Конференция «РусКрипто'2008»
программа конфереции и материалы к докладам

День заезда. 3 апреля, четверг

17:00	**Отъезд из Москвы** Станция метро «Полежаевская», выход из первого вагона при движении из центра, в подземном переходе налево, автобус с табличкой «РусКрипто'2008»
18:00 — 19:00	**Регистрация и расселение участников в пансионате «Липки»**
19:00 — 20:00	Ужин
20:00 — 23:00	**Пивная вечеринка от спонсоров, знакомство участников конференции**

День первый. 4 апреля, пятница

8:45 — 10:00	Завтрак	
10:00 — 10:10	**Открытие конференции**	
10:10 — 11:45	**Доклады первого дня** Выступают представители компаний Cisco, «ИнфоТеКС», «Актив», ЦБИ и др. Список докладов	
11:50 — 12:10	Перерыв. Чай, кофе.	
12:10 — 13:30	**Доклады первого дня** Продолжение	
13:50 — 15:00	Обед	
15:00 — 16:30	**Круглый стол «ЭЦП и юридически значимый электронный документооборот»** · Изотов Б.С., ФГУП НИИ «Восход» · Курепкин И.А., «Крипто-Про» · Волчков А.А., Ассоциация «РусКрипто» · Анучин Михаил, «СКБ-Контур» Ведущий — Юрий Маслов, «Крипто-Про»	
16:30 — 17:00	Перерыв. Чай, кофе.	
17:00 — 18:30	Экспертная панель **«Инсайдеры. Технологии защиты от внутренних угроз»** · Ашот Оганесян, «Смарт Лайн Инк.» · Алексей Раевский, «SecurIT» · Лев Матвеев, «СофтИнформ» Ведущий — Дмитрий Харченко, «InfoWatch» Список докладов	Блок докладов **«Последние достижения мировой криптографии»** · М. Пудовкина, к.ф.-м.н. доцент МИФИ, директор ассоциации «РусКрипто». · А. Жуков, к.ф.-м.н. доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто» Список докладов
19:00 — 23:00	**Официальный банкет в честь юбилея конференции «РусКрипто»** В течение вечера играют основоположники балканского свинга, группа Blackmailers	

День второй. 5 апреля, суббота

9.00 — 10.00	Завтрак	
10:00 — 11:30	Секция 1. **«Криптография: теория и практика»** Ведущие секции: · Жуков А.Е., к.ф.м.н., ассоциация «РусКрипто» · Попов В.О., к.ф.м.н., компания «Крипто-Про» Список докладов	Секция 2. Закрытая секция **«Практический опыт анализа защищенности информационных систем и разработки индивидуальных решений по безопасности для корпоративных заказчиков»** Организатор — компания «СпецЭкоСтрой».
11:30 — 11:50	Перерыв. Чай, кофе.	
11:50 — 13:50	Секция 1. **«Криптография: теория и практика»** Продолжение работы	Секция 3. **«Защита персональных данных. Что ждет рынок защиты информации?»** Ведущий секции — Юрий Аксененко, ЦБИ.
13:50 — 15:00	Обед	
15:00 — 16:20	Секция 4. **«Реверсинг как искусство. Анализ исполняемого кода и технологии защиты»** Модератор — Ашот Оганесян, технический директор «Смарт Лайн Инк.» Список докладов	Секция 5. **«Интернет и информационная безопасность»** Модератор — Сергей Гордейчик, системный архитектор, компания Positive Technologies Список докладов
16:20 — 16:40	Перерыв. Чай, кофе.	
16:40 — 18:30	Секция 4. **«Реверсинг как искусство. Анализ исполняемого кода и технологии защиты»** Продолжение работы	Секция 5. **«Интернет и информационная безопасность»** Продолжение работы
18:30 — 19:30	Ужин	
19:30 — 21:30	**Дегустация крепких спиртных напитков, неформальное общение** Спонсор вечера — «Косогоров самогон»	

