Программа конференции «РусКрипто2003»

30 Января, четверг

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

ДЕНЬ ПЕРВЫЙ: 31 января, пятница

9.00 – 10.00	*Завтрак*
10.00 – 10.10	**Открытие конференции**.
10.10 – 10.55	**Основные достижения теоретической криптологии в 2002 году** (по материалам международных конференций CRYPTO, EUROCRYPT и др.) *Жуков А. Е., к.ф.-м.н., доцент МГТУ, директор ассоциации «РусКрипто»* Новые результаты по стойкости криптографических систем. Перспективные направления в криптографии. Приложения для бизнеса
10.55 – 11.30	**О ходе конкурса на новые европейские криптографические стандарты "CryptoNESSIE"** *Лебедев А. Н., к.ф.-м.н., президент «ЛАН Крипто», директор ассоциации «РусКрипто»* Какими будут новые европейские стандарты К чему готовится российским производителям Перспективы развития стандартов цифровой подписи в Европе
11.30 – 12.00	*Перерыв. Чай, кофе.*

Инфраструктуры открытых ключей (PKI). Международный и российский опыт.

Вопросы к обсуждению: Какие системы PKI реально востребованы в России. Есть ли перспективы у публичных удостоверяющих центров. Корпоративные удостоверяющие центры практический опыт. Российские стандарты и стандарты международные – как совместить "полезное с приятным". Решения для пользователей.

12.00 – 12.30	**Опыт создания и эксплуатации PKI в Канаде.** *Шефановский Д.Б. Компания «Демос», эксперт по криптографии.* Формирование требований к системам PKI Принципы регулирования и саморегулирования Действующая инфраструктура PKI развитого государства.
12.30 – 13.00	**О практике, рисках и обычаях использования электронных подписей.** *Дзержинский Ф. Я., Банк «Российский кредит», начальник отдела.* Применение электронных подписей (ЭЦП и АСП): подход на основе управления рисками. Юристы и программисты. Обычаи делового оборота и электронные подписи в международной практике. Международные документы, как источник сведений об этих обычаях. Директива Евросоюза и типовой закон ЮНСИТРАЛ об электронной подписи.
13.00 – 13.30	**Требования к иерархической системе PKI масштаба государства.** (на примере рабочего проекта PKI для Индии). *Волчков А.А., президент ассоциации «РусКрипто».* Требования к крупномасштабным иерархическим системам PKI. Техника, технология и методология построения. Проблемы проектирования и внедрения
13.30 – 15.00	*Обед*

Инфраструктуры открытых ключей (PKI). Российский и международный опыт (продолжение).

15.00 – 15.25	**Опыт создания и модернизации корпоративного Центра Сертификации компании «Русский алюминий»** *Лебедев А.Н., президент компании «ЛАН Крипто»* Работа единого Центра Сертификации с программами разных производителей. Опыт внедрения и модернизации.
15.25 – 15.45	**Система электронного документооборота с гарантированной доставкой сообщений на базе системы PKI. Практический опыт.** *Сухоруков А.В. вице-президент НП "Фондовая биржа РТС".* Опыт использования цифровой подписи в биржевой системе и электронном документообороте Практика работы с системой регистрации сертификатов. Бизнес приложения. Стратегия развития и расширения системы.
15.45 – 16.05	**Вопросы обеспечения информационной безопасности инфраструктуры открытых ключей.** *Попов В.О. к.ф.-м.н, компания «КриптоПро», ведущий специалист.* Требования по безопасности к созданию и работе программ PKI.
16.05 – 16.30	**Нужны ли системы PKI** *Иванов А.Г., к.ф.-м.н., директор ассоциации РусКрипто, эксперт по системам цифровой подписи.* Разновидности систем цифровой подписи – не все подписи одинаково полезны. Востребованы ли сегодня системы PKI. Кому нужны системы PKI? Производителям или потребителям. Как жить без удостоверяющих центров? Альтернативные системы управления цифровыми подписями. Корпоративным пользователям выгодно применять простые технологии.
16.30 – 17.00	*Перерыв. Чай, кофе.*

Инфраструктуры открытых ключей (PKI). Российский и международный опыт (продолжение).

