Общество с ограниченной ответственностью
«Учебно-научный центр информационной безопасности»

УТВЕРЖДАЮ
Директор
ООО «УЦИБ»
_____ А.В. Гришин
«17» сентября 2013 г.

УЧЕБНЫЙ ПЛАН

повышения квалификации специалистов по программе
«Безопасность информационных технологий»

Цель:
Более подробно и углубленно рассмотрение проблемы компьютерной безопасности, как наиболее актуальной для систем управления и обработки информации, что обусловлено широким применением компьютерных технологий в различных сферах жизнедеятельности общества

Категория слушателей:
- Руководителей и сотрудники предприятий и организаций, осуществляющих сбор, обработку, хранение и передачу информации;
- Руководители и сотрудники подразделений защиты информации, ответственные за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информации;
- Аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности, определение требований к защищенности подсистем автоматизированных систем и путей обеспечения их защиты;
- Специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- Администраторы средств защиты, контроля и управления безопасностью, ответственные за сопровождение и администрирование средств защиты информации, средств анализа защищенности подсистем автоматизированных систем;
- Менеджеры, ответственные за работу с персоналом по вопросам обеспечения информационной безопасности;
- Преподаватели учебных заведений, в которых ведется подготовка специалистов по различным направлениям информационной безопасности

Срок обучения: 80 часов (2 недели)
Режим занятий: 8 часов в день

№ п/п	Наименование разделов и тем	Всего часов	В том числе		Формы контроля
			Лекции	Практические занятия	
1	2	3	4	5	6
Раздел 1. Безопасность информационных технологий					
1.	Основные понятия безопасности информационных технологий	2	2		зачет

1	2	3	4	5	6
2.	Угрозы информационной безопасности и их классификация	2	2		зачет
3.	Виды мер обеспечения информационной безопасности	2	2		зачет
4.	Основные защитные механизмы	2	2		зачет
Раздел 2. Правовые основы обеспечения информационной безопасности					
5.	Законы РФ и другие нормативно-правовые документы	2	2		зачет
Раздел 3. Организационные меры защиты					
6.	Состав и организационная структура системы обеспечения информационной безопасности	2	2		зачет
7.	Регламентация процессов и действий персонала	4	2	2	зачет
8.	Обязанности сотрудников по обеспечению информационной безопасности	2	2		зачет
9.	Регламентация процесса авторизации	4	2	2	зачет
10.	Регламентация процесса внесения изменений в аппаратно-программную конфигурацию подсистем	2	2	0	зачет
11.	Регламентация процесса информационного обмена со сторонними организациями	4	2	2	зачет
12.	Регламентация применения средств защиты информации	2	2		зачет
13.	Регламентация действий в нештатных ситуациях	2	2		зачет
14.	Определение требований к защищенности ресурсов	4	2	2	зачет
Раздел 4. Средства защиты от внутренних нарушителей					
15.	Задачи, решаемые средствами защиты информации от несанкционированного доступа	4	4		зачет
16.	Основные возможности и защитные механизмы	8	4	4	зачет
Раздел 5. Обеспечение безопасности компьютерных сетей					
17.	Проблемы обеспечения безопасности в сетях	6	4	2	зачет
18.	Межсетевые экраны	8	4	4	зачет
19.	Виртуальные частные сети (VPN).	8	4	4	зачет
20.	Средства выявления уязвимостей узлов сетей и средства обнаружения атак на узлы, протоколы и сетевые службы	8	4	4	зачет
21.	Итоговое занятие. Прием зачета	2			2
	Всего	**80**	**52**	**26**	**2**