День третий. 6 апреля, воскресенье

9:00 — 10:00	Завтрак	
10:00 — 12:20	Секция 6. **«Свободное программное обеспечение и информационная безопасность»** *В работе секции принимают участие эксперты компаний IBM, VDEL, ИВК, Mandriva.* Ведущий и модератор — Алексей Смирнов, генеральный директор, «ALT Linux». Список докладов	Секция 7. **«Теория и практика создания систем информационной безопасности»** Ведущий и модератор — Котенко Игорь Витальевич, д.т.н., профессор, руководитель научно-исследовательской группы компьютерной безопасности, СПИИРАН Список докладов
12:20 — 12:40	Перерыв. Чай, кофе.	
12:40 — 13:40	Заключительная секция **«На третий день»** Мини-доклады от наиболее ярких докладчиков конференции, все самое интересное, что не уместилось в рамки секций предыдущих дней. Обсуждение наиболее важных вопросов и проблем, которые были подняты на конференции. Ответы экспертов на вопросы, которые требовали времени на подготовку или уточнения. Обсуждение формата и тем следующей конференции. Торжественное закрытие юбилейной конференции.	
13:30 — 15:00	Обед	
15:00 — 16:00	**Отъезд в Москву**	

Доклады первого дня

Часть первая

«10 лет Ассоциации «РусКрипто»: чему учит опыт»
А. Волчков, президент Ассоциации «РусКрипто»
За 10 лет изменился не только рынок информационной безопасности, принципиально изменились угрозы бизнесу и приоритетные задачи по защите информации. Опыт показывает, что часто мы защищаемся от несуществующих угроз и не замечаем реальных. Ошибки пользователей, недостатки решений и другие примеры из жизни, а также, где искать пути решения — ответы на эти вопросы вы услышите в докладе.

«Тенденции современной криптологии»
А.Г. Иванов, к.ф.-м.н., директор ассоциации «РусКрипто»
Обзорный доклад, посвященный основным событиям в гражданской криптологии за прошедший год. Кратко об основных международных криптографических конференциях и результатах наиболее интересных работ.

«Что интересного произошло на мировом рынке ИБ в 2007 году: тенденции, факты, курьезы»
Д. Скляров, эксперт, «Элкомсофт»
Признанный российский эксперт в области информационной безопасности, криптоаналитик компании «Элкомсофт» и доцент МГТУ им. Баумана — расскажет о наиболее ярких и важных тенденциях в области информационной безопасности и криптографии.

«Защита персональных данных. Что ждет рынок защиты информации?»
Юрий Аксененко, к.т.н., Председатель Центра безопасности информации (ЦБИ)
Информационные системы, работающие с персональными данными, в соответствии с законом должны соответствовать некоторым требованиям. Что это за требования? В каких документах они сформулированы? Что ждет участников рынка?

«Об использовании средств криптографической защиты информации для защиты персональных данных»
Ю. Маслов, коммерческий директор, «Крипто-Про»
В большом количестве нормативно-правовых актов мы сталкиваемся с понятием «персональные данные». Следует отметить Постановление Правительства РФ от 17.11.2007 N 781, т.к. именно оно узаконивает тенденции, которые сложились в сфере применения шифровальных (криптографических) средств (СКЗИ). В докладе будет рассказано о том, какие средства СКЗИ необходимо использовать, как проводить тематические исследования, создавать эксплуатационную и другую документации.

Часть вторая

«Вопросы стандартизации криптографических методов защиты информации»
А.В. Лунин, начальник аналитического отдела, «ИнфоТеКС»
Благодаря усилиям российских госрегуляторов и разработчиков СКЗИ ситуация со стандартизацией алгоритмов и протоколов меняется в лучшую сторону. Создан российский технический комитет по стандартизации «Криптографическая защита информации». Идет активная работа в ISO. IETF утвердил российские рекомендации. Расширяются спецификации PKCS#11. Но есть и проблемы...

