Тайм-лайн конференции

30 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 - 21.00	Ужин. Свободное время
21.00 – 22.00	Шоу-программа «Welcome party». *Концертный зал ресторанного комплекса*

31 марта, четверг. Первый день работы конференции

8.00 – 9.45	Завтрак	
9.45 – 10.00	Регистрация участников конференции	
10.00- 11.30	**Открытие. Пленарное заседание.** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.3*	
11.30 - 12.00	Перерыв	
12.00 – 13.30	**Круглый стол "Российский рынок СКЗИ"** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.3*	**Закрытый мастер класс "Способы расследования компьютерных преступлений в кредитно-финансовой сфере"** *Конференц-зал 1* *Подробнее на стр.8*
13.30 – 14.30	Обед	
14.30 – 16.30	**Секция "Криптография и криптоанализ: теория и практика " Часть 1** *Конференц-зал 1* *Подробнее на стр.3*	**Секция «Интернет и информационная безопасность»** *Конференц-зал 2* *Подробнее на стр.6*
16.30 – 17.00	Перерыв	
17.00 – 18.30	**Секция "Криптография и криптоанализ: теория и практика " Часть 2** *Конференц-зал 1* *Подробнее на стр.3*	**Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»** *Конференц-зал 2* *Подробнее на стр.7*
19.30 – 22.30	Банкет в честь открытия конференции	

1 апреля, пятница. Второй день работы конференции

9.00 – 10.00	Завтрак		
10.00 – 11.20	**Секция «Преподавание криптографических дисциплин в высшей школе»** *Конференц-зал 1* *Подробнее на стр.9*	**Секция «Общие вопросы информационной безопасности»** *Конференц-зал 2* *Подробнее на стр.10*	**Соревнования РусКрипто CTF** *Подробнее на стр.9*
11.20 – 11.40	Перерыв		
11.40 – 13.00	**Секция «Преподавание криптографических дисциплин в высшей школе»** *Конференц-зал 1* *Подробнее на стр.9*	**Секция «Общие вопросы информационной безопасности»** *Конференц-зал 2* *Подробнее на стр10.*	
13.00 – 14.00	Обед		
14.00 – 16.00	**Секция «Академические исследования в сфере информационной безопасности»** *Конференц-зал 1* *Подробнее на стр.12*	**Секция «Криптография при оказании государственных услуг в электронном виде. Универсальная электронная карта»** *Конференц-зал 2* *Подробнее на стр.15*	**Соревнования РусКрипто CTF** *Подробнее на стр.9*
16.00 – 16.20	Перерыв		
16.20 – 18.00	**Секция «Академические исследования в сфере информационной безопасности»** *Конференц-зал 1* *Подробнее на стр.12*	**Мастер класс «Конкурентная разведка в интернет»** *Конференц-зал 2* *Подробнее на стр.16*	
19.00 - 20.00	Ужин		
20.00 – 20.30	**Награждение победителей номинаций конференции** *Лобби-бар*		
20.30 – 23.00	**Тематический игровой вечер в стиле «Чикаго»** *Развлекательный комплекс*		

2 апреля, 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	**Открытие. Пленарное заседание** *Конференц-зал (Ресторанный комплекс)*

Приветственное слово от оргкомитета конференции

Значение моделирования в криптографических исследованиях.
Баранов Александр Павлович, *первый заместитель начальника Центра ФСБ России, д.ф-м.н., с.н.с., председатель ТК26, действительный член Академии криптографии Российской Федерации*

Математические модели криптографии.
Жуков Алексей Евгеньевич, *к.ф.-м.н., доцент МГТУ им. Баумана, председатель совета директоров ассоциации «РусКрипто»*

Перспективные направления развития криптографии на современном этапе
Кузьмин Алексей Сергеевич, *заместитель начальника Центра ФСБ России, д.ф-м.н., профессор, действительный член Академии криптографии Российской Федерации*

Проблемы построения и функционирования больших систем информационной безопасности.
Попов Владимир Олегович, *к.ф.-м.н., Крипто-Про, директор Ассоциации «РусКрипто»*

12:00 – 13:30	**Круглый стол «Российский рынок СКЗИ»** *Конференц-зал (Ресторанный комплекс)*

Ведущие: *Баранов Александр Павлович, первый заместитель начальника Центра ФСБ России, д.ф-м.н., с.н.с., председатель ТК26, действительный член Академии криптографии Российской Федерации; Емельянов Геннадий Васильевич, Председатель Совета МОО «Ассоциация Защиты Информации».*

Участники: *Маслов Юрий Геннадьевич, Крипто-Про; Горелов Дмитрий Львович, компания Актив; Соколов Александр Васильевич, Ассоциация АП КИТ; Рябко Сергей Дмитриевич С-Терра СиЭсП и др.*

Сферы применения средств криптографической защиты информации. Требования рынка и регуляторов. Насущные проблемы и пути их решения. Вопросы совместимости, стандарты качества. К участию приглашены представители ФСБ России и ведущие эксперты отрасли.

