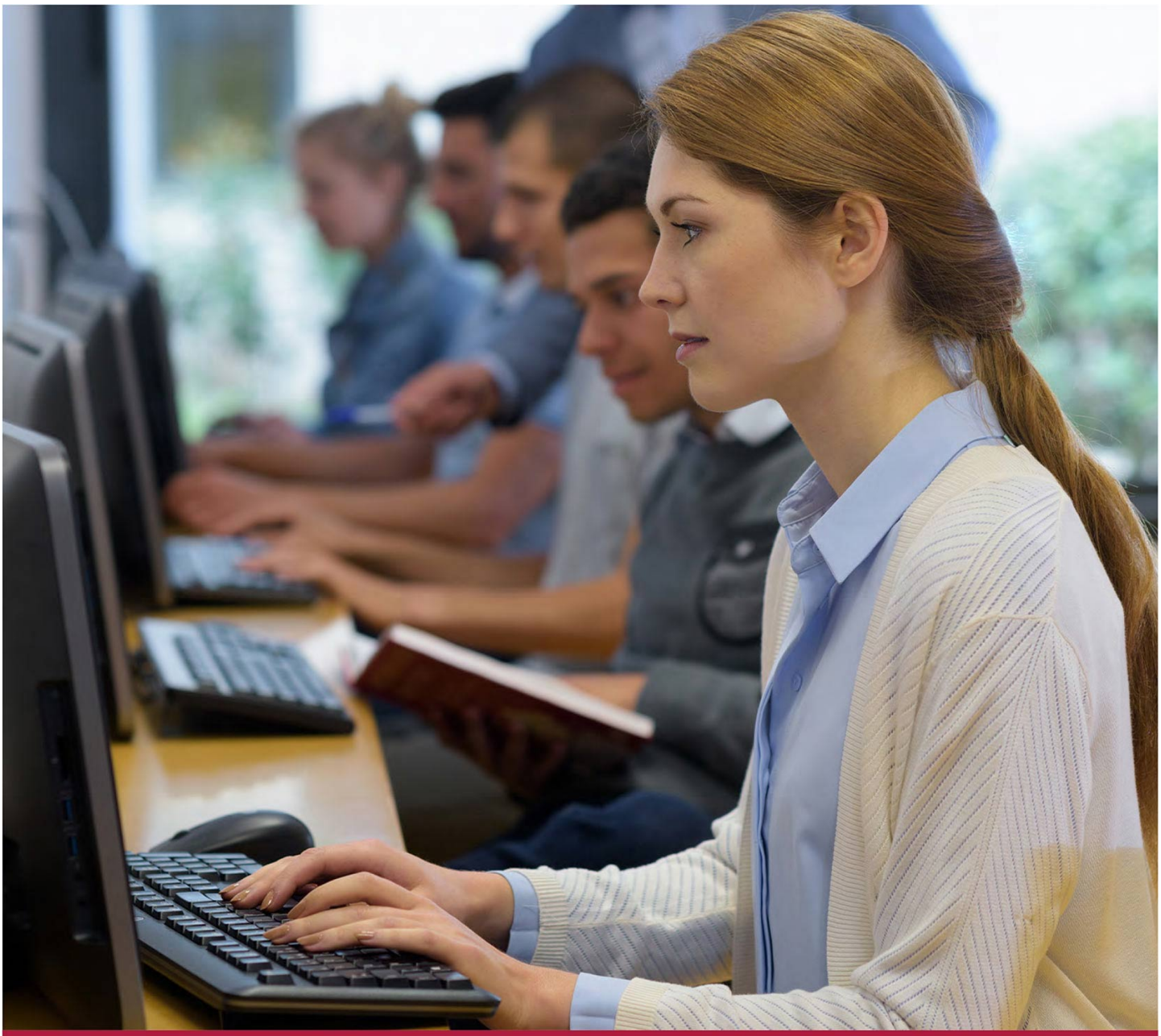
Академия АйТи
a Softline Company



Организация и обеспечение информационной безопасности в органе (организации)

Код курса: ПП1272

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Организация и обеспечение информационной безопасности в органе (организации)

Код курса: ПП1272

Длительность	520 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Информационная безопасность является одним из фундаментальных вопросов стабильного и постоянного функционирования органов и организации. Организация функционирования структурных подразделений, ответственных за информационную безопасность требует глубоких комплексных компетенций для обеспечения высокого уровня соответствия актуальным нормам безопасности. В рамках данной программы подробно изучаются вопросы обеспечения информационной безопасности и ее фундаментальные концепции для руководителей служб информационной безопасности, основные принципы архитектуры информационной инфраструктуры, а также конкретные меры и средства обеспечения ИБ в органе (организации), обнаружения, предотвращения и обнаружения атак, а также организации контролирующих мероприятий состояния информационной безопасности. Настоящая программа разработана с учетом положений: - Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»; - Федерального закона от от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; - Указа Президента Российской Федерации от 21 февраля 2019 г. №250 «О профессиональном развитии государственных гражданских служащих Российской Федерации»; - Типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), утвержденного постановлением Правительства Российской Федерации от 15 июля 2022 г. № 1272; - приказа Министерства науки и высшего образования Российской Федерации от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»; - профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 9 августа 2022 г. № 474н; - профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 536н; - профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 533н; - профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 525н; - федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26

ноября 2020 г № 1457; - примерной программы профессиональной переподготовки «Организация и обеспечение информационной безопасности в органе (организации)», утвержденной ФСТЭК России 25 ноября 2024 г.

