Институт мониторинга и оценки информационной безопасности
119454, г. Москва, пр. Вернадского 14А, пом. 4
Тел: +7 (495) 268-13-42, +7 (499) 130-06-34
Email: info@imoib.ru Сайт: imoib.ru
Лицензия на право осуществления образовательной деятельности №038554 от 24.07.17 Департамента образования города Москвы

Главному врачу

Исх. №02 от 16 января 2023 года

Согласно, **Указа Президента Российской Федерации от 01.05.2022 № 250** "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» в организациях - субъектах критической информационной инфраструктуры (КИИ), на **заместителя руководителя организации возлагаются полномочия по обеспечению информационной безопасности**.

Федеральным законом от 26.05.2021 № 141-ФЗ установлены штрафы за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры РФ и за неисполнение обязанности по представлению сведений, предусмотренных законодательством в области обеспечения безопасности КИИ.

В соответствии с требованиями законодательства РФ по КИИ **один раз в год необходимо проводить обучение работников по вопросам обеспечения безопасности критической информационной инфраструктуры** (п.15 Приказа №235 ФСТЭК от 21.12.2017) и в соответствии с ПП РФ №808 от 11.07.2018г, обязательно повышать квалификацию ответственных за обеспечение информационной безопасности:

09 – 10 февраля 2023 года

ДИСТАНЦИОННЫЙ КУРС ПОВЫШЕНИЯ КВАЛИФИКАЦИИ (ВЕБИНАР)

«Обеспечение безопасности объектов критической информационной инфраструктуры в учреждениях здравоохранения».

с учетом требований ФСТЭК России

с выдачей удостоверения о повышении квалификации в объеме 40 или 72 часа

ОСНОВНЫЕ ВОПРОСЫ, РАССМАТРИВАЕМЫЕ НА КУРСЕ

- Что из законодательства о критической информационной инфраструктуре нужно знать руководителям учреждений здравоохранения, ответственных за обеспечение безопасности, чтобы минимизировать риски привлечения к административной и уголовной ответственности. Первоочередные действия руководителя учреждения здравоохранения.
- Впервые за защиту информации введена уголовная ответственность. Какие составы ст.274.1 Уголовного кодекса РФ являются критичными для руководителей учреждений и ответственных за обеспечение безопасности?
- Административная ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры РФ. Федеральный закон от 26.05.2021 № 141-ФЗ.
- Судебная практика в сфере критической информационной инфраструктуры за 2020-2021 года.
- Основные понятия и определения в области КИИ. Какими нормативно правовыми актами Правительства РФ, ФСТЭК РФ и ФСБ РФ необходимо руководствоваться при организации работ по категорированию объектов КИИ в сфере здравоохранения?
- Какие сроки I, II и III этапов определены регуляторами по выполнению требований ФЗ-187 и обязательные мероприятия этих этапов?
- Кто должен войти в состав комиссии и кого нужно назначить ответственным в учреждении здравоохранения?
- Какие процессы в учреждении необходимо отнести к критическим и как оценить последствия их нарушений? Как определить взаимосвязь объекта КИИ с критическими процессами в учреждении?
- Особенности формирования перечня объектов КИИ в учреждении здравоохранения. Какие объекты нужно категорировать?
- Какие объекты КИИ учреждения обязаны будут отнести к значимым объектам?
- В каком виде необходимо отправить в Министерство, Департаменты и ФСТЭК обязательный

перечень объектов КИИ? Форма документа. Какой срок установил ФСТЭК РФ для предоставления актов категорирования объектов КИИ в Управление ФСТЭК?