14:30 – 18:30	**Секция «Криптография и криптоанализ: теория и практика».** *Конференц-зал 1 (Бизнес-центр)*

Ведущие: *Кузьмин Алексей Сергеевич, заместитель начальника Центра ФСБ России,*

д.ф-м.н., профессор, действительный член Академии криптографии Российской Федерации; Лунин Анатолий Васильевич, компания «ИнфоТеКС», заместитель секретаря технического комитета по стандартизации ТК 26; Попов Владимир Олегович, к.ф.-м.н., компания «Крипто-Про», директор Ассоциации «РусКрипто».

Традиционная секция конференции «РусКрипто». Российские и международные криптографические стандарты. Нюансы реализации и технологии использования. Реальные и мнимые уязвимости. Теоретическое обоснование стойкости криптографических алгоритмов. Криптографические протоколы, использование российских стандартов в международных криптографических протоколах. Новости криптологии.

О невозможных разностях блочных шифров на основе SL-преобразований.

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

За последние 10 лет разработан ряд блочных шифров на основе SL-преобразований, где S-нелинейный слой (слой s-боксов), L-линейный слой (линейное преобразование). В основе ряда шифров лежит алгоритм шифрования Фейстеля. Примерами данной конструкции служат шифры Camellia, MIBS. В докладе в зависимости от свойств линейного слоя L описываются классы невозможных разностей для разного числа раундов. Приводится иллюстрация полученных результатов на примере линейных преобразований, используемых в ряде блочных шифров.

Пас из-за границы - атака на ГОСТ.

***Алексей Чиликов,** к.ф.-м.н., МГТУ им. Н.Э. Баумана.*

ГОСТ 28147-89 в последнее время привлекает значительное внимание криптоаналитиков. До последнего времени он оставался одним из немногих "классических" алгоритмов, для которого не было опубликовано даже теоретических атак, понижающих стойкость в рамках "классических" моделей (known-plaintext attack, и т.п.). Но на конференции FSE 2011 японским исследователем Takanori Isobe была предложена атака на полную версию алгоритма шифрования, с общей сложностью ~2^225 (против 2^256 для полного перебора). В настоящем докладе подробно рассматривается данная атака, и связанные с ней особенности алгоритма ГОСТ. Также будет рассмотрен вопрос о границах практической применимости данной атаки.

О некоторых подходах к оценке эффективности методов криптографического анализа использующих связанные ключи.

***Владимир Рудской,** МГУ имени М.В. Ломоносова.*

В докладе показано, что если метод определения ключа алгоритма шифрования использует связанные ключи, то оценка его эффективности путем сравнения с методом полного перебора ключей является некорректной. Предложены два альтернативных подхода к решению этой задачи, которые приводят к одинаковым результатам.

О некоторых свойствах схем выработки общего ключа, использующих инфраструктуру открытых ключей, в контексте разработки стандартизированных криптографических решений.

***Матюхин Дмитрий Викторович,** ФСБ России.*

В докладе рассматриваются угрозы безопасности схем выработки общего ключа двумя абонентами по открытому каналу связи, участники которых используют долговременные ключевые пары с сертификатами открытых ключей. Проводится анализ защищенности от этих угроз

ряда схем, являющихся международными стандартами.

Открытые ключи на неассоциативных алгебраических структурах.

Нечаев Александр Александрович, *Академия криптографии Российской Федерации*

Открытый ключ на некоммутативных алгебраических структурах.

Нечаев Александр Александрович, *Академия криптографии Российской Федерации*

О деятельности технического комитета по стандартизации (ТК26) «Криптографическая защита информации».

Лунин Анатолий Васильевич, *компания «ИнфоТеКС», заместитель секретаря ТК по стандартизации «Криптографическая защита информации»*

В докладе будут освещены основные результаты деятельности технического комитета по стандартизации за прошедший год и направления его дальнейшей работы.

Гомоморфное шифрование. Защищенные облачные вычисления.

Кренделев Сергей Федорович, *к.ф.-м.н., доцент, лаборатория НГУ-Параллелс*

Что такое гомоморфная криптография. Для чего ее можно использовать. Что на самом деле придумали в IBM и почему это очень просто. Пример полностью гомоморфного шифрования для целых чисел.

О предложениях французских специалистов по международной стандартизации программного датчика случайных чисел на основе систем квадратичных уравнений.

