Программа конференции «РусКрипто 2004»

ДЕНЬ ПЕРВЫЙ: 30 января, пятница

9.00 – 10.00	**Завтрак**
10.00	**Открытие конференции.**
10.00 – 10.20	**Отчет о работе ассоциации “РусКрипто” в 2003 году и подготовке к конференции EUROCRYPT 2006** *По инициативе ассоциации «РусКрипто» международная конференция EUROCRYPT 2006 пройдет в Санкт-Петербурге в мае 2006 года. Ассоциация «РусКрипто» объявляет конкурс на открытые стандарты защиты информации* Волчков А. А. – президент ассоциации “РусКрипто”
10.20 – 11.30	**Основные достижения теоретической криптологии в 2003 году (по материалам международных конференций CRYPTO’2003, EUROCRYPT’2003, ASIACRYPT’2003 и др.)** Жуков А.Е., к.ф.-м.н., доцент МГТУ им. Баумана, директор ассоциации “РусКрипто” Варфоломеев А.А., к.ф.-м.н., доцент МИФИ, директор ассоциации “РусКрипто” Иванов А.Г. – к.ф.-м.н., директор ассоциации “РусКрипто”
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.40	**Технологии безопасности в продуктах компании Microsoft. Настоящее и будущее.** *Компания Microsoft предлагает использовать все более широкие возможности операционной системы по обеспечению безопасности. Что планирует компания представить на суд пользователей в ближайшее время.* Мамыкин В.Н. – менеджер по информационной безопасности российского представительства компании Microsoft
12.40 – 13.00	**Современные тенденции развития криптографических технологий в Республике Беларусь.** Микулич Н.Д., Комисаренко В.В., Государственный центр безопасности информации При Президенте Республики Беларусь
13.00 – 13.30	**Методика создания систем информационной безопасности крупных телекоммуникационных компаний.** *В 2003 году компанией “ЛАН Крипто” разработаны единые принципы и методика построения систем информационной безопасности для крупнейших операторских компаний. Полученные результаты позволили разработать концепции обеспечения информационной безопасности для нескольких российских операторов связи.* Лебедев А.Н., к.ф.м.н. президент компании “ЛАН Крипто”
13.30 – 15.00	***Обед***
15.00 – 16.30	**Защита корпоративных сетей и распределенных баз данных** *Корпоративные сети компаний и их базы данных становятся объектами пристального внимания конкурентов и злоумышленников. Как надежно защитить себя от непрошенного вторжения чужаков в “частную жизнь” организации***.**
15.00 – 15.30	**Новые разработки компании “ДиалогНаука”** Антимонов С.Г., к.ф.-м.н., генеральный директор компании “ДиалогНаука”
15.30 – 16.00	**Аудит информационных систем – ожидания и результаты** *Как правильно оценить необходимость использования тех или иных механизмов защиты, что такое защищенность, как и в чем ее измерить.* Огородников Д.В., начальник отдела проектирования защищенных систем компании “Инфосистемы Джет”
16.00 – 16.30	**Построение и проверка путей сертификации. Современные тенденции** *Цифровые сертификаты – основа для многих систем цифровой подписи. В докладе представлены результаты исследований группы PKIX и разработчиков стандартов X.509 версии 5.* Шефановский Д.Б., эксперт по криптографии компании “Демос”
16.30 – 17.00	***Перерыв. Чай, кофе.***
17.00 – 18.00	**Защита корпоративных сетей и распределенных баз данных (продолжение)**
17.00 – 17.30	**Эволюция технологий обнаружения и предотвращения атак** *Дается экскурс в технологию обнаружения атак и анализируются пути ее развития. Говорится о новой технологии предотвращения атак, интеграции межсетевых экранов и систем обнаружения атак, об "интеллектуальных" технологиях слияния сканеров безопасности и систем обнаружения атак..* Лукацкий А.В., - руководитель отдела интернет-решений НИП "Информзащита"
17.30 – 18.00	**Создание виртуальных приватных сетей – основа защиты телекоммуникационной инфраструктуры** *Стратегия защиты телекоммуникационной инфраструктуры. Основные модули VPN. Стратегия разработки и внедрения VPN систем.* Шустиков Д.В. - ведущий разработчик компании “ЛАН Крипто”
19.30 – 23.00	***Официальный ужин. Знакомство участников конференции***

