Тайм-лайн конференции

28 марта, среда. День заезда

16.30	Трансферт в отель «Солнечный PARK HOTEL & SPA»
18:00 – 19:00	Заезд и регистрация участников, проживающих в отеле
19:00 – 20:00	Ужин. Свободное время
20:00 – 21:00	Шоу-программа «Welcome party» *Развлекательный центр (на улице)*

29 марта, четверг. Первый день работы конференции

8:00 – 9:45	Завтрак	
9:30 – 10:00	Регистрация участников конференции	
10:00 – 11:30	**Пленарное заседание** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.3*	
11:30 – 12:00	Перерыв	
12:00 – 14:00	**Круглый стол «Закон «Об электронной подписи» и его подзаконные акты. Как быть Удостоверяющим Центрам и операторам информационных систем?»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.3*	
14:00 – 15:00	Обед	
15:00 – 16:40	**Секция «Криптография и криптоанализ»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.4*	**Деловая игра «Что будет если?»** *Конференц-зал (Ресторанный комплекс)*
16:40 – 17:00	Перерыв	
17:00 – 19:00	**Секция «Криптография и криптоанализ»** *Продолжение работы секции*	**Секция «Настоящее и будущее антивирусной индустрии»** *Конференц-зал «Юпитер» (Конференц-комплекс)* *Подробнее на стр.6*
19:10 – 21:00	Церемония открытия конференции «РусКрипто'2012». Фуршет *Конференц-зал (Ресторанный комплекс)*	

30 марта, пятница. Второй день работы конференции

9:00 – 10:00	Завтрак	
10:00 – 11:40	**Круглый стол «Технологии безопасности систем ДБО»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.7*	**Секция «Технологии защиты и нападения»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.7*
11:40 – 12:00	Перерыв	
12:00 – 13:30	**Круглый стол «Рынок сетевой безопасности России на пути из прошлого в будущее»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.8*	**Секция «Электронная подпись без границ»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.8*
13:30 – 14:30	Обед	
14:30 – 16:10	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.9*	**Секция «Криптография в облачных решениях, безопасность информационных систем с размытыми контурами»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.12*
16:10 – 16:30	Перерыв	
16:30 – 19:00	**Секция «Перспективные исследования в области кибербезопасности»** *Продолжение работы секции*	**Секция «Продукты и технологии информационной безопасности»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.13*
19:00 – 20:00	Ужин	
20:00 – 23:00	**Тематический игровой вечер «Стиляги»** *Развлекательный комплекс*	

31 марта, суббота. День отъезда

9:00 –11:00	Завтрак
12.00	Трансферт из отеля в Москву (м. Речной вокзал)

Первый день работы конференции

10:00 – 11:30	**Пленарное заседание** *Конференц-зал (Ресторанный комплекс)*

Актуальные задачи обеспечения информационной безопасности конфиденциальной информации современных компьютерных систем.
***Баранов Александр Павлович**, заместитель директора ФГУП ГНИВЦ ФНС России, профессор Высшей Школы Экономики, д.ф.м.н.*

Дайджест новостей мировой криптографии.
***Жуков Алексей Евгеньевич**, к.ф.-м.н., доцент МГТУ им. Баумана, председатель совета директоров Ассоциации «РусКрипто».*

Информационное общество и криптография.
***Кузьмин Алексей Сергеевич**, первый заместитель начальника центра ФСБ России, д.ф-м.н., профессор, действительный член Академии криптографии Российской Федерации. **Лунин Анатолий Васильевич,** заместитель Секретаря ТК-26 «Криптографическая защита информации».*

Перспективы открытой криптографии в России.
***Попов Владимир Олегович,** директор Ассоциации «РусКрипто», ООО «Крипто-Про».*

12:00 – 14:00	**Круглый стол «Закон «Об электронной подписи» и его подзаконные акты. Как быть Удостоверяющим Центрам и операторам информационных систем?»** *Конференц-зал (Ресторанный комплекс)*

***Ведущие:** Представитель Минкомсвязи России (по согласованию);*
Маслов Юрий Геннадьевич, коммерческий директор ООО «Крипто-Про»;
Дзержинский Федор Янович, начальник отдела системной экспертизы Департамента информационных технологий ОАО "Промсвязьбанк".

От ЭЦП к ЭП в системах ДБО и не только.
***Дзержинский Федор Янович**, начальник отдела системной экспертизы Департамента информационных технологий, ОАО "Промсвязьбанк".*
Первого июля 2012 года закончится действие закона о ЭЦП. Все системы, использующие технологии электронной подписи, должны будут существовать только в рамках нового закона. Как быть операторам систем? Что ждет системы ДБО? Что должны успеть сделать юристы и технари до 01.07.2012 и успеют ли?

От ЕПД к ИС ГУЦ – состояние и перспективы единого пространства доверия.
***Трифаленков Илья Анатольевич**, начальник отдела информационной безопасности проекта «Информационное общество», ОАО «Ростелеком».*
В 2011 году произошли существенные изменения в проекте по созданию единого пространства доверия. Единое пространство доверия начало функционировать как реально действующий набор сервисов, доступных для пользователей вне зависимости от того, какой из УЦ, аккредитованных в ЕПД, с ним работает. Наиболее значимым явился сервис проверки электронной подписи, ныне широко используемый в системе межведомственного электронного взаимодействия. В 2012 году предполагается развитие основных сервисов с использованием сертификатов ЭП, а также запуск целого ряда управляющих систем, обеспечивающих широкое применение ЭП в интересах как государственных, так и коммерческих организаций.

Использование электронной подписи в ежедневной деятельности организации.

***Левиев Дмитрий Олегович**, Академия Информационных Систем.*

В докладе рассматриваются вопросы реализации требований ФСБ России к средствам электронной подписи, а также вопросы реализации требований к удостоверяющим центрам в организационно-технических мероприятиях и локальных нормативных актах организации, которая использует электронную подпись в ежедневной деятельности с собственным и внешним удостоверяющим центром. В ходе рассмотрения приводится перечень необходимых изменений в локальные нормативные акты по использованию электронной подписи.

15:00 – 19:00	**Секция «Криптография и криптоанализ»** *Конференц-зал «Марс» (Конференц-комплекс)*

***Ведущие:** Кузьмин Алексей Сергеевич, ФСБ России; Попов Владимир Олегович, Ассоциация РусКрипто, ООО «Крипто-Про»; Лунин Анатолий Васильевич, ОАО «ИнфоТеКС», ТК26.*

Часть 1 (15:00-16:40)

Развитие базовых стандартов криптографической защиты информации в России и за рубежом.

