Институт мониторинга и оценки информационной безопасности
119618, г. Москва, ул. 50 лет Октября, д. 4
Тел.: +7 (495) 268 13 42, +7 (499) 130-06-34
e-mail info@imoib.ru сайт: imoib.ru
Лицензия на право осуществления образовательной деятельности №038554 от 24.07.17 Департамента образования города Москвы

Руководителю

Исх. № 08 от 29 июля 2024 года

26 августа – 26 сентября 2024 года

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

«Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

с выдачей удостоверения в объеме 216 часов

(программа согласованна со ФСТЭК России)

Приглашаем: заместителей руководителя – ответственных за информационную безопасность, руководителей и специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации субъектов критической информационной инфраструктуры РФ.

Программа реализуется: Институтом мониторинга и оценки информационной безопасности (№53 в реестре образовательных организаций ФСТЭК России) совместно с МКЦ «АСТА-информ» (лицензиат ФСТЭК и ФСБ России).

ПРОГРАММА КУРСА

1. ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

1.1. Правовые основы обеспечения безопасности КИИ Российской Федерации

- Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ.
- Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
- Основные понятия, термины и определения в области обеспечения безопасности ЗОКИИ. Система безопасности ЗОКИИ.
- Права и обязанности субъектов критической информационной инфраструктуры.
- Государственный контроль в области обеспечения безопасности ЗОКИИ. Цели государственного контроля в области обеспечения безопасности значимых объектов КИИ. Виды и периодичность.

1.2.Угрозы безопасности информации, обрабатываемой на объектах КИИ

- Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении ЗОКИИ. Модель угроз безопасности информации ЗОКИИ.
- Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия
- Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
- Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
- Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей ЗОКИИ, возможных способов реализации (возникновения) угроз безопасности информации и последствий от их реализации.
- Объекты оценки уязвимости: код, конфигурация и архитектура ЗОКИИ для всех программных и программно-аппаратных средств, в том числе средств защиты информации ЗОКИИ.
- Оценка возможных последствий реализации возникновения угроз безопасности информации в ЗОКИИ.

2. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА КИИ

2.1. Категорирование объектов КИИ

- Правила и порядок, сроки категорирования объектов КИИ.

- Реестр значимых объектов КИИ. Цель ведения реестра.
- Формирование комиссии по категорированию объектов КИИ.
- Формирование перечня объектов КИИ, подлежащих категорированию.
- Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.
- Перечень показателей критериев ЗОКИИ и их значения.
- Оценка в соответствии с перечнем показателей критериев ЗОКИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.
- Присвоение объектам КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.
- Подготовка необходимых документов в рамках категорирования объектов КИИ

2.2 Требования по обеспечению безопасности значимых объектов КИИ

- Установление требований по обеспечению безопасности ЗОКИИ.
- Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности ЗОКИИ.
- Планирование, разработка и совершенствование мероприятий по обеспечению безопасности ЗОКИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности ЗОКИИ.
- Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ.
- Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации.
- Выбор организационных и технических мер для обеспечения безопасности ЗОКИИ.
- Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности. Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ.

2.3. Система безопасности значимого объекта КИИ

- Цели и задачи системы безопасности значимого объекта КИИ.
- Требования к созданию систем безопасности значимых объектов КИИ.
- Требования к силам обеспечения безопасности значимых объектов КИИ.
- Требования к организационно-распорядительным документам по безопасности ЗОКИИ.
- Структура системы безопасности ЗОКИИ.
- Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ и обеспечения их функционирования.

2.4. Стадии (этапы) работ по созданию систем безопасности

- Этапы жизненного цикла системы безопасности ЗОКИИ.
- Стадии (этапы) работ по созданию систем безопасности ЗОКИИ.
- Разработка эксплуатационной, организационно-распорядительной документации на значимый объект КИИ и его систему безопасности.
- Внедрение системы безопасности значимого объекта КИИ.
- Установка и настройка средств защиты информации.
- Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ.
- Предварительные испытания значимого объекта КИИ и его системы безопасности.
- Опытная эксплуатация значимого объекта КИИ и его системы безопасности.
- Приемочные испытания значимого объекта КИИ и его системы безопасности.

3. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА КИИ

- Контроль за обеспечением уровня безопасности ЗОКИИ. Виды контроля (мониторинга) за обеспечением уровня безопасности значимого объекта КИИ и его системы безопасности.
- Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ.
- Оценка соответствия значимых объектов КИИ требованиям по безопасности.
- Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ и эффективности, принимаемых организационных и технических мер.

- Контроль (анализ) защищенности ЗОКИИ с учетом особенностей его функционирования.
- Анализ и оценка функционирования значимого объекта КИИ и его системы безопасности, включая выявление, анализ и устранение недостатков в функционировании системы безопасности значимого объекта КИИ.
- Документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ.

ПРЕПОДАВАТЕЛИ КУРСА

М.Ю. Шевченко – специалист - практик в области защиты информации, преподаватель дисциплин по технической защите информации, читает курсы по технической защите конфиденциальной информации и обеспечению безопасности значимых объектов КИИ.

И.М. Бирюк - реализовал более 450 проектов по защите информации и аттестовал свыше 290 ИС. 37 организаций подготовлены и успешно прошли проверки Роскомнадзора, ФСБ и ФСТЭК. Реализовал более 40 проектов по категорированию и защите объектов КИИ, читает курс по организации защиты конфиденциальной информации на объектах информатизации, категорированию и обеспечению безопасности объектов КИИ и т.д.

В.С. Крашаков - реализовал более 150 проектов по защите конфиденциальной информации. Реализовал более 20 проектов по категорированию и защите объектов КИИ. Читает курс по моделированию угроз значимых объектов КИИ, обеспечению безопасности объектов КИИ и т.д.

А.В. Лукацкий - ведущий эксперт РФ по информационной безопасности, читает курс по моделированию угроз, реагированию на инциденты, управлению ИБ

В.В. Комаров - ведущий эксперт в области защиты информации, практик, начальник отдела обеспечения осведомлённости Управления информационной безопасности Департамента информационных технологий г. Москва

Повышение квалификации проводят практикующие специалисты в области защиты информации, сотрудники организации-лицензиата ФСТЭК России, реализовавшие более 700 проектов по защите информации в государственных, муниципальных и коммерческих организациях. Аттестовавшие более 300 АС, ГИС, ИСПДн и подготовивших более 150 организаций к проверкам ФСТЭК России, ФСБ России и Роскомнадзора.

УСЛОВИЯ УЧАСТИЯ

ОБУЧЕНИЕ С ПРИМЕНЕНИЕМ ДИСТАНЦИОННЫХ ТЕХНОЛОГИЙ

Даты обучения	**26 августа 2024 по 26 сентября 2024г. (1 мес.)**
Время обучения	согласно расписания
Аттестация (тестирование)	26 сентября 2024 г.
Место обучения	рабочее или удаленное место слушателя
В стоимость обучения входит	методические материалы, видеозапись вебинаров, презентации лекторов
СТОИМОСТЬ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ	**29 990 рублей**
СТОИМОСТЬ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ	**27 990 рублей**

По окончанию обучения выдается **удостоверение установленного образца в объеме 216 часов**

Лицензии:

1. Лицензия ФСТЭК России № 1028 от 04.03.2010 на деятельность по технической защите конфиденциальной информации. Лицензия действует бессрочно.
2. Лицензия на право осуществления образовательной деятельности № 038554 Департамента образования города Москвы. Лицензия действует бессрочно.

ПРЕДВАРИТЕЛЬНАЯ РЕГИСТРАЦИЯ ОБЯЗАТЕЛЬНА

тел. 8 (495) 268-13-42 тел. 8 (499) 130-06-34 e-mail: info@imoib.ru **www.imoib.ru**

ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ НА САЙТЕ: https://imoib.ru/training/course/1417

Руководитель Института МОИБ

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01C6B8490093B0AABA4A7F4BC236938DF7
Владелец: АСТАХОВ АЛЕКСАНДР ГЕННАДЬЕВИЧ
Действителен: с 06.10.2023 до 06.01.2025

А.Г. Астахов