«Защита информации и свободное программное обеспечение»
Алексей Смирнов, генеральный директор, «ALT Linux»
Свободное программное обеспечение всё шире используется как на серверах, так и на рабочих станциях в решениях, требующих обеспечения информационной безопасности. У российских фирм есть опыт сертификации решений на базе СПО как для работы с конфиденциальной информацией, так и с гостайной. Важно, что при использовании СПО возможно проведение независимого аудита информационной безопасности. Обращается внимание на важность воспроизводимости сборочной среды.

«Интеллектуальные ключевые носители для российских систем PKI»
Горелов Дмитрий, коммерческий директор, «Актив»
Применение электронно-цифровой подписи в России достигло промышленных масштабов. Это технология, приносящая реальную пользу в масштабах государства. Каков дальнейший сценарий развития программных и аппаратных средств ЭЦП? Какие средства и технологии будут использоваться для хранения и использования криптографических ключей?

«Анализ существующих стандартов управления ИБ: ISO 27001, ISM3, ISF SoGP и др.»
Алексей Лукацкий, бизнес-консультант по безопасности, «Cisco»
Все, что делается в области информационной безопасности, начиная от проверки готовности предприятия к новым требованиям по безопасности и заканчивая реагированием на инциденты, должно быть очерчено четкими рамками, выход за которые недопустим. Необходимо соблюдать жизненный цикл информационной безопасности, который имеет начало, но не имеет конца, ибо безопасность — не состояние, а процесс, причем непрерывный. Что же это за процесс и как правильно его соблюдать и контролировать?

Экспертная панель «Инсайдеры. Технологии защиты от внутренних угроз»

Защита от внутренних угроз — одна из самых актуальных тем сегодняшнего дня. В одном зале соберутся ведущие специалисты и технические идеологи наиболее известных компаний, работающих в этой области. Доклады о новых технологиях, тенденции рынка, дискуссии.

«Общая теория и реальная практика контроля утечек конфиденциальной информации»
Дмитрий Харченко, директор по продуктам, «InfoWatch»
В докладе будут кратко рассмотрены основные подходы к проектированию DLP-систем. Типичные ошибки, трудности, а также способы их преодоления, возникающие при внедрении систем контроля утечек конфиденциальной информации.

«Современные тенденции в борьбе с внутренними угрозами информационной безопасности предприятий»
Алексей Раевский, генеральный директор, «SecurIT»
В настоящее время вопрос борьбы с внутренними угрозами информационной безопасности (с инсайдерами) является наиболее актуальным. В первую очередь, проблема внутренних угроз важна потому, что инсайдером может оказаться и лояльный, но невнимательный сотрудник, и курьер, который перевозит магнитную ленту с резервной копией в депозитарий. В докладе подробно анализируются наиболее распространенные внутренние угрозы и современные методы борьбы с ними.

«Компоненты систем информационной безопасности»
Лев Матвеев, генеральный директор, СофтИнформ
Существующие архитектуры комплексных решений для обеспечения информационной безопасности, их плюсы и минусы. Контроль существующих путей утечки информации. Полнотекстовый поиск как основной инструмент интеллектуального анализа перехваченной информации. Требования по системе разграничения прав доступа в системах информационной безопасности.

«Презентация продукта InfoWatch CryptoStorage»
Левин Константин, менеджер по работе с корпоративными заказчиками, «InfoWatch»
Компания InfoWatch представляет новый продукт InfoWatch CryptoStorage, предназначенный для централизованной защиты конфиденциальной информации с использованием шифрования в процессе ее хранения и обработки. Использование решения позволит значительно расширить границы и возможности системы обеспечения информационной безопасности предприятия. Теперь решения InfoWatch не только позволяют предотвратить утечку конфиденциальных данных из сети организации, но и обеспечивают защиту информации, санкционировано оказавшейся и используемой вне пределов корпоративной сети. Широкие функциональные возможности и централизованное управление позволяют максимально адаптировать продукт под нужды заказчика.