***Лунин Анатолий Васильевич,** ОАО «ИнфоТеКС», Секретариат Технического комитета по стандартизации (ТК26)«Криптографическая защита информации», GOST R Expert.*

Обзор деятельности ТК26 в 2011 г. в части развития базовых стандартов: обсуждение и передача в Росстандарт проектов стандартов на электронную подпись и функцию хэширования; разработка и экспертиза транспортных контейнеров и контейнеров хранения ключей, а также дополнений к криптографическим протоколам – будущих рекомендаций по стандартизации; участие в работе ISO JTC1 SC27 WG2.

Криптография и информационная безопасность в проекте Универсальная Электронная Карта.

***Азин Дмитрий Вячеславович,** начальник отдела защиты коммерческой тайны и персональных данных, ОАО «Универсальная электронная карта».*

Рассматриваются используемые в проекте Единой платежно-сервисной системы Универсальной электронной карты средства криптографической защиты информации, протоколы аутентификации, инфраструктура ключей и сертификатов, сочетание применения зарубежных и российских криптографических стандартов в системе.

Операционная система смарт-карты проекта УЭК. Архитектура и криптографические возможности.

***Мытник Константин Яковлевич,** начальник отдела смарт-карт ОАО «НИИМЭ и Микрон».*

В докладе дается обзор защищенного микроконтроллера и архитектуры операционной системы, разработанных ОАО «НИИМЭ и Микрон» для УЭК. Описывается схема защищенной сессии между картой УЭК и терминалом.

Криптография в коммерческих системах.

***Симаков Сергей Владимирович,** Security Architect, Microsoft Global Security Center of Excellence.*

Методы и подходы к встраиванию средств криптографической защиты информации в системы, используемые миллионами пользователей, и применение служб Cryptography Next Generation для поддержки различных криптографических стандартов.

Противодействие атакам на протокол TLS.

***Смышляев Станислав Витальевич,** инженер-аналитик, ООО «КРИПТО-ПРО».*

Проводится обзор и классификация построенных атак на протокол TLS, для каждой из атак выделяются необходимые и достаточные для успешного проведения атаки свойства реализации протокола, рассматривается влияние изменений в различных версиях SSL/TLS на применимость каждой из атак на какую-либо реализацию TLS, не противоречащую требованиям конкретной версии. Проводится обсуждение применимости атак из рассматриваемого класса к версиям 1.0 и 1.1–1.2 протокола TLS и конкретным сюитам, а также предлагается некоторая использующая временные характеристики модификация данных атак, возможная несмотря на принятые в версиях 1.1–1.2 протокола TLS контрмеры.

Часть 2 (17:00-19:00)

Обзор последних публикаций по криптографическим исследованиям алгоритма шифрования ГОСТ 28147-89.

Рудской Владимир Игоревич, *ФСБ России.*

С момента опубликования в 2011 году известной работы японского специалиста T. Isobe было предпринято несколько попыток улучшить содержащиеся в ней результаты. В докладе будет дан критический анализ соответствующих публикаций с точки зрения корректности и практической значимости полученных в них оценок стойкости алгоритма ГОСТ 28147-89.

Современные алгоритмы вычисления кратной точки и суммы кратных точек эллиптической кривой над конечным простым полем и их приложение к реализации схемы электронной цифровой подписи ГОСТ Р 34.10.

Гребнев Сергей Владимирович, Дыгин Денис Михайлович, *ФСБ России.*

В докладе представлены результаты теоретических и экспериментальных исследований указанных в названии алгоритмов в связи с дополнением национального стандарта ГОСТ Р 34.10 вариантом требований к параметрам, предполагающим использование кривых над полями размера порядка 512 бит.

О периодичности функционирования генератора псевдослучайных чисел RC4.

Бабаш Александр Владимирович, *доктор физ.-мат. наук, профессор, МЭСИ.*

Генератор RC4 представим последовательным соединением автономного полноциклового автомата с неавтономным автоматом, состояниями последнего являются пары: подстановка степени 2**n и вычет из кольца вычетов по модулю n. Доказано, что периоды последовательностей подстановок кратны числу 2**(n-1) и даны достаточные условия, при которых эти периоды кратны 2**n.

О разностных характеристиках обобщенного алгоритма шифрования Фейстеля 2-го типа.

Пудовкина Марина Александровна, *к.ф.-м.н., доцент МИФИ, директор Ассоциации «РусКрипто».*

Обобщенные алгоритмы шифрования Фейстеля лежат в основе таких шифрсистем как CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT, и др. В последние годы стали предлагаться модификации обобщенных алгоритмов шифрования Фейстеля, улучшающие их свойства рассеивания и перемешивания. В докладе рассматривается одно из таких таких обобщений. Для него показано наличие большого числа полнораундовых невозможных разностей и разностных характеристик с вероятностью единица.

Об одном протоколе выработки общего ключа.

Нестеренко Алексей Юрьевич, *к.ф.-м.н., доцент кафедры «Информационная безопасность» НИУ ВШЭ МИЭМ.*

Исследуется возможность компрометации нового протокола выработки общего ключа, реализованного в группе точек эллиптической кривой. Показано соответствие протокола основным криптографическим требованиям.

Прыгающие клеточные автоматы и регистры сдвига. Обзор результатов.

Дрелихов Владимир Олегович, *ФСБ России.*

Клеточные автоматы являются примером линейных автоматов, имеющих эффективную аппаратную реализацию. Вводится понятие индекса прыжка линейного автомата, позволяющее реализовать нерегулярное движение по его цикловой структуре. Излагаются способы синтеза клеточных автоматов и прыгающих клеточных автоматов.

17:00 – 19:00	**Секция «Настоящее и будущее антивирусной индустрии»** *Конференц-зал «Юпитер» (Конференц- комплекс)*

Ведущий: *Шабанов Илья, Anti-Malware.ru*.

Антивирусная защита сегодня. Большой технологический переход или затыкание дыр?

Шабанов Илья*, Управляющий партнер Anti-Malware.ru.*

Технологии антивирусной защиты значительно эволюционируют последние несколько лет. Появляются не только новые подходы, но и делаются попытки принципиальной смены парадигмы защиты. Рассмотрим, насколько эти изменения помогут лучше противостоять текущим и новым угрозам, и не являются ли они очередной "модной маркетинговой фишкой".

Тайна Duqu.

Гостев Александр*, главный антивирусный эксперт «Лаборатории Касперского».*

Duqu — сложная троянская программа, которая, похоже, была написана создателями скандально известного червя Stuxnet. Ее основная цель - действовать в качестве бэкдора в системе, упрощая кражу частной информации. Это его основное отличие от Stuxnet, главной целью которого были диверсии на промышленных объектах. Эксперты Лаборатории Касперского обнаружили способ проникновения вредоносной программы в атакованные системы, а также провели несколько операций, связанных с захватом ряда серверов управления Duqu, расположенных в разных странах мира. Результаты этих исследований представлены в докладе.

Реальна ли виртуальная защита?

