

Программа конференции «РусКрипто2002»

31 января: четверг

18.00 - Отъезд из Москвы (автобусом от Савеловского вокзала) в пансионат «Озеро Круглое».

ДЕНЬ ПЕРВЫЙ: 1 февраля, пятница

9.20 – 10.00	<i>Завтрак</i>
10.00 – 10.05	Открытие конференции.
10.05 – 10.35	Современные криптографические технологии и средства защиты информации (обзор мирового и отечественного рынка). Волчков А.А. президент Ассоциации «РусКрипто»
10.35 – 11.05	Основные достижения теоретической криптологии в 2001 году (по материалам международных конференций CRYPTO'2001, EUROCRYPT'2001, ASIACRYPT'2001 и др.) Жуков А.Е., к.ф.-м.н., доцент МГТУ
11.05 – 11.30	Сравнение современных алгоритмов цифровой подписи. Иванов А.Г., к.ф.-м.н., с.н.с.
11.30 – 12.00	<i>Перерыв. Чай, кофе, ...</i>
12.00 – 12.30	«CRYPTONESSIE» конкурс на новые европейские криптографические стандарты. Лебедев А.Н., президент ЛАН Крипто
12.30 – 13.00	Криптография в программах обучения защите информации в университетах мира. Варфоломеев А.А., к.ф.-м.н., доцент МИФИ
13.00 – 13.30	Что и как регулируется в области криптографии в России. Волчков А.А. президент РусКрипто
13.30 – 15.00	<i>Обед</i>
15.00 – 16.30	Круглый стол: «Потребители и поставщики систем защиты информации». Что нужно потребителю и что предлагают поставщики. Чем определяется выбор решений по защите информации. Как сравнить средства защиты информации. Опыт проведения тендеров по системам защиты информации. Совместное использование средств защиты информации от разных производителей. Ответственность производителей и поставщиков решений. <i>Участствуют:</i> ГАЗПРОМ, МПС, ПФ РФ, РАО «ЕЭС России», ГЦБИ при Президенте Беларуси, ... ЭЛВИС+. Инфосистемы Jet, InterTrust, Алладин, ЛАН Крипто, ...
16.30 – 17.00	<i>Перерыв. Чай, кофе, ...</i>
17.00 – 18.30	Практические последствия принятия новых законов «О лицензировании...» и «Об электронной цифровой подписи» для потребителей и поставщиков средств защиты информации. Соловяненко Н.И., к.ю.н., с.н.с. Института государства и права РАН Пахутко О.П., юрист НАУФОР Волков П.М., начальник отдела Минэкономразвития Волчков А.А., президент РусКрипто
19.30 – 23.00	<i>Официальный ужин. Знакомство участников конференции.</i>

ДЕНЬ ВТОРОЙ: 2 февраля, суббота

9.20 – 10.00	<i>Завтрак.</i>
Программа «Электронная Россия» и развитие информационных технологий.	
10.00 – 10.30	Приведение российского законодательства в области ИТ, в частности, в области защиты информации, в соответствие с общепринятыми международными стандартами. Церенов Ц.В., руководитель департамента регулирования предпринимательской деятельности Минэкономразвития
10.30 – 10.50	Волков П.М., начальник отдела правового департамента Минэкономразвития
10.50 – 11.10	Изменение отечественной системы стандартизации в области защиты информации. Попов Ю.Г., начальник отдела лицензирования Гостехкомиссии России
11.10 – 11.30	Необходимость либерализации регулирования в области защиты информации в РФ. Нисневич Ю.А., д.полит. н., Главный. Консультант Центра полититической консультации.
11.30 – 12.00	<i>Перерыв. Чай, кофе, ...</i>
12.00 – 12.30	История криптологии: отечественные шифровальные службы во второй половине XX века. Соболева Т.А., кандидат филолог. наук, независимый эксперт
12.30 - 13.30	Российская открытая криптология: первые десять лет. Участствуют: Анашин В.С., Варфоломеев А.А., Волчков А.А., Жуков А.Е., Лебедев А.Н., Молдовян Н.А., Носов В.А., Сидельников В.М., Ященко В.В.

13.30 – 15.00	<i>Обед.</i>
15.00 – 18.15	Секционные заседания.
Практика создания систем информационной безопасности	Теоретические вопросы криптологии
Концепции обеспечения безопасности в Windows 2000. (Microsoft).	Блочные алгоритмы шифрования для специальных применений. Иванов А.Г.
Обеспечение безопасности в ОС Linux. (ALT Linux)	Управляемые блочные шифры. Молдовян Н.А.
Мониторинг безопасности сети серверов AS/400. (Пенсионный Фонд РФ)	Теоретические основы построения поточных шифров. Пудовкина М.А.
Средства разработки систем информационной безопасности (Macadam)	Криптоанализ алгоритмов семейства RC. Пудовкина М.А.
Проблемы реализации алгоритмов генерации ключей и случайных чисел. (РусКрипто).	Слабости алгоритма генерации ключей в системе iBank. Чиликов А.
Разработка и внедрение СКЗИ. (Крипто Про)	Новые алгоритмы шифрования. Комиссаренко В.В., Микулич Н.Д.
Практика создания и поддержки системы РКІ (ЛАН Крипто)	
16.30 – 16.50	<i>Перерыв.</i>
18.15 – 19.00	Компании «ЛАН Крипто» 10 лет. Лебедев А.Н. президент
19.00 – 23.00	<i>Юбилейный вечер «ЛАН Крипто»</i>

ДЕНЬ ТРЕТИЙ: 3 февраля, воскресенье

9.20 – 10.00	<i>Завтрак.</i>
10.00 – 11.30	Презентации компаний-разработчиков.
10.00 – 10.30	Microsoft (Д. Вишняков)
10.30 – 11.00	ЛАН Крипто (О. Лебедев)
11.00 – 11.30	Aladdin (С. Груздев)
11.30 – 12.00	<i>Перерыв. Чай, кофе, ...</i>
12.00 - 13.45	Презентации компаний-разработчиков.
12.00 – 12.30	Диалог-Наука (С. Антимонов)
12.30 – 13.00	ООО «Крейф» (Д.А. Гергер)
13.00 – 13.30	АО «ЭлиПС» (А. Воеводин)
13.30 – 13.45	BioLink (А. Галицкий)
13.45 – 14.15	Методы современной стеганографии. (Профессор Мельников Ю.Н., Егоров А.Е.)
14.15 – 15.00	<i>Обед.</i>
15.00 – 15.30	Научно-методическое обеспечение подготовки специалистов по математической и компьютерной криптологии. Харин Ю.С., д.ф.-м.н., профессор, завю кафедрой, Агиевич С.В., к.ф.-м.н., доцент
15.30 – 16.00	Математические основы надежности цифровой подписи. Схмаев И.А., д.ф.-м.н.
16.00 – 16.20	Проблемы защиты учрежденческих АТС с функцией DISA. Лысенко Ю., Global One
16.20 – 16.35	Телефонные аппараты с абонентским шифрованием Сотов А., АО «ФРАКТАЛ»
16.35 – 17.00	<i>Перерыв. Чай, кофе, ...</i>
17.00 – 18.00	«ElcomSoftAdobe» - конфликт технологии и закона. Каталов А., президент ElcomSoft, Складов Д., программист
18.00 – 18.15	Закрытие конференции «РусКрипто 2002» Волчков А.А., президент Ассоциации «РусКрипто»
18.15 – 19.00	<i>Ужин.</i>
19.00	<i>Отъезд в Москву.</i>