Блок докладов «Последние достижения мировой криптографии»

Подробные научные доклады, посвященные самым интересным и важным результатам, полученным за последнее время в криптографии. По материалам конференций IACR и другим открытым публикациям. От директоров ассоциации «РусКрипто».

«Актуальные вопросы криптографии: обзор результатов по материалам криптографических конференций»
М. Пудовкина, к.ф.м.н. доцент МИФИ, директор ассоциации «РусКрипто»
За прошедший год с момента окончания предыдущей конференции РусКрипто'2007 получены новые важные результаты по криптоанализу и синтезу криптосистем (блочных шифров, поточных шифров, хеш-функций), используемых в современных системах защиты информации. Также получен ряд интересных математических результатов, имеющих приложение в криптографии. В докладе в концентрированном виде собрана самая актуальная и интересная информация по исследованиям, проведенным в 2007 году и начале 2008 года.

«Обратимость конечных автоматов. Современное состояние теории и практические приложения»
А. Жуков, к.ф.м.н. доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто»
Обратимость конечных автоматов обычно считается чисто академическим вопросом. Между тем обратимые автоматы находят свое применение в таких прикладных вопросах, как криптография, в том числе и криптография с открытым ключом. В докладе будет рассмотрено современное состояние этого раздела дискретной математики и обрисованы перспективы развития.

Секция 1. Криптография: теория и практика

Ведущие секции «Криптография: теория и практика» — Жуков Алексей Евгеньевич, к.ф.м.н. доцент МГТУ им. Баумана, директор ассоциации «РусКрипто» и Попов Владимир Олегович, к.ф.м.н., компания Крипто-Про.

Часть первая

Тема 1. Анализ и синтез криптографических систем

«Применение запутывающих преобразований в криптографических целях»
Евгений Родионов, МИФИ
Асимметричные алгоритмы шифрования по сравнению с симметричными помимо плюсов имеют и недостатки, заключающиеся в размере ключевой информации и скорости зашифрования/расшифрования. Можно ли с помощью применения запутывающих преобразований к симметричным шифрам получить надёжные алгоритмы шифрования с открытым ключом? Насколько они будут эффективными и надёжными?

«Групповые свойства Rijndael-подобных шифров»
Михаил Хоменко, МИФИ
В работе были изучены цикловые свойства линейных преобразований MixCol и ShiftRow; показано, что их композиция порождает группу подстановок G порядка ordG=8. Для группы G найдены все орбиты, число и формулы, по которым их можно построить; построена система блоков импримитивности, являющихся разбиением. Построена атака на Rijndael-подобный шифр, использующая различные системы блоков импримитивности.

«Анализ модификаций криптосистемы Нидеррайтера»
Марина Самохина, МФТИ
Одним из классических представителей криптосистем с открытым ключом, основанных на линейных кодах, является система Нидеррайтера. На сегодняшний день, интерес вызывает не столько сама классическая система Нидеррайтера, сколько ее различные современные модификации. В докладе приведено построение криптосистем-модификаций и на основании анализа ряда атак показано, что этот класс криптосистем является стойким и не уступает аналогам, применяемым на практике.

Новое в восстановлении паролей: Thunder Tables и GPU
Андрей Беленко, аналитик по информационной безопасности, «Элкомсофт»
В докладе будут рассмотрены две новые технологии, предложенные в прошлом году. Первая — улучшение Rainbow-таблиц, позволяющее преодолеть вероятностную природу этой атаки и гарантировать 100%. Вторая — использование распространенных видеоадаптеров для ускорения криптографических вычислений, для перебора ключей шифрования и паролей методом «грубой силы».

Часть вторая

Тема 2. Анализ и синтез ключевых систем

«Вопросы повышения защищённости ключей пользователей при их использовании в вычислительных системах»
Веденьёв Л.Т. Леонтьев С.Е. Попов В.О.

Рассмотрены вопросы уязвимости ключей СКЗИ в среде вычислительной системы и использования интеллектуальных карт для обеспечения их повышенной защищённости.

