Учебный план

программы повышения квалификации

«Основы информационной безопасности»

Программа повышения квалификации «**Основы информационной безопасности**» предназначена для слушателей, объектами профессиональной деятельности которых являются:

– автоматизированные системы, функционирующие в условиях существования информационных угроз и обладающие ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования информационных угроз и задействующие ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем.

Уровень образования лиц, поступающих на обучение – среднее профессиональное образование или высшее образование, подтверждённое документом об образовании.

Общая трудоёмкость обучения составляет 72 часа.

Форма обучения – очно-заочная (с применением дистанционных технологий).

№ п/п	Наименование разделов	Всего, час.	В том числе	
			лекции	практич. и лаборат. занятия
1	Угрозы безопасности компьютерных систем	20	10	10
2	Защита операционных систем и программных средств	12	8	4
3	Методы и модели контроля доступа	12	8	4
4	Мониторинг и аудит	10	6	4
5	Резервирование и аварийное восстановление	10	6	4

6	Социальные аспекты безопасности	6	6	–
Итоговая аттестация		2	зачёт	

В случае прохождения стажировки в профильной организации объём в часах, выделяемый на изучение разделов и тем, корректируется.

Учебно-тематический план

программы повышения квалификации

«Основы информационной безопасности»

№ п/п	Наименование разделов и тем	Всего, час.	В том числе	
			лекции	практич. и лаборат. занятия
1	2	3	4	5
1	**Угрозы безопасности компьютерных систем**	**20**	**10**	**10**
1.1	Вредоносные программы*	2	2	–
1.2	Способы доставки вредоносного программного обеспечения*	2	2	–
1.3	Предотвращение и устранение проблем, вызванных вредоносными программами*	6	2	4
1.4	Использование приложений для обеспечения безопасности	6	2	4
1.5	Защита компьютерного оборудования и периферийных устройств	4	2	2
2	**Защита операционных систем и программных средств**	**12**	**8**	**4**
2.1	Защита операционных систем*	9	6	4
2.2	Обеспечения безопасной работы в браузере*	3	2	–
3	**Методы и модели контроля доступа**	**12**	**8**	**4**
3.1	Модели управления доступом*	6	4	2
3.2	Методы контроля доступа	6	4	2
4	**Мониторинг и аудит**	**10**	**6**	**4**
4.1	Мониторинг систем и сетей	6	4	–
4.2	Аудит*	4	2	4
5	**Резервирование и аварийное восстановление**	**10**	**6**	**4**
5.1	Планирование избыточности*	5	3	2

5.2	Планирование и процедуры аварийного восстановления*	5	3	2
6	**Социальные аспекты безопасности**	**6**	**6**	–
6.1	Социальная инженерия*	3	3	–
6.2	Законодательная и организационная политика*	3	3	–
	Итоговая аттестация	**2**		

* – занятия по теме проводятся с применением дистанционных технологий