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 Департамента образования города Москвы

Руководителю организации, предприятия, учреждения

Исх. № 11 от 20 апреля 2021 года

5 февраля 2021 года ФСТЭК России утвердила новую методику оценки (моделирования) угроз, использование которой является обязательным для всех операторов и владельцев информационных систем персональных данных, государственных и муниципальных информационных систем, автоматизированных систем управления технологическим процессом, значимых объектах критической информационной инфраструктуры, информационных систем управления производством, используемых в оборонно-промышленном комплексе, и т.п.

Возникают вопросы к данной теме. Как построить модель? Надо ли ее согласовывать с регуляторами? Что она должна включать? Как определить актуальность угроз? Какой формат должен быть у модели угрозы? Можно ли оптимизировать ее разработку? На все эти вопросы, а также на многие другие ответит данный курс.

28 мая 2021 года

КУРС ПОВЫШЕНИЯ КВАЛИФИКАЦИИ А.В. ЛУКАЦКОГО

«Моделирование угроз 2021: построение, оценка, внедрение».

в соответствии с «Методикой оценки угроз безопасности информации»
ФСТЭК России от 05.02.2021г.

с выдачей удостоверения о повышении квалификации в объеме 40 часов

Целью повышения квалификации: является формирования компетенций и навыков у специалистов по защите информации в сфере моделирования угроз в соответствии с требованиями ФСТЭК России.

Приглашаем: руководителей и специалистов по защите информации, должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса, организациях и компаниях различных организационных форм и форм собственности. Советников по безопасности, экспертов по безопасности. Руководителей и специалистов организаций специализирующихся на выполнении работ и предоставлении услуг по технической защите конфиденциальной информации. Разработчиков программного обеспечения.

ОСНОВНЫЕ ВОПРОСЫ, РАССМАТРИВАЕМЫЕ НА КУРСЕ

- Каковы первоочередные действия ответственных за защиту информации лиц в связи с утверждением ФСТЭК России «Методики оценки угроз безопасности информации»?
- В какие сроки необходимо актуализировать «Модели угроз» в организации? В каких случаях необходимо актуализировать модель угроз?
- Каковы основные шаги при моделировании угроз?
- На каких этапах жизненного цикла системы надо моделировать угрозы?
- Кого можно привлекать для разработки модели угроз и модели нарушителя? Только ли лицензиатов по ТЗКИ или можно дипломированных специалистов со стороны?
- Кто готовит модель угроз и модель нарушителя: оператор информационной системы или обладатель информации?
- Как классифицировать нарушителей?
- В чем отличие оценки рисков и оценки угроз?
- Что является результатом оценки рисков у оператора, на который можно сослаться при моделировании угроз?
- Какие источники угроз бывают?
- Насколько детализировано необходимо описывать объекты воздействия на аппаратном, системном, прикладном уровнях, на уровне сети и на уровне пользователя?
- Возможно ли и как сопоставить 4 уровня возможностей нарушителей и 3 типа потенциала

нарушителя?

- Что согласно новой методике корректно относить к интерфейсам пользовательского, прикладного и системного уровней?
- Каким образом может быть описан сценарий для непреднамеренной угрозы?
- На основе чего определяется перечень возможных угроз?
- Как осуществляется и оформляется экспертная оценка?
- Можно ли расширить перечень тактик и техник применительно к конкретной угрозе безопасности информации?
- Возможно ли составлять единые сценарии для сходных по типу и возможностям категорий нарушителей?
- Каким образом определяется актуальность угроз, связанных с техническими каналами утечки информации?
- Как проверить адекватность модели угроз?
- Какими каталогами угроз можно пользоваться?
- Как оформлять модель угроз?
- Надо ли согласовывать модель угроз с регуляторами?
- Как можно оптимизировать разработку модели угроз?
- Можно ли вести модель угроз в электронном виде?
- Что делать, если у меня уже есть модель угроз – надо ли ее переделывать под новую методику?
- Как часто надо обновлять модель угроз?

ПРЕПОДАВАТЕЛЬ КУРСА:
Лукацкий Алексей Викторович, ведущий российский эксперт в области информационной безопасности.

УСЛОВИЯ УЧАСТИЯ В КУРСЕ
ДИСТАНЦИОННОЕ ОБУЧЕНИЕ (ВЕБИНАР):

Даты обучения	**28 мая 2021 г.**
Время обучения	10.00 – 16.30 (МСК)
В стоимость обучения входит	запись курса, презентации лектора, материалы для самоподготовки, аттестация (тестирование)
СТОИМОСТЬ ОБУЧЕНИЯ для юридических лиц с выдачей удостоверения о повышении квалификации в **объеме 40 часов**	8 990 руб.
СТОИМОСТЬ ОБУЧЕНИЯ для физических лиц (предоплата 100%) с выдачей удостоверения о повышении квалификации в **объеме 40 часов**	6 990 руб.

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/731