«Об опасности ошибок вычислений при использовании стандарта ГОСТ Р34.10-2001»
Веденьёв Л.Т. Леонтьев С.Е. Попов В.О.
Рассмотрен вопрос о влиянии ошибок вычислений на стойкость криптоалгоритмов ЭЦП ГОСТ Р 34.10-2001 и Диффи-Хеллмана на базе эллиптических кривых.

«Вопросы контроля срока действия закрытых ключей»
Павел Смирнов, к.т.н., ведущий специалист, Крипто-Про
Все криптографические ключи имеют ограниченные сроки использования. В докладе будет рассмотрена целесообразность выдачи сертификатов со сроком действия, превышающим срок действия соответствующего закрытого ключа, а также предложены технические меры для контроля регламента использования закрытых ключей.

Тема 3. Оптимизация криптографических алгоритмов

«Эффективное скалярное умножение точек эллиптических кривых»
Олег Тараскин, главный аналитик, «Актив»
Актуальность эллиптических кривых (ECC vs RSA, DH). Развитие методов ускорения скалярного умножения точки на число. Скорость вычислений и устойчивость к side-channel атакам. Лучшие на сегодняшний день результаты.

Тема 4. Стеганография

«Применение стеганографии в системах видеоконференции»
Наталья Семенова, МИЭМ
Методы стеганографии позволяют скрытно передавать информацию между адресатами, путем встраивания ее в некоторый безобидный, не привлекающий внимание объект (стегоконтейнер). При этом тайной является сам факт существования передаваемого сообщения. В докладе описана стеганографическая система, которая позволяет встраивать информацию в потоковое видео с целью ее скрытной передачи. Приведен пример реализации разработанного алгоритма в системе видеоконференции.

Секция 4. Реверсинг как искусство

В работе секции «Реверсинг как искусство. Анализ исполняемого кода и технологии защиты» принимают участие специалисты компаний «Актив», «Смарт Лайн Инк.», эксперт компании «Элкомсофт» Дмитрий Скляров.

Модератор секции — Ашот Оганесян, технический директор, Смарт Лайн Инк.

Часть первая

«Технология Authenticode в исполняемых файлах формата Portable Executable»
Винокуров Станислав, главный разработчик/эксперт по инфобезопасности, «Смарт Лайн Инк.»
В докладе описан механизм реализации Authenticode для цифровой подписи Portable Executable файлов, а также его применение для защиты приложений от модификации. Проверка цифровой подписи без вызова внешних crypto-API функций.

«Способы исследования и перехвата RPC-интерфейсов в ОС Windows»
Гольчиков Андрей, аналитик, Смарт Лайн Инк.
Remote Procedure Call (RPC) — технология, позволяющая компьютерным программам вызывать функции или процедуры в другом адресном пространстве (например, на удалённых компьютерах). Как работает RPC в Windows? Какие существуют способы перехвата RPC-клиентов и RPC-серверов? Для чего это нужно и чем это опасно.

«Механизмы поиска оригинальной точки входа исполняемого файла»
В.А. Букасов, МИФИ
Если исследуемый исполняемый файл накрыт упаковщиком (протектором), то поиск оригинальной точки входа в программе может превратиться в нетривиальную задачу. Поиск посредством динамического анализа имеет ряд подходов, обобщив которые можно получить универсальный способ. Насколько эффективен такой подход? Как он упрощает жизнь аналитикам исполняемого кода?

Часть вторая

«Применение запутывающих преобразований и полиморфных технологий для автоматической защиты исполняемых файлов от исследования и модификации»
Щелкунов Д.А., системный программист, «Актив»
В настоящее время существует целый ряд подходов к защите исполняемых файлов от исследования и модификации. Основные из них — это применение конвертов и виртуализация кода приложения. Можно легко увидеть, что качество практически всех подходов, применяемых для защиты ПО, напрямую зависит от качества запутывающих преобразований.