17.30 – 18.00	**Характеристики промышленных систем PKI** *Огородников Д.В., «Инфосистемы Джет», зам. нач. отдела*. Основные особенности промышленных систем PKI. Сравнительные характеристики. Что необходимо потребителю, варианты решений.
18.00 – 18.30	**Организация инфраструктуры PKI предприятия на базе Unicert.** *Ляшенко В.В., «Компьюлинк», нач. отдела информационной безопасности*. Технические проблемы развертывания промышленных систем PKI. Опыт компании по внедрению инфраструктуры PKI.
19.30 – 23.00	*Официальный ужин. Знакомство участников конференции*

ДЕНЬ ВТОРОЙ: 1 Февраля, суббота

9.00 – 10.00	*Завтрак*
10.00 – 10.20	**Приведение российского законодательства в области ИТ, в частности, в области защиты информации, в соответствие с общепринятыми международными стандартами.** *Церенов Ц.В., Министерство экономического развития РФ, начальник департамента.* Новые инициативы министерства по дерегулированию экономики. Теперь и в области информационных технологий. Что ждать производителям и потребителям. Программа «Электронная Россия» в 2003 году.
10.20 – 10.40	**Что и как регулируется в области криптографии и цифровой подписи в России.** *А. Шадрин. Фонд «Новая экономика», эксперт.* Полный обзор всех действующих нормативных актов РФ в области защиты информации (с комментариями). Концепция изменения регулирования в области защиты информации и информационных технологий, разработанная по заказу Минэкономики РФ. Свежий взгляд на регулирование информационных технологий.
10.40 – 11.00	**Изменение нормативно-методической базы в области технической защиты информации.** *Калайда И.А., Гостехкомиссия России, зам. Начальника отдела лицензирования.* Самые свежие нормативные документы по технической защите информации. С 2004 года изменяется порядок сертификации средств защиты информации в системе Гостехкомиссии РФ. Как готовиться Гостехкомиссия к изменениям системы сертификации в 2003 году. Когда в России будут признавать международные сертификаты IT SEC. Нужны ли пользователям конфиденциальной информации лицензии.
11.00 – 11.30	**Круглый стол «Практические последствия от принятия новых законов “О лицензировании …”, “Об ЭЦП” и иных нормативных актов для потребителей и поставщиков средств защиты информации».** Электронный документ и цифровая подпись в новом арбитражном процессуальном кодексе (комментарии юристов). Электронный документ как доказательство в суде. Юридические риски при попытках соблюдения закона об ЭЦП. Предложения рабочей группы Совета Федерации по изменению в законах «Об ЭЦП» и «О лицензировании …». Персональные данные и конфиденциальная информация. Законодательные инициативы, какой следующий шаг. **Ведущая** *Соловяненко Н.И, директор ассоциации «РусКрипто», к.ю.н., с.н.с. Института государства и права РАН*. **Участвуют:** *Волков П.М. - Минэкономики РФ, юридический департамент, начальник отдела, Волчинская Е.К. – советник комитета по безопасности ГД РФ* *Левенчук А.И. – эксперт комитета по промышленной политике СФ РФ* *Терещенко Л.К. – с.н.с. Института законодательства и сравнительного правоведения при правительстве РФ*.
11.30 – 12.00	*Перерыв. Чай, кофе.*
12.00 – 13.30	**Круглый стол «Практические последствия принятия новых законов «О лицензировании …», «Об ЭЦП» и иных нормативных актов для потребителей и поставщиков средств защиты информации (продолжение).**
13.30 – 15.00	*Обед*

Секционные заседания (15.00 -18.00).