Шабуров Олег*, компания Symantec.*

Специфика антивирусной защиты виртуальных сред. Как достичь максимального уровня защиты без проблем с производительностью. Для виртуальных сред характерны такие ситуации как виртуальные штормы или штормы сканирования. В борьбе с ними некоторые производители идут по пути оптимизации в ущерб уровню защиты. Каким образом мы достигаем минимизации нагрузки без потерь защищенности?

Модный тренд APT. Беспечность и как с ней бороться.

Шелестова Олеся*, эксперт Positive Technologies.*

Последние годы термин Advanced Persistent Threat стал ночным кошмаром как для ИБ, так и для бизнеса. Принципиальность новизны — изменение вектора целей и методов атакующих. В докладе будут рассмотрены основные методы заражения от социальной инжинерии до использования 0-day уязвимостей, рассмотрены причины массовости случаев, последствия, а также методы борьбы с данным видом атак.

Почему молчит антивирус (и куда при этом утекают онлайн-деньги).

Шевченко Алиса*, Esage Lab.*

Доклад о новейших исследованиях в области технологий цифровых атак. Тенденции, демо и новые подходы к защите.

Второй день работы конференции

10:00 – 11:40	**Круглый стол «Технологии безопасности систем ДБО»** *Конференц-зал (Ресторанный комплекс)*

Ведущие: *Представитель Управления К МВД России; Сычев Артем Михайлович, ОАО «Россельхозбанк»; Горелов Дмитрий Львович, компания «Актив»; Медведовский Илья Давидович, Digital Security.*

Проблемы ДБО, взгляд со стороны банка.
Сычев Артем Михайлович, *ОАО «Россельхозбанк».*

Где лежат деньги: результаты исследования российских ДБО за 2009-2011гг.
Синцов Алексей, *Digital Security.*

Обзор современных средств технической защиты клиентских мест дистанционного банковского обслуживания.
Горелов Дмитрий Львович, *компания «Актив».*

Уязвимости систем дистанционного банковского обслуживания.
Смышляев Станислав Витальевич, *инженер-аналитик, ООО «КРИПТО-ПРО».*

10:00 – 11:40	**Секция «Технологии защиты и нападения»** *Конференц-зал «Марс» (Конференц-комплекс)*

Ведущие: *Кислицин Никита, главный редактор журнала Хакер; Гордейчик Сергей, технический директор Positive Technologies.*

Невидимость исполняемого кода в Windows NT.
Гилязов Руслан Раджабович, *инженер-аналитик, ООО «КРИПТО-ПРО».*
Обобщен и структурирован известный материал по технологиям сокрытия и детектирования сокрытия исполняемого кода, проведен комплексный анализ используемых технологий защитного программного обеспечения и систем безопасности в операционных системах семейства Windows NT, дано практическое и теоретическое описание невидимых модулей в классе данных операционных систем. На основе полученных теоретических и практических результатов разработан программный продукт, позволяющий в скрытом режиме обходить системы безопасности существующего защитного программного обеспечения и систем безопасности Windows NT.

Некоторые подходы к оценке пропускной способности скрытых каналов в IP-сетях
Матвеев Сергей Васильевич, *Пензенский филиал ФГУП «НТЦ «Атлас».*
Организация скрытых каналов при подключении обособленного сегмента IP-сети к общедоступной сети посредством граничного маршрутизатора. Приводится перечень возможных скрытых каналов утечки информации, рассматриваются меры защиты от организации скрытых каналов, приводится расчет теоретической пропускной способности для некоторых видов скрытых каналов.

Новые техники защиты от старых угроз – обойти невозможно!
Ушаков Дмитрий Вячеславович, *руководитель отдела по подготовке технических решений Stonesoft Corp., к.т.н.*
Новые типы угроз для информационных систем, связанные с применением техник обхода (evasion techniques). Кто из крупных вендоров замалчивает и игнорирует эту проблему? Большинство решений остаются уязвимыми даже к ординарным техникам обхода, не говоря уже про их комбинации или применение динамических техник (AET).

Скрытые методы защиты информации и их применение для противодействия инсайдерам.

Гончаров Павел Игоревич, *ОАО «Концерн «Системпром»;* ***Миронов Алексей Геннадьевич,*** *ФСО России.*

В данном докладе представлены основные методы скрытого наблюдения за сотрудниками и их применение для выявления инсайдеров на основе поведенческого анализа.

Тренды сетевых атак, вызванных активными действиями пользователей: честная и нечестная монетизация бесплатных ресурсов. Данные за период: 12/2011-03/2012.

Кропотов Владимир Борисович, *аналитик ИБ, ТНК-ВР;* ***Ярочкин Федор Владимирович,*** *аналитик по безопасности, P1 Security , Академия Синика.*

Риски и последствия, связанные с попытками пользователей найти в Интернет и бесплатно скачать книги, музыку, видео, драйверы, обновления ПО и т.п. Примеры сайтов, анализ географического расположения подобных ресурсов, часть из которых находится в оффшорных зонах. Показаны зафиксированные системами защиты информации примеры того, как пользователи указывали свои данные, которые затем использовались для монетизации, и примеры поведения пользователей, чьи деньги «ушли» к владельцам подобных ресурсов.

12:00 – 13:30 Круглый стол «Рынок сетевой безопасности России на пути из прошлого в будущее»

Конференц-зал (Ресторанный комплекс)

Ведущий: *Рябко Сергей Дмитриевич, президент группы компаний «С-Терра».*

Участники:

- **Кадер Михаил Юрьевич**, заслуженный системный инженер, ООО «Сиско Систем»
- **Широков Василий Васильевич**, генеральный директор, Check Point Software Technologies Russia
- **Романов Михаил Юрьевич**, директор российского филиала, компания StoneSoft
- **Немошкалов Александр Михайлович**, менеджер по продуктам, ООО «Код безопасности», ГК «Информзащита»
- **Гусев Дмитрий Михайлович**, заместитель генерального директора, ОАО «Инфотекс»
- **Попов Владимир Олегович**, начальник отдела защиты информации, ООО «КРИПТО-ПРО»
- **Растренин Олег Валентинович**, генеральный директор, ЗАО «С-Терра СиЭсПи»
- **Федотов Андрей Владимирович**, заместитель начальника отдела разработки средств защиты информации и СКЗИ, ООО «Фактор ТС»
- **Кошелев Марк Юрьевич**, начальник отдела разработки программного обеспечения, ООО «ЭЛВИС-ПЛЮС».

12:00 – 13:30 Секция «Электронная подпись без границ»

Конференц-зал «Марс» (Конференц-комплекс)

Ведущие: *Домрачев Алексей Александрович, советник Департамента электронного правительства Министерства связи и массовых коммуникаций Российской Федерации; Кирюшкин Сергей Анатольевич, советник генерального директора «Газинформсервис».*

Легализация иностранных электронных документов в интернет экономике.