Маршалко Григорий Борисович, Покровский Алексей Вячеславович*, ФСБ России*

В докладе приводятся основные положения стандарта ISO/IEC 18031, а также описание предложенного французскими специалистами ПДСЧ задаваемого системой квадратичных уравнений над полем. Приводятся основные результаты исследований по его анализу.

Теоретико-автоматные методы в криптографии.

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

Применение теоретико-автоматных методов в криптографии. Задачи решения автоматных уравнений с помощью построения различных приближенных моделей заданного автомата. Задачи оценки периодов выходных последовательностей автомата при заданной входной периодической последовательности и оценки мер их приближенных периодов.

Обеспечение безопасного доступа к ключам в слабозащищенных системах.

Гилязов Руслан Раджабович, *инженер-аналитик, Крипто-Про,*

Смышляев Станислав Витальевич, *инженер-аналитик, Крипто-Про*

Рассматриваются вопросы доступа к ключам в определенном классе компьютерных систем при повышенных требованиях к безопасности. Строится математическая модель и предлагается практический метод, позволяющий эффективно противодействовать технологиям перехвата вводимых паролей на ключевой контейнер, что в рассматриваемой модели решает задачу обеспечения безопасного доступа к ключам.

Технологии создания и применение вычислительных ошибок в микроконтроллере, реализующим криптографический алгоритм.

Коркикян Роман Геворкович, *Санкт Петербургский государственный университет телекоммуникаций.*

На примере конкретного микроконтроллера исследуются возможность использования сбоев в его работе для вычисления ключа криптографического алгоритма CRT RSA. Особое внима-

ние уделено вопросам преодоления защиты, основанной на операции условного сравнения.

Атака на основе коллизий на AES-подобные алгоритмы блочного шифрования.

Машошин Сергей Николаевич, *НИЯУ "МИФИ", факультет "Информационная безопасность", кафедра "Криптология и дискретная математика"*

В докладе проводилось исследование AES-подобных алгоритмов блочного шифрования. Была построена атака на основе коллизий на алгоритмы блочного шифрования W, Anubis, Square, аналогичная известной атаке на алгоритм блочного шифрования AES. Так же исследовалась зависимость трудоёмкости атаки от применения различных алгоритмов развертывания ключа, и было построено применение атаки с учётом алгоритмов развёртывания ключа.

14:30 – 16:30	**Секция «Интернет и информационная безопасность»** *Конференц-зал 2 (Бизнес-центр)*

Ведущий: *Сачков Илья Константинович, генеральный директор Group-IB.*

Вопросы информационной безопасности, связанные с использованием Интернет и сетевых технологий. Атаки на рабочие станции и серверы приложений, механизмы защиты Интернет-систем. Защита корпоративных систем, использующих Web-технологии. Практика построения защищенных систем, опыт реальных проектов.

Политико-экономические особенности адаптации облачных технологий в России.

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

В докладе рассказывается о политических и экономический причинах распространения облачных технологий в США и Европе и проводится анализ указанных причин в реалиях Российской действительности.

Киберпреступность в России: тенденции развития.

Сачков Илья, *генеральный директор Group-IB*

В докладе будет проведен комплексный анализ состояния рынка киберпреступности в России, в ходе которого будут подробно освещены основные услуги, его составляющие. Также докладчик обратиться к характеристике киберугроз, представляющих наибольшую общественную опасность, включая новые типы компьютерных преступлений. В заключении будут представлены практические примеры успешного противодействия хакерам.

Системы распределения трафика и новые аспекты поиска в нахождении вредоносного кода.

Гончаров Максим, *Старший Вирус Аналитик Trend Micro*

Теория и практика веб-трафика и возможности использования систем получения, фильтрации и его распределения. Как происходит фильтрация, по каким признакам и какими инструментами осуществляется, будет продемонстрировано на основе доступных систем распределения трафика. На примерах мы увидим, зачем используются системы распределения трафика и каким образом они могут послужить нечистым на руку интернет-предпринимателям.

Современная защита от сетевых угроз – безопасность реальна?

Ушаков Дмитрий Вячеславович, *Stonesoft*
Современные средства защиты содержат модули анализа трафика, которые выдают предупреждение по факту срабатывания некоторого правила, суть которого сводится к анализу последовательности символов в потоке информации. Соответственно критичным является корректный разбор и нормализация передаваемых данных. Злоумышленники пользуются этой особенностью и пытаются «обойти» механизмы детектирования с помощью различных методик. Техники обхода были известны еще с середины 90-х годов, однако лишь в прошлом году их подробное изучение позволило усомниться в адекватности применяемых средств обеспечения безопасности.

Сравнение эффективности средств обнаружения уязвимостей SQL injection.

