

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

УТВЕРЖДАЮ

Директор  
ООО «УНИЦИБ»

  
А.В. Гришин

«17» сентября 2013 г.



## УЧЕБНЫЙ ПЛАН

### повышения квалификации специалистов по программе «Теория и практика применения PKI»

#### Цель:

Практическое применение и использование электронной подписи для подтверждения подлинности передачи электронных сообщений и систем шифрования с открытым ключом для криптографической защиты конфиденциальности передаваемых электронных сообщений в рамках инфраструктуры открытых ключей (Public Key Infrastructure – PKI)

#### Категория слушателей:

- Специалисты в области информационных технологий, ответственные за выбор, внедрение и администрирование средств построения инфраструктуры открытых ключей;
- Сотрудники предприятий и организаций любых форм собственности, обеспечивающие практическое использование комплекса программно-аппаратных средств шифрования с открытым ключом для обеспечения конфиденциальности информации и подтверждение подлинности передаваемых сообщений путем применения средств электронной подписи

**Срок обучения:** 80 часов (2 недели)

**Режим занятий:** 8 часов в день

№ п/п	Наименование разделов, тем	Всего часов	В том числе		Формы контроля
			Лекции	Практические занятия	
1	2	3	4	5	6
<b>Раздел 1. Место и роль криптографии в обеспечении безопасности информационных технологий</b>					
1	Актуальность проблемы безопасности сетевых технологий. Место и роль криптографических методов и средств в системах управления и электронной коммерции. Задачи, решаемые средствами криптографической защиты информации: конфиденциальность, доступность, целостность и аутентичность данных, аутентификации абонентов	6	6		зачет
<b>Раздел 2. Криптографические примитивы и механизмы PKI</b>					
2	Электронные подписи. Механизмы электронной подписи. Криптографические хэш-функции. Схемы подписи RSA и Эль-Гамала	12	8	4	зачет

1	2	3	4	5	6
<b>Раздел 3. Практические аспекты использования РКІ</b>					
3	Понятие сертификата ключа подписи. Жизненный цикл сертификата: генерация, отзыв, приостановка действия, истечение сроков действия.	16	10	6	зачет
4	Форматы сертификатов. Отзыв сертификатов. Распространение информации в РКІ.	10	6	4	зачет
5	Проблемы, возникающие при реализации РКІ. Резервное копирование и восстановление ключей. Дублирование и депонирование ключей. Метки времени. Перекрестная сертификация. Разбор конфликтных ситуаций при доказательстве подлинности ЭП.	28	12	16	зачет
<b>Раздел 4. Правовые вопросы применения средств криптографической защиты информации</b>					
6	Закон РФ об электронной подписи, отдельные статьи УК РФ. Доктрина информационной безопасности РФ.	4	4		зачет
7	Итоговое занятие, прием зачета	4			4
<b>Итого</b>		<b>80</b>	<b>46</b>	<b>30</b>	<b>4</b>