Секция 1. Практика создания систем информационной безопасности **Ведущий** *Микулич Н.Д.,* *директор ассоциации «РусКрипто»*	Секция 2: Теоретические вопросы криптологии **Ведущая** *Пудовкина М.А.,* *директор ассоциации «РусКрипто»*
Электронное казино. *Иванов А.Г., к.ф.-м.н. эксперт «ЛАН Крипто».* Как заработать денег на криптографии в виртуальном пространстве.	**Алгоритм ГОСТ 28147-89 ненадежен.** *Калядин О.А., эксперт «ЛАН Крипто».* Алгоритм ГОСТ 28147-89 допускает практическую подделку контрольных сумм (имитовставок). ГОСТ нельзя использовать для подтверждения подлинности сообщений.
Практика использования средств защиты информации в корпоративных системах документооборота. *Митричев И.В., зам. Ген. Директора АО "РФК", директор ассоциации «РусКрипто».* Практика – это живая комбинация решений технических, организационных, юридических, эргономических и даже психологических.	**Создание высокоскоростных шифров.** *Молдовян Н.А., д.т.н., профессор,ГУП СЦПС «Спектр», директор ассоциации «РусКрипто».* Построение современных шифров с гибкой схемой – теоретические основы.
Защищенная операционная система ALT LINUX *Смирнов А.В., ген. директор ALT LINUX* Версия ОС сертифицирована Гостехкомиссией РФ, готова к применению. Криптография - в ядре операционной системы.	**Булевы функции в криптографии** *Жуков А.Е., к.ф.-м.н., доцент МГТУ, директор ассоциации «РусКрипто».* Описываются основные свойства булевых функций наиболее важные для криптографии. Что нужно знать и уметь криптологу, опыт преподавателя МГТУ.
Аппаратная реализация высокоскоростного алгоритма шифрования. *Молдовян Н.А., д.т.н., профессор,ГУП СЦПС «Спектр», директор ассоциации «РусКрипто».* Новая микросхема, реализующая алгоритм шифрования данных. Опыт разработки.	**Многозначные гомоморфизмы автоматов.** *Быков А.В., Ин-т Криптографии Академии ФСБ РФ.* Делается важный шаг в классификации устройств шифрования как конечных автоматов.
	Новые результаты криптографических исследований в БГУ (г. Минск). *Харин Ю.С., д.ф.-м.н., профессор, зав. кафедрой БГУ* *Костевич А.Л., к.ф.-м.н., вед. н.с.*
16.30 – 17.00 *Перерыв. Чай, кофе.*	
Секция 1. **Практика создания систем информационной безопасности** **Ведущий** *Варфоломеев А.А., к.ф.-м.н.,* *директор ассоциации «РусКрипто»*	**Секция 2:** **Теоретические вопросы криптологии** **Ведущий** *Молдовян Н.А., д.т.н.,* *директор ассоциации «РусКрипто»*
Новые разработки ГЦБИ республики Беларусь. *Микулич Н.Д., начальник отдела ГЦБИ РБ.* Практические реализации национальных стандартов. Аппаратные системы идентификации – действительно удобно, дешево и надежно.	**Анализ алгоритмов шифрования**. *Пудовкина М.А., МИФИ,* *директор ассоциации «РусКрипто»* Результаты анализа несколько популярных алгоритмов шифрования. Все ли из них можно использовать.
Метод построения программно-физического датчика случайных чисел. *Амербаев В.М., Зверев Е.М., Шарамок А.В., ГУП НПЦ "СПУРТ" (г. Зеленоград).* После опубликования алгоритмов шифрования датчик случайных чисел остается наиболее удобной точкой для встраивания "потайных ходов" в криптосистемы.	**Помехоустойчивое кодирование мультимедийных данных в реальном масштабе времени.** *Герасименко В.Г., Тупота В.И., Тупота А.В., НИИ Гостехкомиссии РФ (г. Воронеж).* Рассматриваются методы поточного кодирования данных на основе вычислений в конечных полях. Обсуждается их применение в радиоканалах.
Новый быстрый алгоритм кодирования для процессора Intel Pentium III – IV. *Калядин О.А., эксперит "ЛАН Крипто"* Кодировать данные со скоростью 1Gb в секунду можно программой!	**Построение системы защиты данных в ЭПС на основе субъектно-объектной модели.** *Мельников Ю.Н., д.т.н., Теренин А.А., МЭИ.* В терминах субъектно-объектной модели формулируются требования к системе защиты данных
	Методы анализа искажений графических контейнеров, вносимых стеганографическими системами. *Аграновский А.В., Жижелев А.В., ГНУ НИИ "Спецвузавтоматика" (г. Ростов-на-Дону).*
18.30 – 19.30	*Ужин*
19.30 – 21.30	*Вечер авторской песни.*

