Программа конференции

День заезда. 2 апреля, четверг		
18:00 – 19:00	Регистрация и расселение участников в пансионате «Липки»	
18:30 – 20:00	Ужин	
20:00 – 23:00	Пивная вечеринка от спонсоров, знакомство участников конференции	
День первый. 3 апреля, пятница		
9:00 – 10:00	Завтрак	
10:00 – 10:20	**Открытие конференции, приветственные доклады** *Большой зал*	
10:20 – 11:40	**Круглый стол «Российский рынок информационной безопасности. Прогнозы и перспективы»** *Большой зал* ***Подробнее на стр.2***	
11:40 – 12:00	Кофе-брейк	
12:00 – 13:40	**Секция «Электронный документооборот. Защищенный и/или с ЭЦП»** *Большой зал* ***Подробнее на стр.2***	
13:40 – 15:00	Обед	
15:00 – 17:20	**Секция «Общие вопросы информационной безопасности»** *Большой зал* ***Подробнее на стр.3***	**Секция «Защита персональных данных. Вопросы и ответы»** *Малый зал №2* ***Подробнее на стр.4***
17:20 – 17:40	Кофе-брейк	
17:40 – 18:40	**Круглый стол «Compliance management по-русски»** *Большой зал* ***Подробнее на стр.6***	**Блок докладов «Последние достижения мировой криптографии»** *Малый зал №2* ***Подробнее на стр.6***
19:00 – 23:00	Официальный банкет конференции «РусКрипто»	
День второй. 4 апреля, суббота		**с 9:00 до 15:00**
9:00 – 10:00	Завтрак	
10:30 – 11:30	**Секция «Интернет и информационная безопасность»** *Большой зал* ***Подробнее на стр.7***	**Секция «Криптография: теория и практика»** *Малый зал №2* ***Подробнее на стр.9***
11:30 – 11:50	Кофе-брейк	
11:50 – 13:40	**Секция «Интернет и информационная безопасность»** *Большой зал* ***Подробнее на стр.8***	**Секция «Криптография: теория и практика»** *Малый зал №2* ***Подробнее на стр.10***
13:40 – 15:00	Обед	

День второй. 4 апреля, суббота				**с 15:00 до 22:00**
15:00 – 16:20	**Блок докладов «Как обманывают клиентов производители средств защиты»** *Большой зал* ***Подробнее на стр.11***		**Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»** *Малый зал №2* ***Подробнее на стр.12***	
16:20 – 16:40	Кофе-брейк			
16:40 – 18:40	**Научная секция «Защита информации в распределенных компьютерных системах». Часть 1** *Большой зал* ***Подробнее на стр.14***		**Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»** *Малый зал №2* ***Подробнее на стр.13***	
18:40 – 20:00	Ужин			
20:00 – 22:00	**Вечерняя rump-session** *Малый зал №2*			
День третий. 5 апреля, воскресенье				
9:00 – 10:00	Завтрак			
10:00 – 11:00	**Секция «Свободное ПО и информационная безопасность»** *Большой зал* ***Подробнее на стр.16***	**Научная секция «Защита информации в распределенных компьютерных системах». Часть 2** *Малый зал №2* ***Подробнее на стр.17***	**Студенческий день** *Малый зал №1* ***Подробнее на стр.19***	
11:00 – 12:00		**Секция «Доклады победителей конкурса докладов»** *Малый зал №2* ***Подробнее на стр.17***		
12:00 – 12:30	Кофе-брейк			
12:30 – 13:30	**Подведение итогов, закрытие конференции** *Большой зал*			
13:30 – 15:00	Обед			
15:30	Отъезд в Москву			

10:00 – 10:20	**Открытие конференции, приветственные доклады** *Большой зал*
10:20 – 11:40	**Круглый стол «Российский рынок информационной безопасности. Прогнозы и перспективы»** *Большой зал*

Ведущие эксперты отрасли обсудят перспективы развития рынка информационной безопасности. В каких направлениях будет двигаться развитие основных сегментов рынка? Какие угрозы станут наиболее актуальными в ближайшем будущем? В чем основные проблемы? Как изменился рынок из-за мирового финансового кризиса?