«Построение эффективных запутывающих преобразований с учетом специфики объектно-ориентированного кода»
Олег Рыськов, разработчик, «Актив»
Большую популярность получили объектно-ориентированные языки программирования, которые обеспечивают независимость кода от аппаратной и программной среды путем компиляции в промежуточный код. Структурные особенности промежуточного кода не позволяют с должной эффективностью использовать методы защиты, применяемые к обычному native-код. Как решать эту проблему?

«Черно-белые ящики, или патогенез использования криптографии в условиях открытых платформ»
Дмитрий Скляров, Андрей Беленко, аналитик по информационной безопасности, «Элкомсофт»
Одна из функций криптографии — обеспечение секретности данных, но в условиях, когда среда выполнения подконтрольна противнику, традиционная криптография оказывается бессильна. На помощь приходят black-box и white-box реализации, но надежны ли они?

«Исследование механизмов защиты исполняемых файлов для ОС LINUX»
Дмитрий Тимовский, МИФИ
В последнее время наблюдается рост количества коммерческого ПО, выпускаемого под открытые ОС, и, как следствие, появилась потребность в обеспечении современного уровня защиты от его нелегального копирования и реверс-инжиниринга. С какими проблемами могут столкнуться разработчики при создании навесных защит для открытых ОС?

«Защита приложений, имеющих промежуточное представление (байт-код)»
Александр Матросов, МИФИ
Учитывая особенности среды выполнения с промежуточным представлением (Java, .NET), можно построить систему защиты основанную на виртуализации байт-кода. Суть такой защиты будет заключаться в построении альтернативной среды выполнения и транслирования инструкций байт-кода в инструкции защищенной VM. Возможна ли виртуализация байт-кода (Java, .NET) с точки зрения защиты? Какие ограничения существуют у такого подхода к защите ПО?

Секция 5. Интернет и информационная безопасность

Секцию ведет Сергей Гордейчик (MCSE, MCP, MVP Windows:Security, CWNA) системный архитектор компании «Positive Technologies», участник проектов Web Application Security Consortium (WASC).

Часть первая

«Промышленный шпионаж в сети Интернет»
Алиса Белоусова, системный архитектор, «Информзащита»
В докладе рассматриваются вопросы формирования требований к безопасности Web-приложений, подходы к анализу защищенности, статистика уязвимостей Web-систем. Проводится обзор методов и средств защиты с точки зрения их распространенности и эффективности.

«Исследование механизмов защиты от атак DDOS: имитация противоборства интеллектуальных агентов в сети Интернет»
*Котенко И.В., Уланов А.В., Санкт-Петербург, СПИИРАН*Предлагается подход к исследованию атак «распределенный отказ в обслуживании» (DDOS) и механизмов защиты от них. В его основу положено представление сторон атаки и защиты в виде команд интеллектуальных агентов, которые могут противоборствовать, кооперироваться и адаптироваться к действиям друг друга.

«Информационная безопасность и IPv6»
*Андрей Абрамов, Эксперт по ИБ, «Positive Technologies»*Рассматриваются новые угрозы, возникающие в связи с текущим переходом Internet на новую платформу.

«Актуальные уязвимости беспроводных сетей»
Владимир Лепихин, зав. лабораторией, Учебный центр «Информзащита»
Описание проблем, связанных с безопасностью беспроводных сетей, распространенных уязвимостей, обнаруженных в ходе аудитов и тестов на проникновение.

Часть вторая

«Поиск уязвимостей в антивирусах»
Евгений Легеров, GLEG Ltd.
Антивирусы являются наиболее распространенным средством защиты. Более 90 процентов всех компьютеров использует тот или иной антивирус. Однако, как любая программа, антивирусы могут содержать ошибки, в том числе и связанные с безопасностью. В докладе рассматриваются подходы к поиску уязвимостей в библиотеках работы с архивными файлами, используемыми многими антивирусными продуктами. В процессе работы над докладом было проведено поверхностное тестирование нескольких различных антивирусов. В каждом из них были обнаружены ранее неопубликованные уязвимости.