ДЕНЬ ВТОРОЙ: 31 января, суббота

9.00 – 10.00	**Завтрак**
10.00 – 13.30	**Секционные заседания.**

Секция 1. Теория и практика создания систем информационной безопасности	**Секция 2. Юридические аспекты разработки и внедрения систем информационной безопасности**
10.00 – 10.20 **Обратимые схемы и асимметричные преобразования. Один подход к изучению однонаправленности.** Жуков А.Е., - к.ф.м.н., доцент МГТУ, директор ассоциации “РусКрипто”	10.00 -10.25 **Совершенствование правового регулирования применения ИКТ (в том числе средств шифрования) и реализация ФЦП “Электронная Россия”.** Церенов Ц.В., руководитель департамента МЭРТ РФ
10.20 – 10.40 **Стандартизация форматов данных и параметров для взаимодействия средств различных производителей в инфрастуктуре открытых ключей.** Попов В.О., к.ф.-м.н., компания «Крипто Про»	10.25-10.50 **Изменение отечественной системы стандартизации в области защиты информации** Калайда И.А., заместитель начальника отдела Гостехкомисии РФ
10.40 – 11.00 **О поточных шифраторах с динамически меняющимся потоком шифрования.** Анашин В.С., д.ф.-м.н., РГГУ	10.50 – 11.10 **Нормативные документы с терминами и определениями по электронной цифровой подписи: формат сертификатов, списков отозванных сертификатов и т.д.** Микулич Н.Д., Комисаренко В.В., Государственный центр безопасности информации при Президенте Республики Беларусь
11.00 – 11.30 **Стеганография черно-белых изображений при помощи покрывающих кодов.** Кабатянский Г.А., д.ф.-м.н., ИППИ РАН	11.10-11.30 **Нормативная база, регулирующая использование систем защиты информации и цифровой подписи.** Волчков А.А., президент ассоциации “РусКрипто”
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.25 **О новых слабостях алгоритма шифрования RC4.** Пудовкина М.А., МИФИ, директор ассоциации “Рускрипто”	12.00-12.30 **Новое в законодательстве, регулирующем разработку и внедрение систем информационной безопасности.** Соловяненко Н.И., к.ю.н., Институт государства и права РАН, директор ассоциации “РусКрипто”
12.25 – 12.50 **О слабостях алгоритма поточного шифрования Rabbit** Пудовкина М.А., директор ассоциации “Рускрипто” Гавриков Ю.М. ., МИФИ	12.30 – 12.50 **Предложения по изменению регулирования деятельности по защите информации в “Концкпции реформирования отрасли ИКТ”, подготовленной МЭРТ РФ.** Смирнов К.В., фонд “Новая экономика”
	12.50-13.10 **Информационная безопасность и законодательство о госзакупках.** Волков П.М., начальник отдела МЭРТ РФ
12.50 – 13.30 **Новый подход к безусловной секретности в релятивистской квантовой криптографии.** Молотков С.Н., Институт физики твердого тела РАН.	13.10 – 13.30 **Информационная безопасность и коммерческая тайна** *Взаимосвязь нормативных документов.* Волчинская Е.К. к.э.н. советник комитета по безопасности ГД РФ
13.30 – 15.00	***Обед***
15.00 – 15.20 **Методика эффективного перебора паролей на основе моделирования действий пользователя.** Иванов А.Г., к.ф.-м.н., директор ассоциации “РусКрипто” Калядин О.А. , компания “ЛАН Крипто”	**Круглый стол: «Проблемы информационной безопасности в современном законодательстве и правоприменительной практике»** *Работает ли законодательство об информационной безопасности (в частности закон ” Об ЭЦП”) Что в законодательстве об информационной безопасности сегодня более всего мешает бизнесу? К чему бизнес сумел приспособиться и каким образом? Что предпочтительнее: переписать закон об ЭЦП или закрепить достигнутые результаты, если такие имеются?)* Участвуют: Волков П.М., Волчинская Е.К., Волчков А.А., Лебедев А.Н., Смирнов К.В., Соловяненко Н.И.
15.20 – 15.40 **Исследования российских криптографических алгоритмов в Java-картах в целях защиты данных приложений.** Елькин А.В., Конопля А.А., НТЦ “Атлас” Фомичев Н.В., МИФИ	
15.40 – 16.00 **Вопросы безопасности некоторых протоколов мобильных платежей в точке обслуживания.** Варфоломеев А.А., к.ф.-.м.н. компания “Андэк” Жирнов О.А., компания “КриптоЭкс” Устюжанин Д.Д., компания “Вымпелком”	
16.00 – 16.30 **Перспективные направления криптографии – основа обеспечения информационной безопасности.** Молдовян А.А., к.т.н., Молдовян Н.А., д.т.н. СЦПС “Спектр”	
16.30 - 17.00	***Перерыв. Чай, кофе.***
17.00 – 17.20 **Методика построения защищенной платежной сети на**	**Круглый стол. Продолжение.**

основе многокритериальной оптимизации. Мельников Ю.Н., д.т.н., профессор, Теренин А.А., МЭИ	
17.20 – 17.40 **Модулярная модификация криптоалгоритма Хелмана и ее криптоанализ** Зверев Е.М., Амербаев, компания “Спрут” Бияшев “Институт проблем информатики” (Алматы)	
17.40 – 18.00 **Криптографические механизмы защиты информации в СВТ**. Заболотный А.П., Костин А.А., Фахрутдинов Р.Ш., СЦПС “Спектр” (С.-Пб.)	
18.00 – 18.30 **Некоторые сравнительные характеристики российских платежных систем**. Мельников Ю.Н., д.т.н., профессор, Харченко А.С., МЭИ	
18.30 – 19.30	***Ужин***
19.30 – 21.30	***Вечер авторской песни.***