Участники:

- Юрий Аксененко, председатель, Центр безопасности информации (ЦБИ)
- Игорь Курепкин, заместитель генерального директора, компания «Крипто-Про»
- Дмитрий Горелов, коммерческий директор, компания «Актив»
- Сергей Рябко, генеральный директор, С-Терра СиЭсПи
- Сергей Романовский, Директор департамента информационной безопасности, АМТ-груп

Модератор: Александр Власов, издатель журнала Information Security

12:00 – 13:40	**Секция «Электронный документооборот. Защищенный и/или с ЭЦП».** *Большой зал*

Почти все коммерческие системы документооборота декларируют защищенность, юридическую значимость. Идет масса внедрений таких систем, этот рынок бурно растет. С какими проблемами сталкиваются заказчики и разработчики? Какие практические рекомендации могут дать те, кто уже имеет реальный опыт? Что нового предлагают разработчики? Цель секции — обмен реальным опытом, ответы на сложные вопросы, рассказ о новых технологиях.

Модератор: Юрий Маслов, коммерческий директор, компания «Крипто-Про»

Практический опыт эксплуатации систем юридически значимого электронного документооборота

Юрий Маслов, коммерческий директор, ООО «Крипто-Про»

В докладе будут рассмотрены реальные споры и конфликты, связанные с реализацией уязвимостей в действующих системах электронного документооборота. Будут приведены рекомендации по ликвидации уязвимостей, предотвращению их появления и минимизации ущерба в случае их реализации. Также будут приведены основные критерии выбора и способы организации удостоверяющего центра, положительные и отрицательные стороны основных вариантов. Это поможет значительно оптимизировать расходы на применение ЭЦП в системах электронного документооборота. Будут рассмотрены примеры практического опыта эксплуатации систем юридически значимого электронного документооборота.

Информационный обмен между изолированными системами

Сергей Мургов, генеральный директор, ООО «Топ Кросс»

Доклад описывает технологии использования атрибутного сертификата в связке с электронным

документом для инкапсуляции документов, исходящих из системы электронного документооборота во внешние системы.

Защита авторских прав в Интернете с применением ЭЦП

Никита Биге, ведущий специалист, ЗАО «Сигнал-КОМ»

В докладе рассматривается вопрос использования штампов времени в электронном документообороте, при архивном хранении и в иных ситуациях. Дается оценка использования штампов времени для защиты авторских прав на материалы, опубликованные в Интернете.

Дистанционное обучение в области криптографии

Мельников Максим Русланович, начальник отдела дистанционного обучения, АИС

Дистанционное обучение на сегодняшний момент является весьма технологичным и эффективным средством обучения. Однако обучение ЭЦП проходило в основном в очной форме, что в свою очередь связано со сложностью реализации таких дистанционных учебных курсов. Академия Информационных Систем предлагает специализированный методологический подход и техническую реализацию дистанционных учебных курсов по криптографии.

Дискуссия

Обсуждение насущных вопросов. Краткие выступления потребителей об их опыте использования СЭД вместе с ЭЦП. Ответы экспертов на любые вопросы из зала, посвященные теме секции.

15:00 – 17:20 Секция «Общие вопросы информационной безопасности»

Большой зал

Секция посвящена комплексным системам обеспечения информационной безопасности, системам прозрачного шифрования, корпоративным продуктам защиты данных, современных технологиям защиты от внешних и внутренних угроз.

Модератор: Александр Иванов, к.ф.-м.н., директор ассоциации «РусКрипто», ведущий аналитик компании InfoWatch

Шифрование данных, корпоративные решения

Александр Иванов, к.ф.-м.н., директор ассоциации «РусКрипто»

В докладе анализируются отечественные и зарубежные решения, осуществляющие защиту данных путем шифрования и ориентированные на применение в корпоративной информационной сети с использованием централизованной политики безопасности. Основной акцент сделан на угрозы безопасности, которые находятся в центре внимания разработчиков средств защиты, и на те технологии, которые применяются для противодействия им.