«Анализ и оценка безопасности Web-приложений»
Сергей Гордейчик, системный архитектор, «Positive Technologies»
К сожалению, распространенные на настоящий момент стандарты в области ИБ лишь косвенно касаются вопросов защиты приложений. Однако существуют и специализированные документы, такие как OWASP top 10 и Web Application Security

Consortsium Thread Classification. Эти документы посвящены подробному рассмотрению уязвимостей и атак на Web-приложения, и именно их стоит использовать в качестве руководства при оценке защищенности.

«Безопасность как фактор выбора платформы для создания сайта»
Дмитрий Васильев, директор АИСТ/NetCat
Выбор платформы для разработки сайта с точки зрения безопасности. Основные опасности при использовании различных типов CMS. Наиболее распространенные ошибки производителей CMS, разработчиков сайтов и пользователей, грозящие взломами. Анализ статистики обращений в службу поддержки: по каким причинам происходят взломы?

«Процесс обеспечения безопасности Интернет-приложений»
*Андрей Бабий, «Яндекс»*Рассматривается вопросы построения жизненного цикла Интернет-приложений с точки зрения компании, чей бизнес зависит от подобных систем.

Секция 6. Свободное ПО и информационная безопасность

Ведущий и модератор секции — Алексей Смирнов, генеральный директор ALT Linux. В работе секции принимают участие эксперты компаний «IBM», «VDEL», «ИВК», «Mandriva».

«Защита информации и ОС Linux: взгляд IBM»
Алексей Федосеев, Денис Сосновцев, «IBM»
Сертификация Linux по требованиям информационной безопасности в России и за рубежом. Новости. Применение SELinux в госпроектах — опыт IBM в правительственных органах Великобритании. Вопросы общей стоимости владения решений с SE Linux.

«Защищенные информационные системы на основе Linux»
Васюков Алексей Викторович, «VDEL»
Основные пункты доклада: способы контроля доступа и защиты от НСД; управление инфраструктурой — средства централизации управления доступом и применения политик безопасности; сертификации RHEL в области безопасности.

«Сертификация операционных систем Linux и программного обеспечения с открытым исходным кодом по стандартам информационной безопасности»
Котов С.Л., Рожнов М.М., ФГУП ГИЦ ПС ВТ
Операционная система Linux уже давно активно применяется в электронной коммерции и всё чаще внедряется в государственных учреждениях. Доступный исходный код и соответствие стандартам позволяют исследовать безопасность этой операционной системы как коммерческим компаниям, так и нет. Данная работа посвящена обзору основных положений нормативных документов, регламентирующих проектирование, разработку и сертификацию защищенных компьютерных систем. Акцент уделен процессу проверки соответствия требованиям следующих руководящих документов независимыми лабораториям.

«Корпоративные и сертифицированные решения компании Mandriva»
Федосеев Виктор Викторович, генеральный директор, «Mandriva.ru»
В данном докладе речь пойдет о корпоративной линейке компании Mandriva: Mandriva Server, Mandriva Desktop и новейших системах контроля и управления сетью — Mandriva Directory Server и Linbox Rescue Server. Так же будет рассказано о новой версии дистрибутива — Mandriva Linux 2008.1 (Spring Edition), релиз которой ожидается в апреле этого года. Кроме того, в докладе будут затронуты различные аспекты сертифицированных ФСТЭКом дистрибутивов от компании Mandriva.

«ИВК-Кольчуга: средство обеспечения конфиденциальности, целостности и доступности данных на объектах внедрения АС»
В. Андреев, «ИВК»

«Технология безопасной сборки пакетов»
Хачатуров Вартан Микаэлович, менеджер проектов, «ALT Linux»
Рассматривается задача безопасной воспроизводимой сборки дистрибутива, изучаются требования, накладываемые этой задачей на архитектуру системы сборки, рассматривается архитектура hasher'a и существенные моменты её реализации. Приводятся примеры производных решений на базе hasher'a.