ДЕНЬ ТРЕТИЙ: 1 февраля, воскресенье

9.00 – 10.00	**Завтрак**
10.00 – 11.30	**Практическая реализация атак на защищенные данные и программные системы** *Встроенные в операционные системы механизмы защиты. Криптография, которая приходит к Вам от поставщика интегрированных систем. Какова ее надежность. Возможно ли провести анализ и оценить качество.*
10.00 – 10.30	**Анализ уявзвимостей Microsoft Protected Storage** *Система Protected Storage – здесь хранятся Ваши пароли, которые Вы используете при работе с Windows, а также и другая жизненно важная информация. Надеждно ли она защищена. Работа этого сервиса на примере паролей к MS Internet Explorer.* Андрей Малышев, компания «Элкомсофт», аналитик
10.30 – 11.00	**Реконструкция криптографических протоколов** *Защита уже реализована в вашей системе, но Вы не знаете, что лежит в ее основе, можно ли ей доверят. Выход один – анализировать готовую программу. Способы реконструкции примененных криптографических алгоритмов на основе анализа бинарного кода программы.* Дмитрий Скляров, компания «Элкомсофт», аналитик
11.00 – 11.30	**Построение, анализ и примеры уязвимостей систем защиты ПО. Применение современной криптографии** *Защита программного обеспечения от тиражирования. Возможно ли построение надежной системы. Как использовать проверенные методы криптографии в этой области. Слабости и взлом систем защиты. "Черный ход" к конфиденциальной информации* Станислав Винокуров, компания "SmartLine, Inc", эксперт по безопасности
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 13.00	**Платежные системы. Надежность защиты** *Практический опыт специалистов показывает, что взломщику достаточно даже намека на слабость системы, чтобы начать атаку. Какие механизмы защиты реализованы в платежных системах. Как бороться с мошенниками.*
12.00 – 12.30	**Борьба с мошенничествами по пластиковым картам в банковской сфере. Методы и практический опыт** *Богатый практический опыт по расследованию и предотвращению мошенничеств в крупном розничном банке.* Петрусевич А.Г. , независимый эксперт
12.30 – 13.00	**Обзор механизмов защиты в системах микроплатежей.** *На Российском рынке представлены различные платежные системы для организации микроплатежей. Незначительность переводимых сумм не исключает возможность масштабных мошенничеств. В докладе представлен обзор механизмов защиты м наиболее популярных системах.* Митричев И.В., компания "РФК", директор ассоциации "РусКрипто" (doc-zip – 33Kb)
13.00 – 13.30	**Анализ уязвимостей и возможностей вскрытия протоколов сотовой связи.** *Доклад о механизмах защиты, реализованных в сетях GSM (GPRS, WAP, WLAN) и возможности их взлома. Можно ли прослушать Ваш мобильный телефон или дистанционно управлять им? Это не просто теоретическое рассмотрение вопроса, но и обобщение богатого практического опыта.* Шашков Н.Л., менеджер по фроду компании ОАО "Вымпелком".
13.30 – 15.00	***Обед***
15.00 – 17.30	**Презентации разработчиков**
15.00 – 15.30	**ИНДИС – универсальная платформа защиты распределенных данных** *Единый подход к защите данных на серверах и рабочих станциях корпоративных и локальных сетей. Прозрачное кодирование данных. От «коробочных» решений до распределенных систем.* Соколов Д.В. –технический директор компании "ЛАН Крипто",
15.30 – 15.45	**О целях и задачах нового комитета по информационной безопасности АРБ и возможных областях сотрудничества с Ассоциацией РусКрипто** Велигура А.Н., председатель комитета по информационной безопасности АРБ.
15.45 – 16.15	**ruToken - российское средство аутентификации** *Надежная аутентификация – насущная необходимость. Интеллектуальные карты обеспечивают ее, но какой ценой, стоимость решения высока. RuToken – реальная альтернатива.* Иванов В.Е., начальник службы техничкой поддержки компании "Актив" (pdf-zip – 190KB; ppt-zip – 4.6Mb; материалы – pdf-zip – 1.2Mb)
16.15 – 16.45	**Средства защиты телефонных переговоров и передачи данных.** Ильинский О.В., ведущий разработчик компании "Квазар"
16.45 – 17.15	**Аутентификация. Проблемы и решения.** Груздев С.Л. генеральный директор компании "Алладин" (doc-zip – 6Kb)
17.15 – 17.45	**Современные способы и средства защиты от вредоносных программ.** Резник Г.К., к.т.н., коммерческий директор ОДО "ВирусБлокАда" (г. Минск)
17.45 – 17.50	**Закрытие конференции.**
18.00 – 19.00	***Ужин***
19.00	**Отъезд в Москву.**