Концепция безопасности IPC (Information Protection and Control)

Александр Белявский, коммерческий директор, SecurIT

Концепция систем IPC объединяет в себе методы DLP для контроля возможных каналов утечки (интернет, электронная почта, мобильные накопители, принтеры), шифрование для защиты информации на носителях (жесткие диски, магнитные ленты) и на ноутбуках, а также средства аутентификации пользователей.

Презентация нового электронного идентификатора Rutoken Flash

Дмитрий Горелов, коммерческий директор, компания «Актив»

Презентация нового аппаратного решения для аутентификации, ЭЦП и защиты информации от

постоянного спонсора конференции «РусКрипто» компании «Актив».

Технология authenticode на вооружении у службы вирусного мониторинга

С. И. Уласень; Г. К. Резников; к.т.н., с.н.с., ОДО «ВирусБлокАда»

Абсолютное количество файлов возрастает с каждым днем. При этом возрастает нагрузка на службы вирусного мониторинга, в задачу которых входит поиск в данной массе вредоносных файлов. Также вирусным аналитикам приходится решать и обратную задачу – отделение из общей массы заведомо чистых файлов. Еще одной проблемой, которую приходится решать антивирусным компаниям, стало уменьшение числа ложных срабатываний (false positives) и снижение отрицательных последствий, которые данные ложные срабатывания вызывают. Как технология Authenticode помогает решить поставленные задачи?

Архитектура и стратегия ИБ на предприятии

Алексей Лукацкий, бизнес-консультант, Cisco Systems

Часто в повседневной работе служб ИБ приходится сталкиваться с несогласованностью различных подразделений, участвующих в процедуре ИБ, – ИТ, СБ, ИБ, HR, юридический департамент, внутренний контроль и т.п. Да и сама служба нередко упускает из виду различные, нечасто возникающие, а потому забываемые вопросы. А все потому, что в компании отсутствует архитектура желаемой, ИБ и нет плана ее достижения, т.е. стратегии ИБ. Мы посмотрим, что включают эти понятия, и какие особенности их построения существуют.

Восстановление паролей с помощью графических карт

Андрей Беленко, аналитик по информационной безопасности, «Элкомсофт»

Аудит паролей традиционно требует больших вычислительных мощностей, и скоростей обычных процессоров во многих случаях уже не хватает. Для решения этой проблемы некоторые компании предлагают специализированные и дорогостоящие аппаратные ускорители. Но ускорить аудит можно и с помощью обычных видеокарт, о чем и будет подробно рассказано в данном докладе.

Новые возможности защиты информации при помощи решений Лаборатории Касперского. Контроль за интернет-трафиком и управление устройствами

Гуськов Владимир, технический директор, Софтакс

В докладе освещаются вопросы эволюции комплексов по обеспечению информационной безопасности на примере продуктов Лаборатории Касперского. В частности, участники конференции узнают о новых функциях в 9-ой версии Антивируса Касперского, таких как: диспетчер подключенных устройств и система контроля за интернет-трафиком.

15:00 – 17:20	**Секция «Защита персональных данных. Вопросы и ответы»** *Малый зал №2*

Федеральный закон о защите персональных данных уже действует, появился опыт внедрения систем ИБ, учитывающих требования этого закона. Созданы методики и опубликованы разъясняющие документы. Но вопросы остались.

Как должны модифицировать свои информационные системы операторы персональных данных? Какие новые возможности должны добавить в свои решения разработчики систем информационной безопасности?
Модератор: Аксененко Юрий Иванович, председатель, Центр безопасности информации (ЦБИ)

Практический опыт реализации требований по защите ПДн

Аксененко Юрий Иванович, председатель, Центр безопасности информации (ЦБИ)
В связи с принятием закона «О персональных данных» и выпуском ряда нормативных документов проблема защиты ПДн получила значительный общественный резонанс. Основываясь на результатах практической работы в этой области, в докладе демонстрируется, что при наличии желания и достаточного уровня квалификации можно решить значительную часть технологических проблем защиты ПДн, не тратя на это существенную долю бюджета организации. В качестве примеров рассмотрены вопросы рациональной организации информационных ресурсов и применения эффективных информационных технологий, процедуры классификации ИСПДн и типовые решения по защите ПДн в малобюджетной сфере.

Защита персональных данных

Черкас Юрий Владимирович, эксперт в области защиты персональных данных, Рэйнвокс
С принятием закона «О персональных данных» все операторы персональных данных обязаны создать систему защиты, адекватную существующим угрозам, до 01.01.2010 года. При этом методы кражи информации, мошенничества и несанкционированного доступа совершенствуются каждый день. В докладе рассмотрены способы снижения рисков, связанных с возможной утечкой персональных данных, а также методы повышения лояльности и доверия клиентов.

Повышение осведомленности сотрудников компании в вопросах ИБ как один из ключевых аспектов обеспечения защиты персональных данных

Хайров Игорь Евгеньевич, проректор по информационной безопасности, Академия Информационных Систем (АИС)
В докладе рассматриваются основные мероприятия, позволяющие повысить осведомленность сотрудников компании в вопросах обеспечения информационной безопасности. Основной упор делается на повышении уровня компетентности с помощью современных дистанционных технологий.

Проблемные вопросы защиты персональных данных

Сухинин Борис Михайлович, заместитель директора департамента проектов, НПО «Эшелон»
Доклад посвящен проблемным вопросам защиты персональных данных с учетом последних изменений законодательства РФ. В докладе освещены вопросы, связанные с требованиями, предъявляемыми к операторам персональных данных на законодательном уровне (федеральный закон «О персональных данных», Постановления Правительства РФ № 781 и № 687, Приказ «Об утверждении Порядка проведения классификации информационных систем персональных данных»), и требованиями по технической защите персональных данных (документы ФСТЭК России). Также подробно рассматривается общая последовательность действий при построении системы защиты, позволяющая выполнить указанные требования и при этом минимизировать затраты.

17:40 – 18:40	**Круглый стол «Compliance management по-русски»** *Большой зал*

Новомодный термин «Compliance management» присутствует сейчас в описании практически любого средства защиты и в описании услуг большинства игроков рынка ИБ. Что означают эти слова на практике? Сколько стоит «соответствие стандартам»? Стоит ли вообще задумываться о «Compliance management»?

Участвуют эксперты:

- Тарас Иващенко, специалист департамента аудита, компания «Информзащита»;
- Олег Слепов, Инфосистемы Джет;
- Сергей Гордейчик, руководитель отдела консалтинга и аудита, Positive Technologies.

Модератор — Валерий Коржов, обозреватель Computerworld Россия, ведущий ленты новостей портала www.osp.ru по теме «Информационная безопасность».

17:40 – 18:40	**Блок докладов «Последние достижения мировой криптографии»** *Малый зал №2*

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

- Марина Пудовкина, к.ф.-м.н. доцент МИФИ, директор ассоциации «РусКрипто»
- Жуков Алексей Евгеньевич, к.ф.-м.н. доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто»

10:30 – 11:30

Секция «Интернет и информационная безопасность»

Большой зал

Доклады секции охватывают анализ защищенности, сетевые атаки на рабочие станции и серверы приложений, современные механизмы защиты Интернет-систем, тестирование на проникновение. Подсекция безопасности Web-приложений посвящена защите корпоративных и Интернет-систем, использующих Web-технологии.

Специальный гость секции, Rocky Witt из компании Immunity, поделится своим опытом в вопросах проведения тестов на проникновение.

Модератор: Сергей Гордейчик, руководитель отдела консалтинга и аудита, Positive Technologies.

Тенденции борьбы с киберпреступностью в России. Аналитическая сводка по бот-сетям в РФ и в СНГ

Илья Сачков, генеральный директор, Группа информационной безопасности Group-IB

Количество инцидентов информационной безопасности. Соотношение между бюджетами, отводимыми на информационную безопасность, и количеством инцидентов. Проблемы расследования ИБ-инцидентов и преступлений в России. Что нам нужно сделать? Обзор и общая информация о бот-сетях в России и СНГ. В чем особенность данных сетей, их специфические отличия и общие сходства с такими же сетями за рубежами России? В чем заключается бизнес людей, которые создают бот-сети? Возможные связи людей из РФ с такими же группами за гра-ницей. Способы получения денег и легализация. Примеры конкретных групп. Полный цикл работ данных групп над определенным проектом. Внутрироссийские войны (банки, фирмы), в которых используются данные технологии. Способы расследования DDOS атак.