Петухов Андрей Александрович, *Лаборатория Вычислительных Комплексов, факультет Вычислительной Математики и Кибернетики МГУ им. М.В.*
Доклад посвящен задаче сравнения эффективности сканеров веб-приложений в части обнаружения уязвимостей класса SQL Injection. Будет изложена методика построения тестового покрытия, описана процедура проведения тестирования и анализа результатов. Будут приведены результаты тестирования таких известных сканеров как sqlMap, skipfish, wapiti и acunetix.

Совершенствование систем классификации и оценки угроз информационной безопасности на основе анализа защищенности автоматизированных систем технологических процессов.

Комаров Андрей Андреевич, *технический директор НТЦ «Станкоинформзащита»*
Угрозы ИБ промышленных протоколов передачи данных, элементов АСУ ТП трактуют необходимость создания специализированной таксономии и классификации атак в отношении такого рода систем. Приводятся результаты исследований оценки защищенности АСУ ТП известных производителей, модель системы классификации.

17:00 – 18:30	**Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»** *Конференц-зал 2 (Бизнес-центр)*

Ведущий: *Беленко Андрей, CISSP, специалист по информационной безопасности компании "Элкомсофт".*

Секция посвящена вопросам, связанным с выполнением программного кода на недоверенных платформах: технологии защиты и взлома программного обеспечения; обфускация и деобфускация; вопросы DRM и задачи, которые нельзя решить, используя только криптографические методы.

Подделка цифровых подписей Canon.

Скляров Д.В., Беленко А.В., *компания Elcomsoft*
Многие зеркальные цифровые фотоаппараты Canon (все модели среднего и старшего уровня) имеют возможность генерации цифровых подписей для фотографируемых изображений. Эта подпись может быть проверена позднее для удостоверения того, что изображение не подвергалось редактированию. Цифровая подпись также защищает метаданные, такие как время и географические координаты. Проверка цифровой подписи широко применяется,

например, новостными агентствами для удостоверения аутентичности изображения. В докладе будет представлен анализ механизма цифровых подписей Canon и продемонстрирована возможность её подделки.

Поиск криптографических ключей в RAM.

Чиликов Алексей, *к. ф.-м. н., МГТУ им. Н.Э. Баумана*

В данной работе будут рассмотрены вопросы, связанные с поиском и распознаванием криптографических ключей в памяти "живой" системы. Предлагаются различные алгоритмы для решения указанных задач, включая не публиковавшиеся ранее. Также рассматриваются подходы, способные повысить стойкость систем к атакам по памяти.

Выбор точки внедрения для фаззинга в памяти.

Благодаренко Артем Васильевич, *Таганрогский Технологический Институт Южного Федерального Университета*

В данной работе предлагается алгоритм выбора точки программы для тестирования методом черного ящика. На основе статического и динамического анализа собираются данные о связях функций. Анализ связей позволяет построить рейтинг потенциального покрытия кода при тестировании методом черного ящика, начиная с заданной точки.

Диаген. Метод динамического контроля выполнения программы.

Маньков Евгений, *Руководитель группы разработки инструментальных средств "Газинформсервис"*

Метод позволяет контролировать потоки управления программы непосредственно в процессе ее функционирования. Программа предварительно проходит профилирование либо до компиляции – в исходном тексте, либо после компиляции - в исполняемом коде. Контроль осуществляется по автоматически созданному для программы автомату динамического контроля (АДК). АДК представляет собой программу, функционирующую параллельно контролируемой программе и под ее управлением, и содержит в своей реализации только разрешенные (доверенные) потоки управления.

11:30 – 13:30	**Закрытый мастер-класс «Способы расследования компьютерных преступлений в кредитно-финансовой сфере»** *Конференц-зал 1 (Бизнес-центр)*

Мастер-класс для сотрудников отделов информационной безопасности кредитно-финансовых организаций.

Ведущие: *Максим Суханов, ведущий специалист лаборатории компьютерной криминалистики Group-IB, Максим Гончаров, Старший Вирус Аналитик Trend Micro*

Компьютерные преступления: реагирование, минимизация ущерба без потери доказательств, расследование. Компьютерная криминалистика и контр-криминалистика. Мошенничество в ДБО и службы информационной безопасности в банках. Внутренние расследования собственными силами отдела безопасности.

Второй день работы конференции

10:00 – 16:00	**Студенческие соревнования РусКрипто CTF 2011** *Конференц-зал (Ресторанный комплекс)*

В рамках конференции состоится соревнование студенческих команд «РусКрипто CTF 2011». РусКрипто CTF - это открытое соревнование по защите информации, проводимое по принципам игры в Capture the flag (Захват флага).

