Программа конференции «РусКрипто2005»

ДЕНЬ ПЕРВЫЙ: 4 Февраля, Пятница

9.30 – 10.00	**Завтрак**
10.00	**Открытие конференции.**
10.00 – 10.15	**О работе ассоциации «РусКрипто» и подготовке к конференции EUROCRYPT 2006.** Волчков А. А., президент Ассоциации «РусКрипто», Лебедев А.Н., директор Международной Ассоциации IACR.
10.15 – 10.25	**Приветствие «РусКрипто» от имени Международной Ассоциации Криптологических Исследований IACR (International Association for Cryptologic Research).** Эндрю Кларк (Великобритания) – президент Международной ассоциации IACR.
10.25 – 11.30	**Основные достижения теоретической криптологии в 2004 году** (по материалам международных конференций CRYPTO, EUROCRYPT, ASIACRYPT, INDOCRYPT, FSE 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., эксперт «ЛАН Крипто», директор Ассоциации «РусКрипто», Пудовкина М.А., к.ф.-м.н., доцент МИФИ, директор Ассоциации «РусКрипто».
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.40	**Технологии безопасности в продуктах компании «Майкрософт». Настоящее и будущее.** *Компания предлагает использовать все более широкие возможности своей операционной системы по обеспечению безопасности. Что же планируется представить на суд пользователей в ближайшее время.* Мамыкин В.Н., менеджер по информационной безопасности компании «Майкрософт».
12.40 – 13.05	**О новых решениях компании Cisco в области информационной безопасности.** *Расскажет наиболее компетентный в данном вопросе в российском представительстве компании* Лукацкий А.В., Security Business Development Manager, Cisco Systems Russia and CIS.
13.05 – 13.30	**Сертификация в области защиты информации: мифы и реальность.** *За прошедшие 13 лет в России произошло много изменений в отношении к сертификации средств защиты информации, в частности, средств криптографической защиты. Кто и как нас обманывал и каково реальное положение дел сегодня.* Лебедев А.Н., к.ф.-м.н., с.н.с., директор Ассоциации «РусКрипто».
13.30 – 15.00	***Обед***
15.00 – 15.25	**Криптографические свойства булевых преобразований.** *За все время существования стандарта шифрования данных ГОСТ 28147 его важнейшие параметры, так называемые «блоки замены», так и не были официально определены. Как выбрать их правильно и каковы последствия неправильного выбора. На основании теоретических результатов, опубликованных в открытой печати, будет сделана попытка найти оптимальное решение для важной практической задачи криптографии.* Жуков А.Е., к.ф.-м.н., доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто».
15.25 – 15.45	**Вопросы создания и внедрения средств криптографической защиты информации.** *Разработка и применение средств криптографической защиты информации сопряжены с анализом ряда задач, без решения которых невозможно построение надежной системы криптографической защиты информации.* Микулич Н.Д., начальник отдела Государственного центра безопасности информации при Президенте Республики Беларусь, директор Ассоциации «РусКрипто».
15.45 – 16.10	**Тенденции развития технологии электронной цифровой подписи в Республике Беларусь.** *Тенденции развития технологии ЭЦП в Республике Беларусь.Возможность юридически значимого применения ЭЦП для подтверждения подлинности электронных документов в Белоруссии была подтверждена принятием Закона «Об электронном документе» в январе 2000 года, раньше чем в США, ЕС и России.* *Какова ситуация с применением технологии ЭЦП в Республике Беларусь сегодня?* Комисаренко В.В., начальник группы Государственного центра безопасности информации при Президенте Республики Беларусь, директор Ассоциации «РусКрипто».
16.10 – 16.30	**Теория и практика построения защищенных систем хранения информации.** *Специалист-разработчик расскажет об опыте создания программного комплекса защиты данных на основе специально разработанных криптографических алгоритмов.* Бутакова М.В., программист-разработчик компании «ЛАН Крипто», студентка МИФИ.
16.30 – 17.00	***Перерыв. Чай, кофе.***
17.00 – 17.20	**Чем опасен «криптопровайдер»?** *Увлечение в последние годы техникой так называемых «криптопровайдеров» для построения программных средств защиты информации далеко не так безобидно, как это может показаться на первый взгляд.* Калядин О.А., Иванов А.Г., к.ф.-м.н., эксперты-криптографы Ассоциации «РусКрипто».
17.20 – 17.40	**О методах испытаний программных средств криптографической защиты информации.** *Серьезным опытом практической работы в этом направлении поделятся сотрудники Учреждения Белорусского государственного университета – «Национального научно-исследовательского центра прикладных проблем математики и информатики»* Костевич А.Л., к.ф.-м.н., в.н.с., Агиевич С.В., к.ф.-м.н., доцент БГУ.

17.40 – 18.00	**Защита информационных ресурсов в процессе эксплуатации информационной системы.** *Уникальным практическим опытом в этом на российском рынке корпоративных информационных систем и систем государственных организаций поделится крупнейший специалист в данной области* Трифаленков И.А., директор Центра информационной безопасности «Инфорсистемы Джет»
18.00 – 18.30	**Анализ защиты Scratch-карт и аудит процесса их производства.** *Автор самого интересного доклада конференции «РусКрипто 2004» представит некоторые свои новые результаты наблюдений и анализа.* Шашков Н.Л., главный эксперт по управлению фродом и гарантированию доходов компании «Вымпелком»
18.30 – 19.15	**«Johnny Walker» в России: проверка криптографической стойкости.** *Прошлогодняя проверка на конференции «РусКрипто 2004» показала, что для уточнения результатов «нужны дополнительные исследования».* Представители марки «Johnny Walker» в России.
19.30 – 23.00	***Ужин. Знакомство участников конференции..***

ДЕНЬ ВТОРОЙ: 5 Февраля, Суббота

9.30 – 10.00	***Завтрак***
10.00 – 13.30	**Секционные заседания.**

Секция 1. Теория и практика создания систем информационной безопасности.	**Секция 2. Юридические база разработки и внедрения систем информационной безопасности.**
10.00 – 10.30 **Обзор методов «организации скрытых каналов» (information hiding).** *Понятный обзор основных идей и результатов крайне интересного нового направления информационной безопасности дается ведущими российскими специалистами в этой области.* Грушо А.А., д.ф.-м.н., профессор МГУ им. М.В. Ломоносова и РГГУ, Тимонина Е.Е., к.ф.-м.н., доцент РГГУ	10.00 - 10.30 **Концепция архитектуры электронного государства.** *Будет предпринята попытка дать цельную картину того, что нас ожидает (или может ожидать) в ближайшие годы «цифрового будущего».* Левенчук А.И., генеральный директор «Техинвестлаб»
10.30 – 10.50 **О реализации методов подсчета количества точек эллиптических кривых над конечным полем.** *Молодой исследователь представляет свои результаты по данной теме.* Гилев А.М., студент МИФИ	10.30 - 10.50 **Аудит процессов государственного управления в рамках электронного государства.** *Концепция аудита, подходы и механизмы проведения негосударственными организациями независимого информационного аудита, принципы выделения бюджетных средств, баланс интересов граждан, бизнеса и государственных организаций.* Агроскин В.В., член Экспертного совета СФ России
10.50 – 11.30 **Криптографические системы типа RSA над кольцами алгебраических чисел.** *Представление оригинальных результатов ведущего российского специалиста в области алгебраических методов современной криптографии.* Глухов М.М., д.ф.-м.н., профессор (г. Москва)	10.50 - 11.10 **Информационное регулирование в электронном государстве.** Каптерев А.С., эксперт МЭРТ. 11.10 - 11.30 **Изменение регулирования ИТ Министерством связи и информатизации РФ в 2005 году.** Якушев М.В., директор юридического департамента Минсвязи и Информатизации
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.30 **О дизъюнктных кодах в криптографии.** *Ведущий специалист по теории кодов расскажет о своих новых результатах по каскадным дизъюнктным кодам с внутренним W-кодом и произвольным внешним q-ичным V-разделяющим кодом и о приложениях этих результатов в криптографии.* Сидельников В.М., д.ф.-м.н., ведущий научный сотрудник МГУ им. М.В. Ломоносова.	12.00 - 12.20 **Сравнительный анализ опыта развертывания Инфраструктуры открытых ключей (PKI) национального масштаба.** Болдырев А.В., эксперт Ассоциации «РусКрипто». 12.20 - 12.40 **Оценка эффективности инвестиций в информационную безопасность.** Волчков А.А., президент Ассоциации «РусКрипто»
12.30 – 12.50 **Безопасность криптосистем с короткими ключами** *(в свете Постановления Правительства РФ № 691 от 23.09.2002).* *Безопасные системы с короткими ключами возможны.* Варфоломеев А.А., к.ф.-м.н., доцент МИФИ, директор Ассоциации «РусКрипто».	12.40 - 13.00 **Техническое регулирование и экспортный контроль в области информационной безопасности.** *Действующие нормы и правила, проекты регламентов.* Калайда И.А., зам. начальника отдела Федеральной Службы Технического и Экспортного Контроля РФ.

12.50 – 13.10 **Использование уязвимости протокола Comp-128 v1. Программные и аппаратные методы атаки.** Гавриков Ю., Жданов Е., студенты МИФИ 13.10 - 13.30 **О групповых свойствах модификаций алгоритма RC4 и свойствах стандарта шифрования Кореи алгоритма SEED.** Пудовкина М.А., к.ф.-м.н., доцент МИФИ, директор Ассоциации «РусКрипто».	13.00 – 13.30 **Управление рисками электронного банкинга. Организация банковского регулирования и надзора в области Интернет-банкинга.** *Взаимосвязь нормативных документов ЦБ РФ и практических шагов Банка России с международной практики банковского регулирования.* Лямин Л.В., начальник отдела Интернет-банкинга Департамента банковского регулирования и надзора ЦБ РФ.
13.30 – 15.00	***Обед***
15.00 – 18.30	**Секционные заседания (продолжение)**
15.00 – 15.20 **Эффективная реализация операции умножения в группах точек эллиптической кривой.** *Ведущий российский специалист по оптимизации арифметических вычислений в криптографии представит свои новые результаты* Иванов А.Г., к.ф.-м.н., директор Ассоциации «РусКрипто».	15.00 – 16.30 **Круглый стол:** **Государственная власть и правовая база информационной безопасности.** *Использование электронных документов и электронной подписи.* *Административная реформа и закон «Об ЭЦП».* *Инициативы госорганов и потребности потребителей.* *Роль и место саморегулирующихся организаций.* **Ведущая:** Соловяненко Н.И., к.ю.н., с.н.с. Института государства и права РАН, директор Ассоциации «РусКрипто». **Участвуют:** Волков П.М., начальник юридического департамента МЭРТ, Агроскин В.В., член Экспертного совета СФ России, Волчков А.А., президент Ассоциации «РусКрипто», Каптерев А.С., эксперт МЭРТ, Лебедев А.Н., к.ф.-м.н., с.н.с., директор Международной Ассоциации IACR, Левенчук А.И., генеральный директор «Техинвестлаб», Якушев М.В., начальник юридического департамента Минсвязи и Информатизации.
15.20 – 15.40 **Применение методов теории автоматов для решения криптографических задач.** *Ведущий специалист в области применения теории автоматов для решения криптографических задач расскажет о своих новых результатах.* Бабаш А.В., д.ф.-м.н., зав. кафедрой РГСУ	
15.40 – 16.00 **Подходы к сокращению информации, необходимой для аутентификации различных сообщений на основе транзитивных и агрегированных подписей.** Лучник А.И., студентка МИФИ	
16.00 – 16. 20 **Криптографические алгоритмы на основе тригонометрических функций.** *Автор представляет оригинальные разработки криптографических алгоритмов, оценку стойкости которых он основывает на свойствах элементарных тригонометрических функций.* Сизов В.П., инженер ПО «Уралкалий» (г. Березняки)	
16.20 – 16.40 **Новые результаты по криптоанализу и синтезу шифров**. Мещеринов Е.А., эксперт-криптограф.	
16.30 – 17.00	***Перерыв. Чай, кофе.***
17.00 – 17.15 **Криптографические направления в научном филиале ФГУП НИИ "Вектор" – «Спектр» (С.-Пб.).** Молдовян А.А., к.т.н., доцент, Молдовян Н.А., д.т.н., профессор, специалисты ФГУП НИИ «Вектор» (С.-Пб.)	17.00 – 17.25 **Аналог собственноручной подписи для подтверждающих документов (АСППД).** Некоторые программно-инженерные аспекты электронных подписей. Дзержинский Ф.Я., нач. отдела Банка «Российский Кредит»
17.15 – 17.50 **Новая процедура проверки подписи в системе RSA.** Молдовян Д.Н., студент, Молдовян Н.А., д.т.н., профессор, специалисты ФГУП НИИ «Вектор» (С.-Пб.) **Синтез скоростных шифров на основе управляемых подстановочно-перестановочных сетей** Молдовян А.А., к.т.н., доцент, Молдовян Н.А., д.т.н., профессор, специалисты ФГУП НИИ «Вектор» (С.-Пб.)	17.25 – 17.50 **Технические средства защиты авторского права и криптография: что изменилось в законодательстве после судебной победы ЭлкомСофт в США.** *За что судили «ЭлкомСофт» в США и что изменилось в законах об охране интеллектуальной собственности в России и других странах с тех пор.* Моцный И.Н., юрист компании «ЭлкомСофт».
17.50 – 18.10 **Криптосистемы на общих эллиптических кривых, иммунные к канальным атакам.** Скобеев А.В., специалист ЗАО «Кубань-GSM» (Краснодар)	17.50 – 18.10 **О системе стандартов в области информационной безопасности организаций кредитно-финансовой сферы.** Велигура А.Н., к.ф.-м.н., Председатель Комитета АРБ.
18.10 – 18.30	18.10 – 18.30

Анализ современных подходов к использованию цифровых водяных знаков в ПО. Доля А.В., студент Ростовского Гос. Университета (Ростов-на-Дону)	**Регулирование экспорта криптографических технологий в РФ.** Лебедев А.Н., к.ф.-м.н., с.н.с., директор Международной Ассоциации IACR.
18.30 – 19.30	***Ужин***
19.30 – 22.00	***Вечер авторской песни.*** Выступают: почетный гость всех конференций «РусКрипто», начиная с 1999 года, ведущий специалист-психиатр Государственного научного центра социальной и судебной психиатрии им. В.П.Сербского Горячкин Е.А. и другие участники конференции, считающие себя способными выступить публично с пением. Традиционно обстановка на вечере крайне доброжелательная и непринужденная.

ДЕНЬ ТРЕТИЙ: 6 февраля, Воскресенье

9.30 – 10.00	***Завтрак***
10.00 – 10.20	**Аутентификация по паролю: недостатки и уязвимости программных реализаций.** *Оказывается, даже при самых стойких алгоритмах шифрования и ключах сколь угодно большой длины, несерьезные на первый взгляд огрехи в процедурах обработки и хранения паролей могут привести к весьма серьезным последствиям.* Беленко А.В., программист компании «ЭлкомСофт», студент МГТУ
10.20 – 10.40	**Новые разработки средств криптозащиты телефонных переговоров, сотовой связи, беспроводных соединений (Bluetooth) и др.** *Современные криптографические алгоритмы и протоколы и уровень развития элементной базы позволяют эффективно реализовать процедуры крипторафической защиты телефонных переговоров гарантированной стойкости, практически совсем не причиняя пользователям неудобства.* Ильинский О.В., директор ЗАО НПО «КВАЗАР»
10.40 – 10.55	**Обзор последних достижений биометрических методов аутентификации.** *Приближается момент, когда в паспорт каждого гражданина России будут внесены его биометрические данные. Что это будет означать для нас и что еще в запасе у технократов в этой области расскажет ведущий специалист по биометрике* Черномордик О.М., к.ф.-м.н., ген. директор ООО «Биометрические Технологии»
10.55 – 11.10	**Дактилоскопические сканеры с антимуляжной защитой.** *Новые приемы защиты от муляжей при сканировании отпечатков пальцев.* Хиценко Н.А., начальник отдела ООО «Биометрические Технологии»
11.10 – 11.30	**«Магия» - секретное англо-американское оружие в войне против Японии.** *Первая презентация новой работы автора таких известных книг по истории спецслужб и криптографии как «Радиошпионаж», «Погоня за Энигмой», «ВЕНОНА - самая секретная операция американских спецслужб»* Сырков Б.Ю., автор
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.25	**Надежная, удобная, проверенная практикой и сертифицированная технология зашиты данных и управления открытыми ключами.** *Результаты 13-летнего опыта практической работы компании на российском и международном рынке криптографических технологий позволяют нам уверенно говорить о том, что название доклада отражает основные существенные признаки технологии защиты информации «ЛАН Крипто»* Соколов Д.В., директор компании «ЛАН Крипто»
12.25 – 12.45	**Опыт и проблемы организации практической работы региональных удостоверяющих центров в условиях действующего законодательства России.** Афанасьев Г.Э., ген. директор ЗАО «Удостоверяющий центр» (г. Нижний Новгород)
12.45 – 13.05	**Технология защиты аппаратных ресурсов на основе разделения доступа.** *О новых разработках для решения классической задачи информационной безопасности расскажет их главный идеолог и автор* Оганесян А.К., ген. директор компании ЗАО «Смарт Лайн Инк.»
13.05 – 13.30	**Сравнительный анализ механизмов безопасности в системах дистанционного обслуживания клиентов: клиент-банк, интернет-банкинг, телефон-банк, SMS-банкинг.** *Рассматриваются наиболее распространенные механизмы организации подсистем безопасности при оказании банками услуг свои клиентам по дистанционному управлению счетом во взаимосвязи с организационно-юридическим обеспечением таких услуг. Сравниваются системы, базирующиеся на технологиях "толстый клиент", "тонкий клиент", голосовое (телефонное) обслуживание, SMS-банкинг.* Митричев И.В., заместитель генерального директора компании «РФК».
13.30 – 15.00	***Обед***
15.00 – 15.30	**Опыт внедрения смарт-карт и токенов в крупных проектах.** *В докладе рассматриваются тенденции развития мирового рынка смарт-карт в системах информационной безопасности предприятий, приводится российский опыт, рассматриваются технологии и продукты для единого входа и регистрации в системе(SSO), а также управления жизненным циклом "единой" корпоративной карты (Card Management System).* Груздев С.Л., генеральный директор компании «Aladdin».
15.30 – 16.00	**Программно-аппаратные средства защиты от вирусов и других вредоносных программ.**

	Презентацию новых продуктов самой опытной на российском рынке компании в области антивирусной защиты проведет ее бессменный лидер Антимомнов С.Г., к.ф.-м.н., председатель совета директоров АО «ДиалогНаука».
16.00 – 16.30	**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»
16.30 – 17.00	**Современные способы и средства защиты от вредоносных программ.** *Уникальный опыт работы компании на рынке средств защиты информации для государственных и коммерческих организаций Республики Беларусь может оказаться в чем-то полезным для разработчиков и пользователей средств защиты информации в других странах.* Резников Г.К., к.т.н., с.н.с., ген. директор, Барцевич Д.А., начальник отдела ОДО «ВирусБлокАда» (г. Минск)
17.00 – 17.20	**Инструментальные средства обеспечения безопасности RFID-технологий.** *Автор презентует результаты оригинальных отечественных разработок в области технологий создания таких современных средств обеспечения безопасности как радиоэлектронные метки, «интеллектуальная пыль» и т.п.* Кулаков И.А., генеральный директор компании «Random Art»
17.20 – 17.40	**Технологический аудит систем и модулей информационной безопасности.** *Новый взгляд на взаимосвязь качества информационных систем, реализации подсистем защиты информации и алгоритмов, положенных в основу программных и технических средств обеспечения безопасности.* Волчков А. А., президент Ассоциации «РусКрипто»
17.40 – 18.00	**Формирование оргкомитета конференции EUROCRYPT 2006.**
18.00 – 19.00	***Ужин***
19.00	**Отъезд в Москву.**

Резервные доклады.

Новые разработки компании в области криптографических средств защиты информации. Попов В.О., к.ф.-м.н., эксперт компании «КриптоПро»
Использование инструмента CASEBERRY для автоматической генерации политики разграничения прав доступа. Айдаров Ю.Р., аспирант, Пермский государственный университет