



Руководителю

Исх. № 01 от 09 января 2025 года

Согласно Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» в федеральных органах исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятиях, стратегических акционерных обществах и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры, на заместителя руководителя организации возлагаются полномочия по обеспечению информационной безопасности.

Программа курса разработана в соответствии с требованиями постановления Правительства Российской Федерации от 15.07.2022 № 1272 и требованиями ФСТЭК России и ФСБ России, предъявляемыми к заместителю руководителя ответственному за обеспечение информационной безопасности, специалистам по защите информации и к соискателям лицензии на осуществление лицензируемого вида деятельности по технической защите конфиденциальной информации:

**27 января – 30 апреля 2025 года (3 мес.)**  
**ПРОФЕССИОНАЛЬНАЯ ПЕРЕПОДГОТОВКА**

## **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Техническая защита конфиденциальной информации».**

**в соответствии с требованиями ФСБ и ФСТЭК России**  
**с выдачей диплома о профессиональной переподготовке в объеме 508 часов**  
(программа обучения согласована со ФСТЭК России)

**Целью профессиональной переподготовки:** является формирования знаний, умений и компетенций у заместителей руководителя, специалистов по информационной безопасности организаций, учреждений и предприятий, в том числе государственных гражданских служащих и муниципальных служащих для выполнения нового вида профессиональной деятельности.

**Приглашаем:** заместителей руководителя, специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации субъектов КИИ, 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. Руководителей и специалистов организаций специализирующихся на выполнении работ и предоставлении услуг составляющих лицензируемую деятельность по технической защите конфиденциальной информации.

**Программа профессиональной переподготовки реализуется:** Институтом мониторинга и оценки информационной безопасности, состоящий в реестре ФСТЭК России под №53 совместно с МКЦ «АСТА-информ» (организация-лицензиат ФСТЭК и ФСБ России).

### **УЧЕБНЫЕ ДИСЦИПЛИНЫ**

- 1. Организационно – правовые основы защиты информации:** Цели и задачи защиты информации, Основы нормативно-правового обеспечения защиты информации
- 2. Управление информационной безопасностью:** Цели, задачи, этапы управления информационной безопасностью, управление рисками, мониторинг и улучшение системы информационной безопасности.
- 3. Реагирование на инциденты информационной безопасности:** Виды инцидентов, правила, реагирования, требования по реагированию ФСБ России, ФСТЭК России, Банк России и т.д. Взаимодействие с ГОССОПКОЙ.
- 4. Моделирование угроз в соответствии с методикой ФСТЭК России.**
- 5. Обеспечение безопасности объектов критической информационной инфраструктуры.**

- 6. Способы и средства защиты информации от утечки по техническим каналам:** Технические каналы утечки информации. Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок. Способы и средства защиты акустической речевой информации от утечки по техническим каналам
- 7. Меры и средства защиты информации от несанкционированного доступа:** Угрозы безопасности информации, связанные с НСД. Меры и средства защиты информации от НСД.
- 8. Техническая защита конфиденциальной информации от специальных воздействий:** Информация как объект защиты от специальных воздействий. Меры и средства защиты информации от специальных воздействий.
- 9. Организация защиты конфиденциальной информации на объектах информатизации:** Организация защиты конфиденциальной информации на объектах информатизации. Реализация требований по технической защите конфиденциальной информации. Проектирование систем защиты конфиденциальной информации.
- 10. Особенности защиты информации в государственных информационных системах.**
- 11. Организация обработки и обеспечение безопасности персональных данных в организации.**
- 12. Организация работы со средствами защиты информации в соответствии с требованиями ФСТЭК России и ФСБ России.**
- 13. Организация работы со средствами криптографической защиты информации в соответствии с требованиями ФСБ России**
- 14. Аттестация объектов информатизации по требованиям безопасности информации:** Организация аттестации объектов информатизации на соответствие требованиям безопасности информации. Организация аттестации объектов информатизации по требованиям безопасности информации.
- 15. Контроль состояния защиты информации в организации, учреждении и предприятии:** Основы организации контроля состояния ТЗКИ. Методы и средства контроля защищенности конфиденциальной информации. Мониторинг информационной безопасности средств и систем информатизации
- 16. Подготовка организации к проверкам регуляторов в сфере информационной безопасности.**
- 17. ИТОГОВАЯ АТТЕСТАЦИЯ** - тестирование

#### ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

- 1. Практикум:** категорирование объектов критической информационной инфраструктуры.
- 2. Практикум:** организация и проведение работ по аттестации объектов информатизации.
- 3. Практикум:** реагирование на инциденты информационной безопасности, разработка регламента реагирования
- 4. Практикум:** моделирование угроз безопасности информации для информационных систем
- 5. Практикум:** определение мер защиты информации для ИС
- 6. Семинар:** виды компьютерных атак
- 7. Семинар:** противодействие методам социальной инженерии
- 8. Практикум:** тестирование информационных систем на проникновение

В ходе обучения будут рассмотрены не только основные направления, методы, способы и средства защиты информации, но и организационные документы по информационной безопасности необходимые как для работы структурных подразделений по защите информации, так и организации в целом.

#### ПРЕПОДАВАТЕЛИ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

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

**М.Ю. Шевченко** - специалист в области защиты информации, преподаватель дисциплин по технической защите информации, читает курсы по технической защите конфиденциальной информации.

**В.В. Комаров** - ведущий эксперт в области защиты информации, практик, читает курс по защите информации в ГИС и организации повышения осведомленности сотрудников субъектов КИИ.

**И.М. Бирюк** - реализовал более 100 проектов по защите субъектов КИИ и аттестовал свыше 290 ИСПДн. 37 организаций подготовлены и успешно прошли проверки Роскомнадзора, ФСБ и ФСТЭК, читает курсы по обеспечению безопасности и категорированию объектов КИИ в учреждениях здравоохранения, реагированию на инциденты и взаимодействию организаций с ГОССОПКОЙ, организации работы с средствами криптографической

защиты информации.

**В.С. Крашаков** - реализовал более 30 проектов по защите субъектов КИИ и аттестовал свыше 20 ИСПДн практикующий специалист в области защиты информации, читает курс по обеспечению безопасности персональных данных в ИСПДн.

**Н.М. Пугачев** - практикующий специалист в области защиты информации, читает курс по организации обработки персональных данных, противодействие угрозам социальной инженерии.

Повышение квалификации проводят практикующие специалисты в области защиты информации, сотрудники организации-лицензиата ФСТЭК России и ФСБ России, реализовавшие более 1200 проектов по защите информации в государственных, муниципальных и коммерческих организациях. Аттестовавшие более 475 АС, ГИС, ИСПДн и подготовивших более 150 организаций к проверкам ФСТЭК России, ФСБ России и Роскомнадзора.

**УСЛОВИЯ и СТОИМОСТЬ УЧАСТИЯ**  
**ОБУЧЕНИЕ ОЧНО-ЗАОЧНОЕ С ПРИМЕНЕНИЕМ**  
**ДИСТАНЦИОННЫХ и ЭЛЕКТРОННЫХ ТЕХНОЛОГИЙ:**

Даты обучения	<b>27 января по 30 апреля 2025г. (3 мес.)</b>
Время обучения	согласно расписания ПП
Место обучения	удаленное место слушателя
В стоимость обучения входит	методические материалы, видеозапись вебинаров, презентации лекторов, примеры шаблонов документов
<b>СТОИМОСТЬ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ</b>	<b>59 990 рублей</b>
<b>СТОИМОСТЬ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ</b> (возможна оплата частями или предоставление банковской рассрочки)	<b>49 990 рублей</b>

**ПО ОКОНЧАНИЮ ОБУЧЕНИЯ ВЫДАЕТСЯ:**

1. **Диплом о профессиональной переподготовке в объеме 508 часов**, который удостоверяет квалификацию специалиста и дает право на ведение профессиональной деятельности в области информационной безопасности.
2. **Заключение** на слушателя о подготовке и допуске к самостоятельной работе с СКЗИ КриптоПро CSP и с СКЗИ ViPNet Client от организации лицензиата ФСБ России.

**Лицензии:**

1. Лицензия ФСТЭК России (№ 1028 от 04.03.2010) на деятельность по технической защите конфиденциальной информации. Лицензия действует бессрочно.
2. Лицензия Управления ФСБ России (№ 271 от 30.12.2014) на осуществление деятельности по распространению шифровальных (криптографических) средств. Лицензия действует бессрочно.
3. 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](mailto:info@imoib.ru) [www.imoib.ru](http://www.imoib.ru)

**ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ НА САЙТЕ:** <https://imoib.ru/training/course/1506>

Руководитель Института МОИБ

А.Г. Астахов