Участники РусКрипто CTF 2011

- Команда «ХакерДом», УГУ им. А.М.Горького, Екатеринбург;
- Команда «SiBears», Томский государственный университет, Томск;
- Команда «Bushwhackers», МГУ, Москва;
- Команда «[Censored]», РГУ им И. Канта, Калининград;
- Команда «Ufologists», Технологический Институт Южного Федерального Университета, Таганрог.

Организаторы соревнования: Ассоциация «РусКрипто», НОУ «Академия Информационных Систем» и СПб ГУТ им. Бонч-Бруевича.

10:00 – 13:00	**Секция «Преподавание криптографических дисциплин в высшей школе»** *Конференц-зал 1 (Бизнес-центр)*

Ведущие: *Коваленко Андрей Петрович, ИКСИ Академии ФСБ России, Председатель УМО ИБ; Кузьмин Алексей Сергеевич, ФСБ России.*

Обсуждение новых федеральных образовательных стандартов. Преподавание криптографических дисциплин в ФГОС третьего поколения в области информационной безопасности. Организаторы секции: УМО ВУЗов по образованию в области информационной безопасности совместно с Институтом криптографии, связи и информатики Академии ФСБ России.

С целью более плодотворного обсуждения актуальных вопросов во время работы секции, участникам предлагается до начала конференции ознакомиться с проектами примерных программ учебных дисциплин по ФГОС, которые опубликованы на сайтах УМО ИБ и РусКрипто:

О преподавании криптографии для специалистов по защите информации (по специальностям 090301, 090302, 090303, 090305).

Шурупов Андрей Николаевич, *к.т.н., Фролов Андрей Александрович, лаборатория ТВП, г. Москва.*

Методические вопросы изучения криптографических приложений в системах и сетях связи (по специальности 090305).

Шалимов Игорь Анатольевич, *д.т.н., доцент, зам. председателя УМС по специальности 090302 УМО ИБ, г. Москва.*

О преподавании дисциплины «Криптографические протоколы» (по специальности 090301).

Черемушкин Александр Васильевич, *д.ф.-м.н., профессор, Институт криптографии, связи и информатики Академии ФСБ России, г. Москва.*

О преподавании дисциплины «Теоретико-числовые методы в криптографии» (по специальности 090301).

Пичкур А.Б., *к.ф.-м.н., доцент, Центр сертификации информации, г. Москва.*

Доклады посвящены обсуждению содержания, особенностей и методики преподавания в рамках новых федеральных государственных образовательных стандартов третьего поколения блока криптографических дисциплин для студентов, обучающихся по специальностям 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем», 090305 «Информационно-аналитические системы безопасности», входящим в группу специальностей 090300 «Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем».

Межрегиональные олимпиады школьников по математике и криптографии.

Сачков Владимир Николаевич, *д.ф.-м.н., профессор, Академия криптографии Российской Федерации,* ***Зубов А.Ю.,*** *к.ф.-м.н., доцент, Институт криптографии, связи и информатики Академии ФСБ России,* ***Язин А.В.,*** *к.ф.-м.н., УМО ИБ, г. Москва.*

В сообщении приводится краткая история и схема организации олимпиад по криптографии для школьников, проводимых уже на протяжении 20 лет. Обсуждается их роль в популяризации математических методов защиты информации и профессиональной ориентации будущих абитуриентов.

Спецкурс «Алгебраическая криптография» в МГТУ им. Баумана.

Пудовкина Марина*, к.ф.-м.н., доцент МГТУ им. Н.Э. Баумана, директор Ассоциации «РусКрипто»*

В докладе обсуждается спецкурс "Алгебраическая криптография", читаемый для студентов 5 курса кафедры "ИУ-8" МГТУ им. Н.Э. Баумана, обучающихся по специальности "Компьютерная безопасность". Спецкурс разделен на две основные части. Первая часть посвящена рассмотрению систем алгебраических уравнений, в частности, в ней вводятся базисы Гребнера, описываются способы их построения и обсуждается их применение в криптографии. Вторая часть спецкурса фокусируется на рассмотрении использования групп подстановок в криптографии.

10:00 – 13:00	**Секция «Общие вопросы информационной безопасности»** *Конференц-зал 2 (Бизнес-центр)*

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

Технические и методические доклады, посвященные технологиям информационной без-

опасности. Опыт реальных проектов и перспективные разработки.

Безопасность облачной платформы.

Симаков Сергей Владимирович, *Security Architect, Microsoft Global Security Center of Excellence*
Рассказ о стратегии компании Майкрософт в области безопасности облачных платформ. Новые продукты, стандарты, место криптографии в построении систем безопасности облачных продуктов.

Защищенный доступ к «облачному ПО (SaaS)».