- Пошаговые действия комиссии при определении категории значимости каждого объекта КИИ.
- Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения от Минздрава России.
- Как быть, если на момент подачи сведений во ФСТЭК, учреждение, из-за отсутствия ресурсов, не приняла организационно-технические меры по обеспечении безопасности?
- Какие приказы ФСТЭК и их содержание, нужно учитывать, кроме документов по КИИ, при категорировании объектов?
- **Что учреждения обязаны делать после категорирования объектов КИИ? Даже при отсутствии значимых объектов КИИ.**
- Ключевые требования приказов N 235 и N 239 ФСТЭК России для создания и обеспечения систем безопасности значимых объектов критической информационной инфраструктуры.
- Какой срок установил ФСТЭК России для мероприятий по обеспечению безопасности значимых объектов КИИ?
- Почему ФСТЭК интересуют только значимые объекты КИИ?
- Почему ФСБ и Прокуратуру интересуют все объекты КИИ в учреждении?
- Как ФСТЭК может привлечь к административной ответственности руководителя учреждения?
- Как ФСБ может привлечь к уголовной ответственности руководителя учреждения?
- Пошаговый алгоритм системы защиты значимых объектов КИИ.
- Формирование требований по обеспечении безопасности значимых объектов.
- Анализ угроз безопасности информации или разработка модели угроз для объекта КИИ.
- В каких случаях направляется Модель угроз безопасности во ФСТЭК и ФСБ на согласование.
- Требования к организационно-распорядительным документам по безопасности значимых объектов.
- Какие средства защиты информации необходимо установить, настроить и провести приемочные испытания?
- Иностранное оборудование и импортозамещение. Какие сроки перехода на отечественное ПО и «железо»?
- Должен ли учитываться и как определить масштаб возможных последствий в случае возникновения компьютерных инцидентов на значимом объекте?
- Можно ли учитывать компенсирующие меры, в случае если не установлены средства защиты информации, при определении категории значимости?
- Почему информирование, обучение персонала и повышение квалификации ответственного за защиту информации стало обязательным по федеральному законодательству? Какие требования предъявляются к обучению работников (пользователей) и ответственных за обеспечение безопасности в учреждении?
- Какую информацию учреждение обязано предоставлять в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты организации?
- Перечень и порядок предоставления информации в ГосСОПКа в соответствии с Приказом ФСБ России№ 367 от 24.07.2018г.
- Порядок обмена информацией о компьютерных инцидентах и Порядок получения информации о средствах и способах проведения компьютерных атак и о методах их предупреждения в соответствии с Приказом ФСБ №368 от 24.07.2018г.
- Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и субъект КИИ. Действия организации и предприятия в соответствии с Приказом ФСБ №366 от 24.07.2018г.
- В НКЦКИ необходимо передавать информацию по каждому компьютерному инциденту или только по инцидентам на значимых объектах КИИ учреждений здравоохранения?
- Кто в учреждении обязан отправлять информацию об компьютерных инцидентах в НКЦКИ?

ПРАКТИЧЕСКОЕ ПОГРУЖЕНИЕ

(практические занятия для подготовки документов по требованиям регуляторов)

- Подготовка перечня критических процессов в учреждении здравоохранения.

- Подготовка перечня объектов КИИ в учреждении здравоохранения, для согласования с вышестоящим министерством, департаментом, комитетом.
- Подготовка документов для ФСТЭК – «Перечень объектов КИИ учреждения здравоохранения», «Результаты категорирования объекта КИИ учреждения здравоохранения».
- Категорирование объектов КИИ согласно Методике Минздрава России.
- Анализ состава и последовательности работ по обеспечению безопасности значимых объектов КИИ после завершения категорирования согласно Методике Минздрава России.

ПРЕПОДАВАТЕЛЬ УЧЕБНОГО КУРСА

Бирюк Игорь Михайлович, преподаватель Института мониторинга и оценки информационной безопасности. Специалист-практик компании-лицензиата ФСТЭК и ФСБ, который провел более **400** курсов и семинаров в сфере защиты информации, на которых прошли обучение более **3500** слушателей. Реализовал более 50 проектов **по категорированию и защите объектов КИИ в учреждениях здравоохранения**. Лично подготовил более **50** организаций к проверкам Роскомнадзора, ФСБ, ФСТЭК.

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ (ВЕБИНАР):

Даты вебинаров	**09-10 февраля 2023 г.**
Время обучения	09.00 – 15.00 (МСК)
Место обучения	Рабочее или удаленное место слушателя
В стоимость обучения входит	видеозапись вебинара; презентации лектора, видео материалы ФСТЭК, ведущих экспертов; НПА по КИИ
УЧАСТИЕ В **1 ДНЕ** ВЕБИНАРА С выдачей удостоверения о повышении квалификации в объеме 40 часов	**5 990 рублей**
УЧАСТИЕ В **2-х ДНЯХ** ВЕБИНАРА С выдачей удостоверения о повышении квалификации в объеме 72 часа	**9 990 рублей**
СТОИМОСТЬ шаблонов документов по КИИ для учреждений здравоохранения	**+ 6 990 рублей**

Лицензии:

1. Лицензия на право осуществления образовательной деятельности № 038554 от 24.07.17 Департамента образования города Москвы. Лицензия действует бессрочно.

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

ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ НА САЙТЕ: https://imoib.ru/training/course/1077

Руководитель Института МОИБ

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 01FD35890010AF1FA74868852CCDC97418
Владелец: АСТАХОВ АЛЕКСАНДР ГЕННАДЬЕВИЧ
Действителен: с 14.09.2022 до 14.12.2023

А.Г. Астахов