



Исх. № 10 от 23 сентября 2026 года

Руководителю

Программа курса разработана согласно **Указа Президента Российской Федерации от 01.05.2022 № 250** "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и в соответствии с требованиями **Постановления Правительства Российской Федерации от 15.07.2022 № 1272** и требованиями **Приказа ФСТЭК России от 11.04.2025 №117** и ФСБ России к специалистам по защите информации:

20 октября 2026 года

курс повышения квалификации для специалистов по защите информации

«СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: противодействие и реагирование»

с выдачей удостоверения о повышении квалификации в объеме 40 часов

Целью повышения квалификации: является ознакомление специалистов по защите информации с тактиками и техниками социальной инженерии, способствующими реализации компьютерных атак, подходами по построению системы защиты и реагирования на компьютерные атаки использующие человеческий фактор.

Приглашаем: специалистов по защите информации, КИИ, АСУ, ответственных за безопасность персональных данных в ИСПДн, специалистов отделов информационных технологий и системных администраторов.

Программа реализуется: Институтом мониторинга и оценки информационной безопасности, состоящий в реестре ФСТЭК России под №53.

ПРОГРАММА КУРСА

1. Основные термины и понятия

- Что такое инцидент информационной безопасности, компьютерный инцидент, компьютерная атака, тактики и техники проведения компьютерной атаки?
- Управление и реагирование на компьютерную атаку и инцидент?
- Социальная инженерия как способ реализации компьютерной атаки. Подходы НЦКИ, ФСТЭК России, Центрального Банка

2. Психологические основы социальной инженерии

- Факторы влияющие на ошибки восприятия информации
- Алгоритмы принятия решений, когнитивные искажения
- Стресс и работоспособность
- Психология влияния и манипулирования (концепция Р. Чалдини)
- Точки контроля и влияния на человека

3. Социальная инженерия как вид атаки на человека и способ реализации компьютерной атаки

4. Каналы реализации социальной инженерии

- При личном взаимодействии
- При проникновении на объект
- При взаимодействии по телефону
- При использовании информационных технологии

5. Противодействие действиям внутреннего нарушителя (инсайдера)

6. Классические техники и тактики социальной инженерии

- Pretexting
- Tailgating
- Shoulder Surfing
- Baiting
- Quid Pro Quo
- Deepfakes
- Phishing

7. Фишинг

- Этапы реализации фишинга
- 11 видов фишинга
- Признаки фишингового письма
- Признаки фишингового сайта
- Виды ВПО

8. Способы противодействия социальной инженерии для работников (пользователей)

- Рекомендации для работников организации
- Распознаем Deepfakes
- Противодействие влиянию и манипуляции

9. Организация мер защиты и реагирования на социальную инженерию для специалистов по защите информации

- Моделирование угроз (ФСТЭК России, MITRE ATT&CK)
- Организационно – технические меры противодействия социальной инженерии (ФСТЭК России, НКЦКИ, Cisco Systems)
- Реагирование на атаку с использованием тактик и техник социальной инженерии

10. Ответы на вопросы

ПРЕПОДАВАТЕЛЬ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Н.М. Пугачев – преподаватель Института МОИБ, практикующий специалист в области защиты информации.

УСЛОВИЯ УЧАСТИЯ

ОБУЧЕНИЕ С ПРИМЕНЕНИЕМ ДИСТАНЦИОННЫХ И ЭЛЕКТРОННЫХ ТЕХНОЛОГИЙ:

Даты обучения	20 октября 2026г.
Даты самоподготовки	21 - 23 октября 2026г.
Аттестация (тестирование)	26 октября 2026г.
Время обучения	10.00 – 14.00 (МСК)
Место обучения	удаленное место слушателя
В стоимость обучения входит	методические материалы, видеозапись, презентации лектора

СТОИМОСТЬ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ 5 990 рублей

С выдачей удостоверения о повышении квалификации в объеме 40 часов

СТОИМОСТЬ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ 5 790 рублей

С выдачей удостоверения о повышении квалификации в объеме 40 часов

По окончании обучения выдается

Удостоверение о повышении квалификации в объеме 40 часов по программе «Социальная инженерия: реагирование и противодействие»

Лицензии:

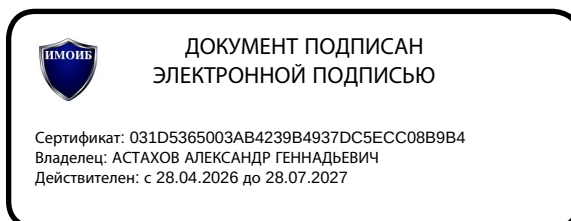
1. Лицензия на право осуществления образовательной деятельности № 038554 Департамента образования города Москвы. Лицензия действует бессрочно.
2. Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации №ЛО24-00107-77/01648168 от 17.12.24

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/2036>

Руководитель Института МОИБ



А.Г. Астахов