Домрачев Алексей Александрович, *советник Департамента электронного правительства Министерства связи и массовых коммуникаций РФ.*

Организация обмена юридически значимыми документами между участниками рынка.

Миклашевич Анатолий Вадимович, *исполнительный директор НП «РОСЭУ».*

Свободный обмен электронными первичными бухгалтерскими и другими юридически значимыми документами ограничен рамками сети отдельных операторов связи. Что необходимо для осуществления полной свободы этого обмена и что уже сделано для унификации разрозненных технологий обмена электронными документами.

Электронная цифровая подпись в опасности! Что делать?!

Комисаренко Владимир Владимирович, *начальник сектора управления защиты информации Оперативно-аналитического центра при Президенте Республики Беларусь;* ***Костевич Андрей Леонидович,*** *НИЛ НИИ ПМИ БГУ.*

В докладе будут рассмотрены основные проблемы, которые были выявлены при испытаниях и эксплуатации средств управления открытыми ключами и электронной цифровой подписи, и обозначены пути их решения.

Инфраструктура открытых ключей – унаследованные проблемы и попытки их решения.

Смирнов Алексей Анатольевич, *Information Security Officer, Parallels.*

Доклад посвящен современной ситуации с доверием к инфраструктуре открытых ключей в масштабах глобальной сети и предлагаемым способам решения сопутствующих проблем в условиях невозможности выделения дополнительных ресурсов на управление доверием со стороны пользователя.

Внедрение ЭП в автоматизированные трансграничные системы документооборота.

Кирюшкин Сергей Анатольевич, *советник генерального директора, ООО «Газинформсервис».*

В докладе рассматриваются ключевые аспекты интеграции электронной подписи в различные системы документооборота с возможностью трансграничного взаимодействия: реализация множественной подписи, доверенная третья сторона, электронная подпись, интерфейсы BHCryptography, интеграция с Citrix, Linux, MacOS, Com, Java, SharePoint, IIS, DVCS.

14:30 – 19:00	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал (Ресторанный комплекс)*

Ведущий: *Котенко Игорь Витальевич, д.т.н., профессор, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности, СПИИРАН.*

Часть 1 (14:30 – 16:10).

Аналитическое моделирование и анализ событий в системах управления информацией и событиями безопасности.

Котенко Игорь Витальевич, *Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Рассматривается общий подход к моделированию атак и анализу событий безопасности, предлагаемый для реализации в системах управления информацией и событиями безопасности. Подход основан на моделировании поведения злоумышленников, генерации графов атак, вычислении различных показателей безопасности и использовании процедур анализа рисков. Ключевыми элементами предлагаемых архитектурных решений являются: использование репозитория безопасности, эффективные методики генерации дерева атак, учет как известных атак, так и атак нулевого дня, стохастическое аналитическое моделирование и интерактивная поддержка принятия решений для выбора предпочтительных решений по безопасности.

Разграничение доступа и минимизация ущерба от атак с помощью сильного принципа наименьших привилегий.

Гамаюнов Денис, *Лаборатория вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова.*

Исследуется возможность реализации сильного принципа наименьших привилегий, при котором набор доступных привилегий меняется со временем - по ходу выполнения приложения. Рассмотрен один из вариантов реализации данного принципа в операционной системе семейства Linux для различных классов приложений, в том числе многопоточных, когда для каждого потока исполнения необходимо обеспечить независимый контроль привилегий.

О проблеме обоснования адекватности формальных моделей безопасности логического управления доступом и их реализации в компьютерных системах

Девянин Петр, *УМО ИБ, Москва.*

Рассматривается проблема синтеза формальных моделей безопасности логического управления доступом и обоснования адекватности их реализации в реальных компьютерных системах. Предлагается подход к поэтапному решению данной проблемы.

Проектирование защищенных информационно-телекоммуникационных систем со встроенными устройствами.

Хосе Франциско Руиз Родригез, *Университет г. Малага (Испания);* ***Десницкий Василий,*** *Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Модели и методики проектирования защищенных информационно-телекоммуникационных систем со встроенными устройствами. Обобщенная метамодель безопасности на основе средств языка моделирования UML, доменно-специфичная модель, определяемая экспертом в сфере некоторого проблемно-предметного домена (для описания семейств систем со сходной функциональностью и общими целями защиты) и методика конфигурирования устройств на основе решения оптимизационной задачи.

Часть 2 (16:30 – 19:00).

Анализ информационных потоков для построения защищенных систем со встроенными устройствами

Колин Фидж, *Технологический Университет Квинсленда (Австралия);* ***Чечулин Андрей,*** *Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Методики анализа информационных потоков для оценки защищенности систем со встроенными устройствами. Информационные потоки анализируются на трех уровнях (аппаратном, программном и сетевом) и на двух этапах (проектирования и реализации). Используется программное средство Secure Information Flow Analyser и методы верификации политик безопасности.

Know Thy Limits или возможности систем обнаружения веб-сайтов, распространяющих вредоносное программное обеспечение.

Петухов Андрей, *Лаборатория вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова.*

Исследуется эффективность средств обнаружения веб-сайтов, реализующих атаки Drive-by-Download – одного из самых распространенных способов доставки вредоносного программного обеспечения на компьютеры пользователей.

Модели и методы противодействия кибератакам на основе теории самоорганизации.

Петренко Сергей, *Военно-космическая академия имени А.Ф.Можайского.*

Рассматриваются подходы к созданию нового класса киберсистем с новыми системными свойствами. Для этого предлагаются модели и методы углубленной проработки семантики вычислительных процессов. Раскрываются соответствующие денотационная, аксиоматическая и операционная семантика вычислений в условиях кибератак.

Средства защиты информации в АСУ ТП – текущее состояние и перспективы развития.

Комаров Андрей, *Group-IB.*

Проводится анализ перспективных направлений и текущих результатов исследований по интеграции специализированных средств защиты информации в АСУ ТП с учетом требований по обеспечению непрерывного и безотказного функционирования. Представляются задачи фильтрации и анализа промышленных протоколов передачи данных, построения отказоустойчивых инфраструктур, дополнение защитных механизмов ОСРВ на примере QNX.

Гибридный метод обнаружения шеллкодов в высокоскоростных каналах передачи данных.

Гайворонская Светлана, *Лаборатория вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова.*

Рассматривается задача обнаружения шеллкодов - атак, эксплуатирующих ошибки переполнения буфера, в высокоскоростных каналах передачи данных. На основе выделенных характеристик вредоносного исполнимого кода произведено разбиение пространства шеллкодов на 19 частично-пересекающихся классов, а также составлена библиотека элементарных классификаторов - алгоритмов, обнаруживающих специфичные классы шеллкодов. Предлагается алгоритм построения гибридного классификатора шеллкодов.

Применение онтологического подхода и логического вывода для управления информацией и событиями безопасности.