ДЕНЬ ТРЕТИЙ: 2 Февраля, воскресенье

9.00 – 10.00	*Завтрак*
10.00 – 11.00	**Безопасность – новая стратегическая задача компании.** *Мамыкин В.Н., представитель компании Microsoft в Москве.* Ровно через два дня после завершения конференции «РусКрипто 2002» Билл Гейтс провозгласил обеспечение безопасности стратегическим направлением в деятельности компании Microsoft.
11.00 – 11.30	**Технология защиты информации "ЛАН Крипто"- от корпоративных стандартов, до прикладных программ и нормативных документов.** Лебедев А.Н., президент "ЛАН Крипто". Выйдя на российский рынок средств защиты информации в декабре 1991 года, компания "ЛАН Крипто" все эти годы неукоснительно следует принципу: "Поставлять только надежные средства защиты информации, открытые для любой экспертизы, и полностью отвечать перед любым заказчиком за их качество". Мы открыто и честно смотрим в глаза всех своих клиентов!
11.30 – 12.00	*Перерыв. Чай, кофе.*
12.00 – 12.30	**Электронные ключи eToken как средство защиты персональных данных и многофакторной аутентификации.** *Груздев С.Л., генеральный директор компании "Аладдин".* Пионер в продвижении на рынок USB-устройств хранения персональных данных и защиты программ остается верен себе, расширяя их возможности и сферы применения.
12.30 – 13.00	**Новые решения DrWeb для корпоративного и индивидуального пользователя.** *Скида М.А., менеджер компании "ДиалогНаука".* Новое поколение компьютерных вирусов и других опасных программ требуют и новых средств борьбы с ними. Пионер отечественного антивирусного движения находит достойные ответы на самые актуальные проблемы любого заказчика.
13.00 – 13.30	**Телефонные аппараты с надежным абонентским шифрованием.** *Ильинский О.В., Сотов А.А., ЗАО НПО "Квазар".* Теперь действительно надежная защита телефонных переговоров на всем пути от абонента до абонента становится реальностью не только для пользователей специальных сетей, но и для широких масс абонентов сотовой связи.
13.30 – 15.00	*Обед*
15.00 – 15.30	**Технология создания интегрированной системы информационной безопасности.** *В.В. Цибин. ЗАО НПП "БИТ"* Взгляд системного интегратора на информационную безопасность. Как оформить комплект документов на систему защиты информации, так, чтобы у Вас не было проблем. Опыт Российского рынка по интегрированным системам информационной безопасности.
15.30 – 16.00	**Анализ системы защиты документов в Microsoft Office XP.** *Малышев А.Е., старший программист ООО "Элкомсофт".* Информация из первых рук о том, как выглядит система защиты документов в Microsoft Office XP с точки зрения профессионала. Есть ли надежные системы защиты.
16.00 – 16.30	**Полная победа в борьбе с DMCA в США. А что нас ждет в России?** *Моцный И.Н. юрист компании "ЭлкомСофт".* Уникальный опыт компании в борьбе за свои права в судах США. Кем и какие аналоги этого закона готовятся в РФ.
16.30 – 17.00	*Перерыв. Чай, кофе.*
17.00 – 17.30	**Из истории криптологии. Проект «Венона».** Сырков Б.Ю., независимый эксперт Советская разведка и ответ США. Уникальная информация от автора книги. Ответы на вопросы.
17.30 – 17.45	**Закрытие конференции.**
18.00 – 19.00	*Ужин*
19.00	*Отъезд в Москву*.