта КИИ (6 ак. ч.).

10.1. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

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

10.3. Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры) **(лабораторная работа)** (1 ак.ч.).

10.4. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности **(лабораторная работа).**

10.5. Организация и порядок проведения контроля за обеспечением безопасности значимого объекта КИИ

10.6. Оценка соответствия значимых объектов КИИ требованиям по безопасности **(семинар)**

11. Документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ (2 ак. ч.).

11.1. Состав комплекта документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

11.2. Разработка документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ **(практическое занятие).**

12. Итоговая аттестация (2 ак. ч.).

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