Полубелова Ольга, *Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Предлагается применение онтологий, дескрипционных логик и логического вывода в системах управления информацией и событиями безопасности. Представляются задачи построения онтологии уязвимостей и анализа программно-аппаратных компонентов, приводящих к возникновению уязвимости. Приводится пример построения репозитория с гибридным хранилищем (реляционное, хранилище триплетов, XML-СУБД), обеспечивающим манипулирование данными о событиях безопасности через вебсервисы.

Механизмы визуализации в SIEM-системах.

Новикова Евгения, *СПбГЭТУ.*

Анализируются современные исследования в области визуального представления информации о событиях безопасности. Рассматривается роль, место, архитектура и перспективные способы реализации механизмов визуализации в системах управления информацией и событиями безопасности.

Верификация требований политик информационной безопасности в системах распределенных вычислений.

Коноплев Артем, *старший аналитик, ООО «НеоБИТ».*

Рассмотрена проблема обеспечения защищенности вычислительных и информационных ресурсов в грид-системах. Проанализированы особенности архитектуры грид-систем, построена модель угроз. Рассмотрены существующие меры по обеспечению безопасности грид-систем, указаны их недостатки. Построена модель безопасности грид-систем, позволяющая контролировать запросы пользователей грид-систем в соответствии с требованиями политик информационной безопасности и верифицировать указанные требования в среде с предустановленными отношениями.

Гетерогенные архитектуры массовых вычислений и новые угрозы кибербезопасности.

Баранович Андрей, Желтов Сергей, *Российский государственный гуманитарный университет, Институт информационных наук и технологий безопасности, Кафедра компьютерной безопасности, Кафедра компьютерной безопасности и математических методов управления, Математический факультет, Тверской государственный университет.*

Анализируются прогностические угрозы в отношении открытого киберпространства, связанные с появлением новых гетерогенных архитектур массовых вычислений, а именно, угрозы реализации несанкционированных «облачных» вычислений и угрозы массового использования гетерогенных архитектур и средств вычислений в целях снижения уровня защищенности асимметричных криптосистем, практическая стойкость которых базируется на сложности решения задач факторизации целых чисел и дискретного логарифмирования на алгебраических структурах.

Разметка сетевого трафика для анализа состояния информационной безопасности.

Качалин Алексей, *ЗАО «Перспективный Мониторинг».*

Рассматривается задачи сбора и исследования сетевого трафика на предмет выявления аномалий для дополнения результатов анализа состояния информационной безопасности автоматизированной информационной системы. Анализируются вопросы достаточности продолжительности и детальности сбора трафика, проблемы идентификации типов и источников трафика, критерии разметки трафика.

14:30 – 16:10	**Секция «Криптография в облачных решениях, безопасность информационных систем с размытыми контурами»** *Конференц-зал «Марс» (Конференц-комплекс)*

Ведущие: *Кузьмин Алексей Сергеевич, ФСБ России;* ***Соколов Александр Васильевич, АП КИТ;***
Климов Евгений Вячеславович, RISSPA.

Облачные вычисления. Виртуальная безопасность или безопасность виртуализации?

Зегжда Петр Дмитриевич, *д.т.н., профессор, Зав. кафедрой Информационной Безопасности Компьютерных Систем СПбГПУ.*

Использование кодовых методов для решения задач информационной безопасности в облачных системах хранения и обработки данных.

Беззатеев Сергей Валентинович, *д.т.н. , доц., зав.каф. технологий защиты информации, Санкт-Петербургский Государственный Университет Аэрокосмического Приборостроения.*

В докладе рассматриваются основные задачи информационной безопасности в облачных системах. Для их решения предлагается использовать единый подход на базе кодов, исправляющих ошибки. Рассматриваются многоуровневые схемы разграничения доступа, системы аутентификации, протоколы, обеспечивающие анонимность пользователей и их запросов.

Строгая аутентификация и квалифицированная электронная подпись для портальных решений и облачных сервисов.

Груздев Сергей Львович, *компания «Аладдин Р.Д.»*

На сегодняшний день традиционные способы получения квалифицированной электронной подписи в веб-ориентированных системах и облачных сервисах не удовлетворяют современным требованиям рынка, таким как легкость, масштабируемость и необходимость обеспечить безопасность работы в заведомо недоверенной среде. Решению перечисленных проблем с помощью новых технологий Аладдин Р.Д. и посвящен доклад.

Построение систем защиты корпоративной инфраструктуры мобильных средств связи на базе систем класса MDM.

Даниленко Антон, *директор Технического центра Научно-испытательного института систем обеспечения комплексной безопасности.*

Анализ современных угроз для корпоративной инфраструктуры мобильных средств связи, основные методы атак и возможности потенциальных злоумышленников с целью получения НСД к конфиденциальной информации. Рассматриваются существующие на настоящий момент корпоративные решения класса MDM (Mobile Device Managment), представляется решение класса MDM разработки НИИ СОКБ - система управления корпоративной сотовой связью SafePhone.

Шифрование данных в облачных инфраструктурах – обзор технологических подходов.

Бескоровайный Денис Игоревич, *RISSPA, Cloud Security Alliance Russian Chapter.*

Описание различных вариантов шифрования данных для различных архитектур облачных вычислений, как на стороне клиентов, так и на стороне провайдеров, с примерами решений. Для каждого варианта приводятся риски, которые снижаются благодаря использованию шифрования.

16:30 – 19:00	**Секция «Продукты и технологии информационной безопасности»** *Конференц-зал «Марс» (Конференц-комплекс)*

Ведущий: *Белявский Александр, коммерческий директор, SecurIT.*

Доверенный сеанс: позиционирование технологии.

Растренин Олег Валентинович, *генеральный директор ЗАО «С-Терра СиЭсПи».*

Технологии построения доверенного сеанса сегодня в фокусе внимания многих производителей. Предмет доклада – состав требований, масштабируемость для систем массового обслуживания, вопросы интеграции и типизации решений, простоты и удобства пользования, особенности «вертикальных» сценариев доверенного сеанса для различных сегментов рынка.

Насколько глубока «песочница».

Смирнов Николай, *начальник отдела научных исследований и развития продуктов ОАО «ИнфоТеКС.»*

В докладе рассматриваются плюсы и минусы типичного для мобильных платформ iOS и Android метода обеспечения информационной безопасности мобильных устройств, именуемого «песочницей» и представляющего собой жесткое разделение ресурсов среды функционирования приложений и методов обеспечения информационной безопасности в мобильных продуктах компании ИнфоТеКС.

DDoS-атака. Нападение и защита. Современные тенденции.

Полунин Алексей, *аналитик АИС.*

Угрозы DDoS известны достаточно давно, но в последнее время можно наблюдать заметную трансформацию как в проведении таких атак, так и в организации защиты от них. В докладе представлен анализ наиболее опасных воздействий и дана оценка методов защиты. Использованы материалы исследования, проведенного по заказу одного из крупных российских операторов связи.