Подробная информация

Профиль аудитории:

- Заместители руководителей органов (организаций), ответственные за обеспечение информационной безопасности в органе (организации)
- Руководители структурных подразделений обеспечивающих информационную безопасность органа (организации)

Предварительные требования:

- Уровень образования лица, поступающего на обучение – высшее образование, подтвержденное документом об образовании

По окончании курса слушатели изучат:

- нормативные правовые акты Российской Федерации, методические документы, международные и национальные стандарты в области информационной безопасности
- нормативные правовые акты, методические документы, международные и национальные стандарты в области криптографической защиты информации;
- цели, задачи и основы обеспечения информационной безопасности органа (организации);
- основные (производственные, управленческие) и бизнес процессы органа (организации);
- цели, задачи, основы организации, основные способы и средства обеспечения информационной безопасности;
- задачи и полномочия подразделения по защите информации;
- порядок организации взаимодействия структурных подразделений органа (организации) при решении вопросов обеспечения информационной безопасности;
- стратегию развития информационной безопасности в органе (организации);
- порядок антикризисного управления при реагировании на компьютерные инциденты в органе (организации);
- цели обеспечения информационной безопасности применительно к основным процессам функционирования органа (организации), реализацию и контроль их достижения;
- основы построения и функционирования информационных систем, основы формирования информационных ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей
- основы построения систем защиты конфиденциальной информации и систем безопасности значимых объектов КИИ Российской Федерации;
- общие требования к созданию систем безопасности в органе (организации);
- основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации;
- возможности типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности, в т.ч. средств криптографической защиты информации (СКЗИ)
- руководящие принципы, правила, процедуры и практические приёмы в области эксплуатации

и сопровождения СКЗИ;
- технические каналы утечки информации, способы защиты информации;
- методы защиты информации от несанкционированного доступа (НСД) и специальных воздействий на нее;
- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в органе (организации);
- порядок организации работ по обеспечению информационной безопасности в органе (организации);
- процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;
- основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности органа (организации) для исключения (невозможности реализации) негативных последствий;
- цели, задачи, основные принципы организации государственного и ведомственного контроля в области обеспечения безопасности значимых объектов КИИ Российской Федерации;
- порядок проведения проверок и контроля результативности применяемых методов и средств обеспечения информационной безопасности в органе (организации);
- средства и методики контроля эффективности защиты информации от утечки по техническим каналам;
- средства и методики контроля защищенности информации от несанкционированного доступа;
- основы лицензирования деятельности по технической защите конфиденциальной информации и криптографической защите информации, не содержащей сведений, составляющих государственную тайну;
- порядок аттестации объектов информатизации на соответствие требованиям о защите информации;
- основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности;
- отраслевые особенности построения вычислительных сетей, сетей и систем передачи информации, телекоммуникационных систем;
- отраслевые особенности задач и полномочий структурного подразделения органа (организации), обеспечивающего информационную безопасность.

Программа курса

Модуль 1 «Основы информационной безопасности в Российской Федерации»

- Основные понятия в области информационной безопасности
- Основы нормативного правового и методического обеспечения технической защиты конфиденциальной информации
- Основные нормативные правовые акты и методические документы в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Модуль 2 «Основы построения и функционирования информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления критической информационной инфраструктуры в органе (организации)»

- Технические средства обработки информации

- Информационные технологии
- Вычислительные сети, сети и системы передачи информации

Модуль 3 «Угрозы информационной безопасности информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления критической инфраструктуры в органе (организации). Управление рисками информационной безопасности»

- Угрозы информационной безопасности в органе (организации)
- Оценка угроз безопасности информации
- Управление рисками информационной безопасности

Модуль 4 «Меры и средства обеспечения информационной безопасности в органе (организации)»

- Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам
- Меры и средства технической защиты конфиденциальной информации от НСД
- Средства криптографической защиты информации, не содержащей сведения, составляющие государственную тайну
- Техническая защита конфиденциальной информации от специальных воздействий
- Меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры

Модуль 5 «Планирование и организация обеспечения информационной безопасности в органе (организации)»

- Планирование работ по обеспечению информационной безопасности в органе (организации)
- Организация защиты конфиденциальной информации на объектах информатизации
- Обеспечение безопасности значимых объектов критической инфраструктуры на различных этапах жизненного цикла

Модуль 6 «Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты»

- Нормативные правовые акты, регламентирующие деятельность по обнаружению, предупреждению и ликвизации последствий компьютерных атак
- Назначение и структура ГосСОПКА
- Организация функционирования ГосСОПКА

Модуль 7 «Контроль за обеспечением информационной безопасности в органе (организации)»

- Основы организации контроля состояния технической защиты конфиденциальной информации
- Мониторинг информационной безопасности средств и систем информатизации
- Государственный контроль в области обеспечения безопасности значимых объектов КИИ
- Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ

Модуль 8 «Отраслевые особенности обеспечения информационной безопасности в органе

(организации)»

- Отраслевые особенности построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов КИИ
- Отраслевые особенности обеспечения информационной безопасности

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru