Программа конференции «РусКрипто2006»

ДЕНЬ ПЕРВЫЙ: 3 февраля, пятница (утро 9.30 – 15.00)

9.30 – 10.00	**Завтрак**
10.00 – 10. 15	**Открытие конференции** Волчков А.А. – президент ассоциации «РусКрипто»
10.15 – 10.30	**О подготовке конференции EUROCRYPT 2006** Лебедев А.Н. – директор Международной ассоциации IACR
10.30 – 11.00	**Основные достижения теоретической криптологии в 2005 году** Жуков А.Е. – к.ф.-м.н., доцент МГТУ им. Баумана, директор ассоциации «РусКрипто»
11.00 – 11.30	**Новые направления в криптографических протоколах и системах цифровой подписи** Варфоломеев А.А. – к.ф.-м.н., доцент МИФИ, директор ассоциации «РусКрипто»
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.45	**Технологии безопасности в продуктах компании Microsoft** *Новые функции операционной системы для обеспечения безопасности.* *Что же планируется представить на суд пользователей в ближайшее время.* Мамыкин В.Н. – директор по информационной безопасности компании Microsoft
12.45 – 13.30	**Обеспечение информационной безопасности в стандарте GSM** Волчков А.А. – эксперт ассоциации «GSM»
13.30 – 15.00	***Обед***

ДЕНЬ ПЕРВЫЙ: 3 февраля, пятница (вечер 15.00 – 23.00)

15.00 – 15.30	**Современное состояние стандартизации в области информационной безопасности** Калайда И.А. **–** вице-президент ассоциации «Евраас»
15.30 – 16.00	**Взаимосвязь классических рисков с рисками несанкционированного доступа к информации.** Болдырев А.В. – директор ассоциации «РусКрипто»
16.00 – 16.30	**Внедрение системы информационной безопасности на основе стандарта ISO 17799** Лебедев А.Н. – к.ф.-м.н., с.н.с., директор ассоциации «РусКрипто»
16.30 – 17.00	***Перерыв. Чай, кофе.***
17.00 – 17.20	**Контроль сетевого доступа (или как проверить соответствие тысяч узлов требованиям корпоративной политики безопасности при минимуме затрат)** Лукацкий А.В. – менеджер по развитию бизнеса компании «Cisco» в России и СНГ
17.20 – 17.45	**Современные методы обеспечения безопасности в международных платежных системах** Петрусевич А.Г. - независимый эксперт»
17.45 – 18.05	**О внедрении средств криптографической защиты для несекретной информации в Беларуси** Микулич Н.Д. – начальник отдела ГЦБИ при Президенте Республики Беларусь
18.05 – 18.30	**Реальное построение коллизий для наиболее известных функций хеширования** Иванов А.Г. **–** к.ф.-м.н., директор ассоциации «РусКрипто»
18.30 – 19.15	**«Johnny Walker» в России: проверка криптографической стойкости** *Прошлогодняя проверка на конференции «РусКрипто 2005» показала, что для уточнения результатов «нужны дополнительные исследования».* Представители марки «Johnny Walker» в России
19.30 – 23.00	***Ужин. Знакомство участников конференции.*** ***Вечерний Symposium.***

ДЕНЬ ВТОРОЙ: 4 февраля, суббота (утро 9.30 – 15.00)

<table>
<tr><td>9.30 – 10.00</td><td colspan="2">Завтрак</td></tr>
<tr><td>10.00 – 13.30</td><td colspan="2">Секционные заседания</td></tr>
<tr><td colspan="2">Секция 1. Организационные вопросы внедрения средств информационной безопасности</td><td>Секция 2. Теория и практика создания систем информационной безопасности</td></tr>
<tr><td colspan="2">10.00 – 10.30
О внесении изменений в законодательство по регулированию защиты информации и электронной подписи
Якушев М.В. – директор Департамента правового обеспечения Мининформсвязи РФ</td><td>10.00 - 10.30
Стохастическая компьютерная вирусология
Иванов М.А. – к.т.н., доцент кафедры «Компьютерные системы и технологии» МИФИ</td></tr>
<tr><td colspan="2" rowspan="2">10.30 – 11.00
Нормативное обеспечение систем информационной безопасности в ФЦП «Электронная Россия»
Черенов Ц.В. - заместитель директора Департамента корпоративного управления Минэкономразвития России</td><td>10.30 – 10.45
Методы обнаружения виртуальных дисков
Кузнецов А.А. – аспирант МГТУ</td></tr>
<tr><td>10.45 – 11.00
Комплексный анализ защищенности компьютерных систем
Ананьев А.П. – студент МИФИ</td></tr>
<tr><td colspan="2">11.00 – 11.30
Комментарии к предлагаемым изменениям в законы об электронной подписи и «об информации, информатизации и защите информации»
Соловяненко Н.И. - к.ю.н., директор ассоциации «РусКрипто»</td><td>11.00 - 11.30
Враждебные многоагентные системы и скрытые каналы
Грушо А.А. - д.ф.-м.н., профессор МГУ и профессор РГГУ
Тимонина Е.В. - к.ф.-м.н., доцент РГГУ</td></tr>
<tr><td>11.30 – 12.00</td><td colspan="2">Перерыв. Чай, кофе.</td></tr>
<tr><td colspan="2" rowspan="2">12.00 – 12.20
Проблемы правовой защиты персональных данных и конфиденциальной информации
Волчинская Е.К. – к.э.н., советник комитета по безопасности Государственной Думы РФ</td><td>12.00 - 12.20
Моделирование конечных автоматов с приложениями в криптографии
Бабаш А.В.– д.ф.-м.н., заведующий кафедрой РГСУ</td></tr>
<tr><td rowspan="3">12.20 - 12.40
Анализ защиты программы «PasswordSafe» Б. Шнайера
Беленко А.В. – аналитик компании «Элкомсофт»</td></tr>
<tr><td colspan="2" rowspan="2">12.20 – 12.50
Практика применения ЭЦП - от внедрения до суда
Маслов Ю.Г. – зам. коммерческого директора компании «Крипто-Про»</td></tr>
<tr><td rowspan="2">12.40 – 13.00
Выявление уязвимостей в программном коде
Лапин С.Н. - академик АПБОП, генеральный директор НПП «БИТ»
Марков А.С. – к.т.н., доцент, CISSP, НПП «БИТ»,
Цирлов В.Л. – CISSP, НПП «БИТ»</td></tr>
<tr><td colspan="2">12.50 – 13.10
Обязательные и добровольные системы сертификации в РФ
Волчков А.А. – президент ассоциации «РусКрипто»</td></tr>
<tr><td colspan="2">13.10 – 13.30
Легализация использования средств защиты информации в органах государственной власти
Лебедев А.Н. - к.ф.-м.н., с.н.с., директор ассоциации «РусКрипто»</td><td>13.00 – 13.30
Обзор математических методов построения поточных шифров (по материалам конкурса ECRYPT)
Жуков А.Е. –к.ф.-м.н., директор ассоциации «РусКрипто»</td></tr>
<tr><td>13.30 – 15.00</td><td colspan="2">Обед</td></tr>
</table>

ДЕНЬ ВТОРОЙ: 4 февраля, суббота (вечер 15.00 – 22.00)

<table>
<tr><td>15.00 – 18.30</td><td colspan="2">Секционные заседания (продолжение)</td></tr>
<tr><td rowspan="2">15.00 – 15.30
Роль ИКТ в современных технологиях организации деятельности любого вида

Левенчук А.И. - генеральный директор «Техинвестлаб»</td><td>15.00 – 15.20
Методика оптимизации криптографических алгоритмов для архитектуры современных компьютеров
Калядин О.А. . - директор ассоциации «РусКрипто»</td></tr>
<tr><td rowspan="2">15.20 -15.40
Анализ стойкости функции хеширования национального стандарта Республики Беларусь
Иванов А.Г. - к.ф.-м.н., директор ассоциации «РусКрипто»</td></tr>
<tr><td>15.30 – 16.00
Доверие и риски при использовании Интернет-технологий
Митричев И.В. - директор ассоциации «РусКрипто»</td><td>15.40 – 16.00
Алгоритм решения систем линейных уравнений в кольцах вычетов.
Авдошин С.М. – к.т.н., МАТИ-РГТУ им.К.Э.Циолковского
Савельева А.А. – МАТИ-РГТУ им. К.Э.Циолковского</td></tr>
<tr><td rowspan="2">16.00 – 16.30
О программно-инженерной казуистике норм и средств электронной подписи.

Дзержинский Ф.Я. - начальник отдела системной экспертизы ОАО "Банк Российский кредит"</td><td>16.00 – 16.15
Антивирусная защита в ОС Linux
Горошко П.П., Санников А.С. – студенты МИФИ.</td></tr>
<tr><td>16.15 – 16.30
Исследования криптографических свойств S-блоков
Чикин А.А., Губарь Н.И., Павлова М.В. – студенты МГТУ им. Баумана</td></tr>
<tr><td>16.30 – 17.00</td><td colspan="2">Перерыв. Чай, кофе.</td></tr>
<tr><td>17.00 – 17.20
Концепции электронного учета, аудита и раскрытия информации
Агроскин В.В. - член Экспертного совета СФ России</td><td>17.00 – 17.20
Масштабируемый алгоритм потокового шифрования NIVA с секретным ключом переменной длины
Васильев Н.П. - доцент МИФИ</td></tr>
<tr><td>17.20 – 17.40
Регулирование отношений в информационном обществе
Каптерев А.С. – эксперт Минэкономразвития России</td><td>17.20 – 17.40
Стохастические системы и их применение в криптографии
Кулаков И.А. – президент компании «Random Art Labs»</td></tr>
<tr><td rowspan="3">17.40 – 18.30

Круглый стол:
Социальные, юридические и технические аспекты сбора, хранения, защиты и обеспечения доступа к общественно значимым массивам информации

Участвуют: Агроскин В.В., Дзержинский Ф.Я., Волчинская Е.К., Волчков А.А., Калайда И.А., Каптерев А.А., Лебедев А.Н., Левенчук А.И., Микулич Н.Д., Соловяненко Н.И.</td><td>17.40 – 18.00
Криптографическая подсистема в информационных технологиях
Попов В.О. – к.ф.-м.н., начальник отдела «Крипто-Про»</td></tr>
<tr><td>18.00 – 18.15
Свойства булевых функций и класса обратимых конечных автоматов
Сухинин Б.М., Аленькина А.В. – студенты МГТУ им. Баумана</td></tr>
<tr><td>18.15 – 18.30
Новый метод проактивной защиты от зловредного ПО
Рабинович И.С. – независимый эксперт</td></tr>
<tr><td>18.30 – 19.30</td><td colspan="2">Ужин</td></tr>
<tr><td>19.30 – 22.00</td><td colspan="2">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 доктор Горячкин Е. А. и другие участники конференции,
считающие себя способными выступить публично с пением.
Традиционно обстановка на вечере очень доброжелательная и непринужденная.</td></tr>
</table>

ДЕНЬ ТРЕТИЙ: 5 февраля, воскресенье (утро 9.30 – 15.00)

9.30 – 10.00	***Завтрак***

10.00 – 10.30	**Технологии одноразовых паролей для усиленной аутентификации при удаленном доступе** Крячков А.В. - директор по продуктам компании «Алладдин»
10.30 – 11.00	**Схема цифровой подписи на базе укороченного ECDSA для удаленного делегирования пользователем прав доступа к USB устройствам, реализованная в системе Device Lock** Винокуров С.В. – компания «SmartLine Inc»
11.00 – 11.30	**Система «Proactive Security Auditor»** Беленко А.В. – компания «Элкомсофт»
11.30 – 12.00	***Перерыв. Чай, кофе.***
12.00 – 12.30	**Использование псевдокода в системах информационной безопасности** Горелов Д.Л. – компания «Актив»
12.30 – 13.00	**Электронный архив системы раскрытия информации в рамках ФЦП «Электронная Россия»** Шустиков Д.В. – компания «ЛАН Крипто»
13.00 – 13.30	**Плюсы и минусы многовендорной антивирусной защиты.** Антимонов С.Г. – компания «ДиалогНаука»
13.30 – 14.00	**Аппаратные решения ОКБ САПР в области криптографической защиты информации** Ращепкин А.К. – компания «ОКБ САПР»
14.00 – 15.00	***Обед***

ДЕНЬ ТРЕТИЙ: 5 февраля, воскресенье (вечер 15.00 – 19.00)

15.00 – 15.30	**Японская радиограмма с “кодом ветров” и Перл-Харбор** Сырков Б.Ю. – эксперт по истории криптографии, автор ряда книг
15.30 – 16.00	**Система защиты от вторжений Safe’n’Sec. Технологии и возможности** Калиниченко М.И. – компания «СтарФорс».
16.00 – 16.30	**Минималистская криптография и ее применение в системах RFID** Кулаков И.А. – компания «Random Art Labs».
16.30 – 17.00	**Испытательный центр ЗАО "НПП "БИТ": восемь лет на рынке** Марков А. С. – руководитель испытательного центра НПП «БИТ», Цирлов В.Л. – руководитель группы НПП «БИТ»
17.00 – 17.30	**Проблемы современных антивирусных программ** Резников Г.К. - к.т.н., с.н.с., коммерческий директор компании «ВирусБлокАда» (г. Минск), Барцевич Д. А. - начальник отдела компании «ВирусБлокАда» (г. Минск)
17.30 – 17.50	**Система контроля доступа на основе биометрии** Черномордик О.М. – к.ф.-м.н., генеральный директор компании «Биометрические технологии»
17.50 - 18.00	**Закрытие конференции «РусКрипто 2006»**
18.00 – 19.00	***Ужин***
19.00	**Отъезд в Москву**

Резервные доклады.

Исследование программы “skype”. Васильев К.П. – МИФИ
Криптоанализ по побочным каналам. Жуков А.Е. – к.ф.-м.н., директор ассоциации «РусКрипто»
Криптографические свойства булевых отображений». Жуков А.Е. – к.ф.-м.н., директор ассоциации «РусКрипто»
Проблемы гарантированного уничтожения информации на жестком диске. Никулин М.Ю. – НПП «БИТ»
Проект федерального закона “Об электронной подписи”. Поздняк И.Г. – Министерство информационных технологий и связи Российской Федерации