«Производство сертифицированного Red Hat Enterprise Linux в ОАО ВНИИНС»
Дмитрий Ефанов, заместитель директора, Центр базовых ИТ ОАО «ВНИИНС»

В 2007 году ОАО «ВНИИНС» и IBM получили сертификаты ФСТЭК России на серийное производство двух вариантов сертифицированных версий RHEL 4: для серверов RHEL 4 AS и для рабочих станций RHEL 4 WS. Были достигнуты следующие показатели: 4 ОУД и 4 уровень контроля НДВ. Сертификация проведена на серверах компании IBM для трёх аппаратных платформ: Intel (64 р.), POWER и мэйнфреймы System z. Серийное производство развернуто в ОАО «ВНИИНС».

Секция 7. Теория и практика создания систем информационной безопасности

Секцию ведёт Котенко Игорь Витальевич, д.т.н., профессор, руководитель научно-исследовательской группы компьютерной безопасности СПИИРАН

«Проактивные механизмы защиты от быстро распространяющихся сетевых червей»
Котенко И.В Санкт-Петербург, СПИИРАН
Предлагается проактивный подход к защите от быстро распространяющихся сетевых червей в сети Интернет, базирующийся на комбинировании механизмов обнаружения и сдерживания и автоматической динамической адаптации механизмов защиты в соответствии с изменением сетевой конфигурации и сетевого трафика.

«Обфускация программ: методы и приложения»
В.А. Захаров, Н.Н. Кузюрин, А.В. Шокуров, Институт системного программирования РАН
Задача обфускации заключается в разработке преобразований, которые сохраняют функциональные характеристики программ, но при этом делают невозможным или чрезвычайно трудоемким извлечение из открытого текста программы полезной информации об устройстве алгоритмов и структур данных. Рассматриваются различные теоретические подходы и реальные приложения данной технологии.

«Реконструкция закрытых форматов почтовых баз (MS Outlook, MS Outlook Express)»
С.И. Уласень, Г.К. Резников, ОДО «ВирусБлокАда», Минск
Почтовая база представляет собой сложный контейнерный объект, который может содержать внутри себя вредоносные вложения. Перед антивирусом встает задача проверки почтовых баз на наличие в них вредоносных объектов и корректного их лечения. Какие задачи должны поставить перед собой разработчики антивируса при поиске вредоносных файлов в почтовых базах? С какими трудностями они сталкиваются?

«Человеческий фактор в системах антивирусной защиты»
А.В. Багмет, В.Ю. Разумков, ООО «ВирусБлокАда», Москва
Система антивирусной защиты, особенно для корпоративного пользователя, представляет собой сложный объект, на функционирование которого в процессе эксплуатации оказывают влияние различные более или менее значимые факторы. При этом, как ни парадоксально, одним из основных является фактор человеческий. Как учесть его влияние при разработке и сопровождении систем антивирусной защиты?

«Механизмы атак с использованием уязвимостей Переполнение Буфера»
Гуркин Ю.Н. , технический специалист, ООО «ГЛЕГ»
В докладе приведена статистика регистрируемых атак, рассмотрены принципы атак использующих уязвимости типа переполнения буфера.

«Разграничение доступа к базам данных в сервис-ориентированных приложениях»
Быков Д.В., «ВолгаБлоб»
В докладе анализируются существующие подходы к аутентификации и разграничению доступа к базам данных при организации трехстороннего взаимодействия: тонкий клиент (web-браузер) — сервер приложений — система управления базами данных (СУБД).

«Анализ подходов к защите mdb-файлов СУБД Microsoft Access с использованием средств шифрования»
Пылин В.В., программист, ФГУ «Росаккредагентство»

В работе представлен анализ встроенного метода шифрования mdb-файлов MS Access. На его основе предложен усовершенствованный метод защиты, повышающий уровень безопасности при сохранении структуры файла и неизменности общего интерфейса работы с файлом при помощи драйвера MS Jet OLEDB 4.0.