Лаптев Андрей Владимирович, *ООО «СИС»*
Вопросы организации защищенного доступа к «облачному ПО». Проблемы, возникающие при переходе на «облачное ПО», и пути их решения на примере SafeNet Authentication Manager. Живая демонстрация.

Обобщенный алгоритм аутентификации в системах Pseudo-SSO.

Аверченко Кирилл Дмитриевич, *инженер-программист ООО «АНКАД»*
Системы единой аутентификации (Single Sign-on, SSO) помогают решить проблему хранения и использования множества пар «идентификатор (логин) – пароль» для доступа пользователя к различным ресурсам. Одним из двух базовых типов SSO-систем являются системы Pseudo-SSO. Доклад посвящен обобщенной схеме взаимодействия пользователя и модулей систем единой аутентификации в системах Pseudo-SSO.

Нет лицензий, а "работать" хочется?!

Белявский Александр, *коммерческий директор SecurIT.*
Что же можно делать в области ИБ без лицензий? Поставлять антивирусы, разрабатывать СУИБ, осуществлять работы по внедрению и настройке. А главное: какая реальная ответственность за работу без лицензии и кто защитит добросовестных участников рынка ИБ от контор, которым все равно, чем заниматься.

Тенденции развития технологии электронной цифровой подписи. Опыт Белоруссии.

Комисаренко Владимир Владимирович, *начальник группы оперативно-аналитического центра при Президенте РБ*
Подробный рассказ об опыте внедрения технологий электронной цифровой подписи в Республике Белоруссия. Развитие проектов, технологии, стандарты.

Методы построения высокопроизводительных систем защищенного взаимодействия на основе криптографических алгоритмов ГОСТ.

Афанасьев Алексей, *Директор специальных проектов, С-Терра СиЭсПи*
Сегодня как никогда важно не просто построение защищенного взаимодействия внутри территориально распределенных предприятий или между предприятиями, но и производительность таких сетей, учет требований регулятора. В докладе рассматриваются методы, позволяющие получить высокопроизводительные решение как в рамках одного устройства, так и на основе группы устройств, построенных на современной аппаратной базе (без применения специальных средств) и общепринятых стандартах и протоколах защищенного взаимодействия.

О реализации систем удалённого хранения ключей и формирования ЭЦП.

Смирнов Павел Владимирович, *к.т.н., ведущий специалист ООО «КРИПТО-ПРО»,*
Меньшенин Александр Олегович, *Демос*

Традиционные средства хранения ключей и формирования ЭЦП имеют ряд недостатков, которые ограничивают их распространение и являются препятствием на пути к повсеместному внедрению ЭЦП: они не дёшевы, имеют ограниченную мобильность, работают далеко не на всех платформах, подвержены рискам компрометации ключей. В докладе рассматривается подход к решению этих проблем путём реализации подписи и хранения ключей пользователей на стороне сервера (server-side signature).

14:00 – 18:00	**Секция «Академические исследования в сфере информационной безопасности».** *Конференц-зал 1 (Бизнес-центр)*

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

На секции обсуждаются вопросы построения перспективных механизмов и средств защиты информации в компьютерных сетях, в том числе криптографические механизмы защиты, управление доступом, идентификация, аутентификация и авторизация, защита встроенных устройств, адаптивные механизмы защиты информации, моделирование атак и механизмов защиты, обнаружение атак и вредоносного программного обеспечения, обманные системы и ловушки, защита от внутренних злоумышленников, интеллектуальный анализ данных и биологические подходы для защиты информации, защита информации на основе репутации и классификации объектов в Интернет и др.

О некоторых семантико-прагматических аспектах криптологии.

Баранович Андрей Евгеньевич, *д.т.н., профессор, Российский государственный гуманитарный университет, Институт информационных наук и технологий безопасности, Москва*

С общих позиций информационно-эволюционного подхода к системному анализу и моделированию сложных систем рассматривается ряд аспектов обеспечения информационной безопасности антропоморфных и антропогенных систем. Раскрываются аксиоматические основы теоретической криптосемантики - класса формальных обратимых преобразований семантики засекречиваемой информации (в историческом плане – “семантических шифров”), в отличие от криптографических шифров (в классической интерпретации К.Шеннона), определяемых на структурно-статистической модели множества открытых текстов и связанных с преобразованиями их формального семиотико-синтаксического представления в модели Дж. фон Неймана.

Моделирование и анализ механизмов кибербезопасности.

Котенко Игорь Витальевич, *д.т.н., профессор, лаборатория проблем компьютерной безопасности, СПИИРАН, г. Санкт-Петербург*

Доклад посвящен разработке методологического подхода к исследованию инфраструктурных атак и механизмов защиты от них на основе комплексного подхода к моделированию,

базирующегося на интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического моделирования, методов эмуляции и виртуализации сетевых процессов, моделей и методов использования зафиксированных записей трафика, генерации трафика на основе моделей и др.