Вторжение как разладка.

Баранов Василий, *СПбГПУ*

Результаты статистической обработки наблюдений над процессами с разладкой, моделирующими работу компьютерной системы с внедрением вируса.

Аппаратная аутентификация на Web-ресурсах. Можно ли сложное сделать простым?

Евгений Сухов, *руководитель отдела перспективных проектов, компания «Актив»*

Традиционная пара логин-пароль уязвима. Троянские программы, фишинг и перехват трафика позволяют злоумышленникам воровать эти данные. Рассказ о решении, которое позволяет свести к нулю риск кражи аутентификационных данных пользователей Web-приложений.

Компания «КРИПТО-ПРО»

С момента создания (2000 г.) компания КРИПТО-ПРО занимает лидирующее положение в области разработки средств криптографической защиты информации (СКЗИ) и развития Инфраструктуры Открытых Ключей (PKI) на территории РФ. Компания внесла существенный вклад в адаптацию международных рекомендаций применительно к российским криптографическим алгоритмам.

Специалистами КРИПТО-ПРО созданы:

- первое в России сертифицированное СКЗИ, интегрированное с операционной системой Microsoft Windows – КриптоПро CSP;
- первое в России сертифицированное средство обеспечения деятельности Удостоверяющих центров – КриптоПро УЦ;
- первые в России сертифицированные службы актуальных статусов сертификатов и штампов времени – КриптоПро OCSP и КриптоПро TSP;
- первый в России сертифицированный аппаратный криптографический модуль – Атликс HSM;
- первые в истории сообщества Интернет-стандарты, описывающие применение российских криптоалгоритмов – RFC 4357, RFC 4490, RFC 4491.

Продукты компании КРИПТО-ПРО широко используются в органах власти федерального и регионального уровней, в коммерческих организациях крупного, среднего и малого бизнеса. Это системы электронного документооборота, исполнения госзаказа, сдачи бухгалтерской и налоговой отчетности и т.п. Внедрение программных продуктов специалисты КРИПТО-ПРО сопровождают полным спектром консалтинговых услуг по применению электронно-цифровой подписи и шифрования. Компания ведет непрерывную разработку в целях улучшения имеющихся программных продуктов и создания нового ПО, призванного оперативно решать новые задачи, возникающие в сфере защиты информации. Решения КРИПТО-ПРО активно используются ведущими российскими и западными разработчиками IT-систем.

Контактная информация:
http://www.cryptopro.ru/
info@cryptopro.ru
+7 (495) 780-4820

Компания «Актив»

Компания «Актив» является ведущим российским разработчиком в сфере защиты информации и ведет свою деятельность с 1994 года. Компания занимается производством аппаратных средств аутентификации Рутокен, а также средств защиты программного обеспечения от нелегального копирования Guardant.

Продукция линейки Рутокен предназначена для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и электронной подписи (ЭП). USB-токены Рутокен являются ключевыми носителями в массовых российских проектах, базирующихся на технологии ЭП и инфраструктуре открытых ключей (PKI). Рутокен используется как самостоятельный продукт, так и в качестве одного из компонентов комплексных решений в области информационной безопасности. Основные сферы применения: системы дистанционного банковского обслуживания, электронные торги, информационные системы органов государственной власти, электронный документооборот B2B, B2C, G2B и внутрикорпоративный документооборот.

Продукция Рутокен имеет сертификаты ФСБ и ФСТЭК, подтверждающие соответствие требованиям к СКЗИ класса КС2 для защиты информации, не содержащей сведений, составляющих гос. тайну, и соответствие требованиям к техническим средствам защиты информации класса НДВ3, которые позволяют использовать идентификаторы Рутокен в системах, обрабатывающих конфиденциальную информацию, а также при работе с информацией, имеющей гриф «С».

Контактная информация:
http://aktiv-company.ru/
info@rutoken.ru
+7 (495) 925-7790

Компания «ИнфоТеКС»

ОАО «ИнфоТеКС» (Информационные Технологии и Коммуникационные Системы) — одна из ведущих High Tech компаний России, является лидером отечественного рынка программных VPN-решений и средств защиты информации в TCP/IP сетях, на рабочих станциях, серверах и мобильных компьютерах. ОАО «ИнфоТеКС» выполняет функции официальной секретарской компании Технического комитета по стандартизации №26 «Криптографическая защита информации». Компания осуществляет полный цикл разработки и технической поддержки целого спектра средств защиты информации ViPNet, рассчитанных на обработку информации ограниченного доступа, включая персональные данные:

- программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI);
- средства межсетевого экранирования и персональные сетевые экраны;
- средства шифрования данных, хранимых и обрабатываемых на компьютерах и в сети;
- системы централизованного управления и мониторинга СЗИ;
- средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы юридически значимого документооборота, порталы и т.п.).

Компания совместно со своими партнерами предлагает полный спектр услуг по проектированию и внедрению систем информационной безопасности на объектах любого уровня сложности:

- проведение обследований ИС;
- разработка и согласование моделей угроз и технических заданий на системы защиты ИС;
- разработка технических проектов на системы защиты ИС;
- установка и настройка средств защиты информации;
- аттестация объектов информатизации;
- техническое сопровождение;
- обучение специалистов заказчика.

Контактная информация:
http://www.infotecs.ru/
soft@infotecs.ru
+7 (495) 737-6192

Компания «Аладдин Р.Д.»

Компания «Аладдин Р.Д.» – ведущий российский разработчик и поставщик средств аутентификации, продуктов и решений для обеспечения информационной безопасности и защиты конфиденциальных данных. Компания была основана в апреле 1995 г. и на протяжении 16 лет является признанным экспертом, специализирующимся на комплексном подходе к решению задач аутентификации и защиты персональных данных. Используя перспективные западные технологии в области USB-токенов и смарт-карт, PKI и информационной безопасности, специалисты компании «Аладдин Р.Д.» создают лучшие отечественные решения для внедрения в рамках комплексных проектов.

«Аладдин Р.Д.» входит в пятерку лидирующих разработчиков российского рынка аппаратного обеспечения для информационной безопасности по итогам рейтинга IDC, ТОП-50 крупнейших ИТ-разработчиков России и ТОП-100 крупнейших ИТ-компаний России согласно рейтингам CNews. Продукты компании «Аладдин Р.Д.» неоднократно были удостоены званий «Продукт года», «Лучший инновационный продукт», «Лучший продукт в области информационной безопасности», «Продукт года в области защиты информации». Ряд продуктов компании имеет сертификаты ФСТЭК и ФСБ России.

Контактная информация:
http://www.aladdin-rd.ru
aladdin@aladdin-rd.ru
+7 (495) 223-0001

Компания «С-Терра СиЭсПи»

Российская компания «С-Терра» основана в 2003 году. Коллектив специалистов компании обладает уникальным многолетним опытом, который берет начало от разработки спецтехники связи и управления для спутниковых систем в советском ВПК, и включает дизайн коммуникационных протоколов, разработку программных продуктов и защищенных систем, а также создание первых продуктов в архитектуре IPSec.

Лицензиат ФСТЭК и ФСБ России с 2004 года, компания «С-Терра» обладает, в том числе лицензией на осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну.

Главная цель производственной деятельности компании – обеспечить российский рынок современными решениями для построения виртуальных частных сетей (VPN), применяя национальные криптографические стандарты при строгом соблюдении требований технического регулирования. Продукты компании в установленном порядке сертифицируются для защиты конфиденциальной информации и информационных систем обработки персональных данных.

Продукты компании «С-Терра» работают на аппаратных платформах как российских («Kraftway», ОКБ САПР), так и ведущих западных производителей (Cisco, HP, IBM, CrossBeam), при этом они с легкостью могут интегрироваться в архитектурные решения мирового лидера сетевой индустрии – Cisco Systems, технологическим партнером которого (Cisco Solution Technology Integrator) компания является с 2005 года. «С-Терра» – соорганизатор доверенного производства продукции компании Cisco в России, и в 2010 году впервые получила сертификаты ФСБ России на свои СКЗИ, применяемые на платформах Cisco. В 2011 году «С-Терра» первой в России и Восточной Европе стала продавать свои продукты компании Cisco как ПО от оригинального производителя Cisco (Cisco's supplier of choice for the locally certified network security software within Russia).

«С-Терра» предлагает российским заказчикам технически совершенные, органически входящие в сетевую инфраструктуру решения, которые характеризуются высокой масштабируемостью, что, наряду с корректным техническим балансом надежности и производительности, обеспечивает высокую экономическую эффективность.

«С-Терра» является ведущим поставщиком средств сетевой информационной безопасности в медицинскую отрасль, банковские структуры. Нам доверяют защиту своей информации такие компании федерального значения, как СИБУР, Норильский никель, МЧС, Почта России. Решения «С-Терра» предназначены для организаций, нуждающихся в надежной защите VPN-соединений с применением российской криптографии, например, для защиты конфиденциальной информации и персональных данных.

Контактная информация:
http://www.s-terra.com/
information@s-terra.com
+7 (499) 940-9061

Компания «Лаборатория Касперского»

«Лаборатория Касперского» – крупнейший в Европе производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама. Компания входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности. Продукты компании надежно защищают компьютеры и мобильные устройства более 300 млн. пользователей во всем мире, технологии используются в продуктах крупнейших мировых поставщиков программных и аппаратных решений.

Контактная информация:
http://www.kaspersky.ru/
sales@kaspersky.com
+7 (495) 797-8700

Компания «Газинформсервис»

ООО «Газинформсервис» — один из крупнейших в России системных интеграторов в области безопасности и разработчик уникальных программных продуктов, специализирующийся на создании систем информационной безопасности и систем обеспечения безопасности объектов для крупных корпораций энергетической и транспортной отраслей, органов государственной власти и местного самоуправления, а также учреждений финансового сектора и сектора здравоохранения.

Сегодня компания специализируется на разработке и внедрении комплексных систем информационной безопасности, внедрении и интеграции инженерных систем безопасности. В области информационных технологий и информационной безопасности «Газинформсервис» выполняет:

- разработку и внедрение уникальных средств защиты информации, комплексных систем информационной безопасности и информационных систем;
- аудит информационной безопасности;
- предоставление расширенного спектра услуг Удостоверяющего центра.

В области интегрированных инженерных систем безопасности «Газинформсервис» выполняет проектирование и внедрение интегрированных систем безопасности, инженерно-технической и антитеррористической защиты предприятий.

Кроме этого, «Газинформсервис» предлагает услуги испытательной лаборатории, проводит аттестацию объектов по требованиям безопасности, при необходимости обеспечивает подготовку специалистов на основе собственных учебно-методических материалов, в том числе с использованием технологий дистанционного обучения, осуществляет поставку оборудования и программного обеспечения.

Контактная информация:
http://www.gaz-is.ru/
resp@gaz-is.ru
+7 (812) 305-2050

Компания Check Point

Компания Check Point Software Technologies Ltd. — мировой лидер в области обеспечения интернет-безопасности, единственный поставщик средств обеспечения полной безопасности Total Security для сетей, данных и конечных узлов, объединенных единой средой управления. Компания Check Point предлагает клиентам высочайший уровень защиты от всех типов угроз, ее решения позволяют упростить управление безопасностью, а также снизить совокупную стоимость владения. Check Point разработала первое в отрасли решение Fire Wall-1 и реализованную в нем запатентованную технологию поиска угроз. Сегодня Check Point продолжает инновации, развивая Software Blade, динамическая архитектура которого позволяет создавать безопасные, гибкие и простые решения, способные полностью адаптироваться к требованиям безопасности любой организации или сетевой среды. Клиентами Check Point стали десятки тысяч предприятий и организаций всех масштабов, в том числе все компании, входящие в список Fortune-100. Отмеченные наградами решения Check Point Zone Alarm защищают миллионы клиентов от хакеров, шпионских программ и незаконного доступа к конфиденциальным данным.

Контактная информация:
http://rus.checkpoint.com/
+7 (495) 967- 74-44

Компания «Ростелеком»

ОАО «Ростелеком» – национальная телекоммуникационная компания России – является крупнейшей российской компанией отрасли.

В своем нынешнем виде компания существует с апреля 2011 года, когда к национальному оператору дальней связи ОАО «Ростелеком» присоединились межрегиональные компании связи ОАО «ЦентрТелеком», ОАО «Северо-Западный Телеком», ОАО «Южная телекоммуникационная компания», ОАО «ВолгаТелеком», ОАО «Уралсвязьинформ», ОАО «Сибирьтелеком», ОАО «Дальсвязь» и ОАО «Дагсвязьинформ».

Объединенная компания продолжила свою деятельность под брэндом «Ростелеком» («Российские телекоммуникации»), который по данным исследовательского холдинга «РОМИР», (www.romir.ru) является одним из самых сильных национальных брэндов, и входит в Top-10 по уровню доверия населения России.

Сегодня «Ростелеком» владеет комплексом государственных лицензий, позволяющих оказывать широкий спектр телекоммуникационных услуг во всех регионах Российской Федерации. Компания располагает самой большой магистральной сетью связи суммарной протяженностью около 500 тыс. км и уникальной инфраструктурой доступа к 35 млн. российских домохозяйств. В итоге различными услугами компании сегодня пользуются более 100 млн. жителей России.