Подходы к разработке формальных моделей управления доступом в защищенных операционных системах семейства LINUX.

Девянин Петр Николаевич, *д.т.н.*
Проскурин В.Г., *к.т.н., Институт криптографии, связи и информатики ФСБ РФ, г. Москва*

Представляются подходы к разработке на основе существующих моделей безопасности управления доступом и информационными потоками в компьютерных системах дискреционной ДП-модели управления доступом и информационными потоками в защищенных ОС и ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux.

Критерий Поппера и исследования в области сетевой безопасности.

Гамаюнов Денис Юрьевич, *к.ф.-м.н., Лаборатория Вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова*

Доклад посвящен вопросу применимости критерия Поппера к исследованиям в области защиты информации. В частности, рассматривается направление сетевой безопасности и борьбы с компьютерными атаками и вредоносным программным обеспечением. Констатируется отсутствие необходимых условий фальсифицируемости теорий, в частности, отсутствие практики опубликования экспериментальных данных. Существующие открытые наборы данных по компьютерным атакам (KDD Cup'99 dataset, VX Heavens dataset) значительно устарели. Новые и активно обновляющиеся банки данных являются де-факто закрытыми. Представляется целесообразным создание и поддержка сообществом исследователей, работающих в области сетевой безопасности, открытого банка данных с актуальными наборами как вредоносного программного обеспечения, так и частично обработанных результатах его анализа.

Метод генетической оптимизации схем ролевого доступа к информации.

Саенко Игорь Борисович, *д.т.н., профессор, лаборатория проблем компьютерной безопасности, СПИИРАН, г. Санкт-Петербург*

Предлагается метод генетической оптимизации схем ролевого разграничения доступа к информации. Постановка задачи оптимизации заключается в поиске такого множества ролей минимальной мощности, а также таких матриц, определяющих отношения "пользователь – роль" и "роль – ресурс", которые позволяют пользователям иметь доступ к тому и только к тому набору ресурсов, который необходим для их деятельности.

Методы обнаружения вредоносного исполнимого кода в высокоскоростных каналах передачи данных.

Гайворонская С.А., *Лаборатория Вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова*

Представляется задача обнаружения вредоносного исполнимого кода в высокоскоростных каналах передачи данных в рамках более общей проблемы обнаружения и фильтрации ботсетей на этапе их распространения. Рассматривается механизм распространения с помощью сетевых червей через уязвимости в распространенном программном обеспечении. Задача обнаружения формулируется как задача распознавания шеллкода в байтовом потоке данных, где для обнаружения шеллкода используется комбинация распознавателей отдельных

признаков шеллкода. Каждый распознаватель характеризуется полнотой обнаружения, уровнем ошибок и вычислительной сложностью.

Унификация процесса построения безопасных встроенных систем.

Десницкий Василий Алексеевич, *лаборатория проблем компьютерной безопасности, СПИИРАН, г. Санкт-Петербург*

Проводится анализ исследований в рамках проекта седьмой рамочной программы Еврокомиссии SecFutur, конечной целью которых является формирование унифицированного процесса построения безопасных встроенных систем. Среди основных задач, являющихся предметом исследования в настоящее время, выделяются задачи построения абстрактной модели встроенных систем, разработки среды тестирования безопасности встроенных систем и построение конфигурационной модели встроенных систем.

Категорирование веб-сайтов для систем блокирования веб-страниц с неприемлемым содержимым.

Комашинский Дмитрий Владимирович, *F-Secure, Финляндия, г. Хельсинки*

Рассматривается процесс разработки и реализации общего подхода к категоризации Web-контента, служащего для решения актуальной в настоящее время задачи категорирования Web-сайтов для систем защиты пользователя от доступа к объектам с неприемлемым содержимым (например, для систем родительского контроля, обеспечивающих блокирование доступа к страницам, тематически относящимся к нежелательным категориям). Описывается интегрированный комплекс классификаторов Web-сайтов, осуществляющих их категорирование на основе анализа URL, текста сайта, отдельных областей текста, связей между сайтами и т.д.

Моделирование противодействия бот-сетей и механизмов защиты от них.

Коновалов Алексей Михайлович, *ЗАО "Аркадия", г. Санкт-Петербург*

Предлагается подход и реализованные модели, предназначенные для имитационного моделирования бот-сетей и механизмов защиты от них. В докладе анализируются сценарии формирования бот-сети, управления бот-сетью и реализации некоторых инфраструктурных атак, выполняемых с помощью бот-сетей, а также различные методы защиты. Для выполнения имитационного моделирования использована разработанная многоуровневая инструментальная среда, реализованная на основе средств OMNeT++, библиотек INET Framework, ReaSE, а также собственных программных компонент.