«Ростелеком» является безусловным лидером российского рынка Интернет-услуг. Суммарная емкость клиентских подключений «Ростелекома» превышает 1,5 Тб/с, что кратно больше аналогичного показателя любой другой российской компании. Кроме того, «Ростелеком» лидирует по показателю качества Интернет-услуг, на протяжении длительного времени занимая верхнюю строку в рейтинге международного агентства Renesys (наиболее авторитетный рейтинг качества Интернет-услуг в мировой телекоммуникационной отрасли).

Сегодня «Ростелеком» является безусловным лидером рынка телекоммуникационных услуг для российских органов государственной власти всех уровней, государственных учреждений и организаций.

«Ростелеком» стал победителем всероссийского конкурса «Лидеры государственных и муниципальных закупок 2011» в номинации «Добросовестный поставщик». По итогам конкурса компания также внесена в Федеральный реестр добросовестных поставщиков.

В декабре 2011 года «Ростелеком» получил сертификат соответствия своей системы менеджмента качества (СМК) требованиям стандарта ISO 9001:2008 сертификационного органа AFNOR Certification, а также сертификат единого международного образца международной сети сертификации IQNet.

Высокое качество и надежность услуг компании «Ростелеком» подтверждены сертификатами соответствия Системы «Связь-Качество» (Система добровольной сертификации услуг связи, средств связи и систем менеджмента качества организаций связи) и Системы качества «ИНТЕРЭКОМС».

Основным акционером ОАО «Ростелеком» является государство, которое через ОАО «Связьинвест», Росимущество и Внешэкономбанк контролирует более 53% обыкновенных акций компании.

Контактная информация:
http://www.rt.ru/
info@rt.ru
+7 (499) 999-82-83

Ассоциация «РусКрипто»

Российская Криптологическая Ассоциация (Ассоциация "РусКрипто") – это общественная организация, объединяющая разработчиков и потребителей информационных технологий, которые заинтересованы в развитии открытой криптографии в России, а также в интеграции России в мировое информационное сообщество. Членами Ассоциации являются ведущие российские специалисты в области криптографии и информационной безопасности

Ассоциация «РусКрипто» ежегодно проводит одноименную конференцию. Конференция «РусКрипто» представляет собой базовую площадку для общения и обмена опытом специалистов в области криптографии и защиты информации. В ней участвуют разработчики и заказчики ИБ-решений, представители науки и образования, регуляторы и государственные чиновники.

«РусКрипто» позволяет участникам не только ознакомиться с передовыми технологиями и получить актуальную информацию о состоянии рынка средств криптозащиты, но и обсудить в неформальной обстановке задачи, которые ставят перед собой специалисты в области информационной безопасности. Аудитория конференции более 250 специалистов. География участников из года в год расширяется, охватывая как новые города России, так и страны СНГ и дальнего зарубежья.

Контактная информация:
http://www.ruscrypto.ru/
info@ruscrypto.ru

Академия Информационных Систем (АИС)

АИС – профессиональный учебный центр подготовки и переподготовки специалистов и руководителей в области информационных технологий, информационной безопасности, управления, международных систем менеджмента. Обучение проводится на основании государственных лицензий и аккредитаций, по окончании обучения слушателям выдаются государственные удостоверения и/или сертификаты вендоров.

- Очное обучение, повышение квалификации и профессиональная переподготовка
  - Авторизованное обучение и авторские курсы, Microsoft, Cisco Systems, Oracle, Check Point, TrendMicro, RIT Technologies, Watch Guard, ViPNet, Крипто Про, Mandriva, AltLinux, StoneGate, Redhat, McAfee и др.
  - Авторские курсы направлений: Linux/Unix, HUAWEI, Alcatel, Samsung & LG, AVAYA DEFINITY, Asterisk, IP-телефония и корпоративные сети, СКС
  - Системы виртуализации VMware, Xen
  - Обеспечение информационной безопасности (свыше 50 курсов), включая программы, согласованные с ФСТЭК России, ФСБ России, Банком России
  - Обучение по программам согласованным с профильными ассоциациями и партнерствами, такими как НП АБИСС, НАУФОР
  - Международные системы менеджмента ISO 9001, ISO 27001, BS 25999, ISO 20000, ISO 14001, PAS99 и др.
  - Конкурентная разведка
- Дистанционное интерактивное обучение в области информационных технологий, информационной безопасности и менеджмента.
- Организация и проведение деловых мероприятий.

Контактная информация:
http://infosystems.ru/
info@infosystem.ru
+7(495) 231-30-49

Даты	Название, место проведения	Сайт
12 апреля 2012 года	**Russian Open Source Summit 2012** *Москва, отель «Ренессанс»*	www.pcweek.ru/foss/conference/
11–16 сентября 2012 года	**XI всероссийская конференция «Информационная безопасность. Региональные аспекты». ИнфоБЕРЕГ-2012** *Сочи*	www.vipforum.ru
ноябрь 2012 года	**II Межбанковский форум «Информационная безопасность в кредитных и финансовых организациях Республики Казахстан»** *Казахстан, Алматы*	www. it-safety.kz
4 декабря 2012 года	**3-я Международная конференция «Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia»** *Москва, Конгресс-центр ТПП РФ*	www.antifraudrussia.ru
февраль 2013 года	**Конференция «ИТ Мобилизация»** *Австрия*	www.infosystems.ru
27–30 марта 2013 года	**15 международная конференция «РусКрипто'2013»** *Подмосковье*	www.ruscrypto.ru

Памятка участникам конференции

Общие правила для участников:

- Пропуск на территорию отеля в период проведения конференции осуществляется строго по спискам зарегистрированных участников.
- Питание на территории отеля организовано по системе «все включено» с 8:00 до 23:00. Время завтраков, обедов и ужинов для участников «РусКрипто'2012» указано в программе.

Трансфер в дни работы конференции (для участников, не проживающих на территории отеля):

- 29 марта в 8.00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel».
- 29 марта в 19.30 вечера трансфер отель «Солнечный Park Hotel» – м. Речной вокзал.
- 30 марта в 8.20 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel».
- 30 марта в 19.30 вечера трансфер отель «Солнечный Park Hotel» – м. Речной вокзал.

Внимание! Указано время отправления автобусов, просим подъезжать за 10-15 минут до времени отправления. В случае опоздания, заранее предупреждайте организаторов.

Организованный выезд из отеля «Солнечный Park Hotel»:

31 марта (суббота) в 12:00 автобусом до станции метро «Речной вокзал». Подача автобусов в 11:45 ч. у ворот отеля.

Внимание! Автобусы с табличкой «РусКрипто'2012» отправятся ровно в 12:00, просьба заранее сдать номера и не опаздывать.

Отель «Солнечный Park Hotel»:

Солнечногорский район, Ленинградское шоссе, 74 км

Телефон/факс: +7 (925) 922-42-00, +7 (499) 755-88-88

Расчетный час:

Заезд – 28 марта 2011 года в 17:00, выезд – 31 марта в 12:00.