Применение метода R-функций в задачах биометрической идентификации.

Басараб М.А., Домрачева А.Б., *Московский государственный технический университет им. Н.Э. Баумана*

Методом R-функций (RFM) построены модели контуров и поверхностей, описывающих кисть руки человека. В отличие от сеточных методов, в RFM геометрия сложного объекта описывается единым аналитическим выражением, которое может быть применено при разработке новых алгоритмов биометрической идентификации.

14:00 – 16:00	**Секция «Криптография при оказании государственных услуг в электронном виде. Универсальная электронная карта»** *Конференц-зал 2 (Бизнес-центр)*

Ведущие: *Баранов Александр Павлович, первый заместитель начальника Центра ФСБ России, д.ф-м.н., с.н.с., председатель ТК26, действительный член Академии криптографии Российской Федерации; Загорский Игорь Иванович, Минкомсвязь России; Звейник Владимир Карлович, начальник управления безопасности ОАО «Универсальная электронная карта».*

Инфраструктура электронного государства требует серьезных вложений в ИБ. Какие требования предъявляются к криптографическим подсистемам, как должны быть использованы технологии шифрования и электронной цифровой подписи? Перспективы развития проектов электронного государства. Требования организаторов системы к российским разработчикам средств информационной безопасности.

Механизмы защиты, реализуемые в единой платежно-сервисной системе универсальной электронной карты.

Азин Дмитрий Вячеславович, *главный специалист отдела методологии управления технологий и методологии ОАО «Универсальная электронная карта»*

Рассматриваются предпосылки создания единой платежно-сервисной системы универсальной электронной карты. Показаны планируемые к использованию механизмы защиты, инфраструктура ключей и сертификатов, сочетание применения зарубежных и российских криптографических стандартов в системе.

Новые инициативы Европейского союза в области электронной подписи.

Смирнов Павел Владимирович, *к.т.н., МИФИ*

Рассматривается опыт Европейского союза по взаимодействию различных систем, использующих электронную подпись. Освещаются нормотворческие инициативы по улучшению их взаимодействия: распределённая верификация подписи, стандартизация форматов подписанных документов, методы трансграничной аутентификации.

Тема доклада уточняется.

Загорский Игорь Иванович, *заместитель директора департамента государственной политики в области создания и развития электронного правительства, Минкомсвязь России*

Крупный удостоверяющий центр. Подводная часть айсберга.

Баранов Никита Валерьевич, *руководитель направления «Услуги Удостоверяющего центра» компании «СКБ Контур».*

Что скрыто за фасадом действительно большого удостоверяющего центра, который функционирует в режиме 24*7 и в день выпускает тысячи сертификатов? Как это все работает и почему организовано именно так.

16:20 – 18:00	**Мастер класс «Конкурентная разведка в Интернете»** *Конференц-зал 2 (Бизнес-центр)*

Ведущий: *Масалович Андрей, руководитель направления конкурентной разведки, «Академия Информационных Систем».*

Методы и приемы раннего обнаружения утечек конфиденциальной информации.

Новые методы защиты и скрытия чувствительной информации (стеганография, легендирование, маркировка).

Методы сбора информации о компании и персоне без нарушения закона «О коммерческой тайне» и закона «О персональных данных».

Методы и приемы поиска в глубинном (невидимом) Интернете.

Методики экспресс-аудита защищенности конфиденциальной информации от действий инсайдеров, рейдеров и мошенников.

Генеральный спонсор конференции

Компания КРИПТО-ПРО была основана в 2000 году. С момента создания 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 (ЭЦП) и шифрования. Помимо этого, компания оказывает услуги удостоверяющего центра.

Решения КРИПТО-ПРО активно используются ведущими российскими и западными разработчиками IT-систем.

За выдающиеся достижения в области информационной безопасности в 2007 году ООО «КРИПТО-ПРО» стало лауреатом премии «За укрепление безопасности России» (ЗУБР-2007), а часть продуктов компании была удостоена Золотых медалей.

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» указано в программе.

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

- 31 марта в 8.00 утра трансферт м.Речной вокзал – отель «Солнечный Park Hotel».
- 31 марта в 19.30 вечера трансферт отель – м. Речной вокзал.
- 1 апреля в 8.00 утра трансферт м. Речной вокзал – отель.
- 1 апреля в 19.30 вечера трансферт отель – 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»:

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

Внимание! Автобусы с табличкой «РусКрипто’2011» 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 – 31 марта 2011 года в 17-00, выезд – 2 апреля в 12-00.