Бизнес против пентестов или пентесты для бизнеса или пентесты как бизнес?

Сергей Гордейчик, руководитель отдела аудита и консалтинга, Positive Technologies

В чем суть тестирования на проникновение? Как отличить «правильный» pentest от упражнений «скрипткиди»? Как донести до заказчика результаты теста, и каким образом использовать их наиболее эффективно? Тестирование на проникновение и Compliance Management – антагонисты или звенья одной цепи?

Проблемы безопасности СУБД Oracle. Последние тенденции

Александр Поляков, аудитор, Digital Security

Общие проблемы и последние тенденции безопасности СУБД Oracle. Уязвимости средств защиты (Database Vault, VPD). Безопасность дополнительных приложений (Oracle Application Server, BI, SES). Написание эксплойтов, новые техники и автоматизация процесса взлома СУБД (Metasploit).

Penetration testing using canvas framework

Rocky Witt, Immunity, Inc

Canvas is advanced attack framework which allows an operator to concentrate on the task of target penetration. CANVAS reduces workload in a number of areas, including exploit development, attack strategy and planning, execution of attacks across heterogeneous real world environments, and providing summary and logging of penetration success. We will present an overview of one of a penetration test we performed for a customer, and demonstrate the power and flexibility of CANVAS in a live environment.

Взгляд на публично доступные уязвимости и эксплойты с точки зрения взломщика

Юрий Гуркин, GLEG

В свободном доступе находится море информации об уязвимостях и использующих их эксплойтах ПО. Насколько эта информация может быть использована взломщиком для совершения атак на компьютерные системы? На первый взгляд информация, найденная нами на публично доступном ресурсе крайне интересна с точки зрения возможности использования при взломе! Однако при попытках установить и протестировать программное обеспечение на наличие уязвимости и работоспособность эксплойта в подавляющем большинстве случаев возникает ряд проблем.

11:50 – 13:40

Секция «Интернет и информационная безопасность»

Большой зал

Продолжение работы.

Безопасность Интернет-проектов: основные проблемы разработки и пути решений

Сергей Рыжиков, генеральный директор, 1С-Битрикс

Реальное положение вещей говорит о том, что даже опытные разработчики, много лет занимающиеся разработкой веб-проектов и знакомые с аспектами безопасности, допускают ошибки, которыми с легкостью могут воспользоваться «новички-хакеры». В чем корень проблемы и возможно ли принципиальное улучшение положения вещей? Как обеспечить безопасность веб-проектов при минимальных затратах и помочь веб-разработчикам сделать функционирование веб-проектов защищенным. Доклад основывается на опыте реализации тысяч интернет-проектов.

Методологии и технологии повышения качества и безопасности кода веб-приложений

Константин Кириллов, эксперт, Аист/NetCat

Широкий круг уязвимостей в современных веб-системах возникает из-за недостаточной строгости многих популярных платформ с одной стороны и низкого уровня осведомленности разработчиков об этой строгости. Решение этой проблемы заменой платформы представляется экономически нецелесообразным, вместо этого предлагается использовать набор методик и технологий, позволяющих ощутимо сократить ошибки в программном коде, приводящие к такого рода уязвимостям. В докладе предполагается рассмотреть один из примеров реализации такого механизма на базе статистики, полученной службой техподдержки компании АИСТ.

Аутентификация с помощью SAML-токенов: возможности, стандарты, продукты, алгоритмы

Павел Смирнов, к.т.н., ведущий специалист, компания «Крипто-Про»

В последнее время очень бурно развивается технология аутентификации по SAML-токенам. По мнению некоторых экспертов эта технология «является самым значительным нововведением в безопасность со времен HTTPS». В докладе будут рассмотрены возможности аутентификации с помощью SAML-токенов, стандарты ее применения, существующие на сегодняшний день продукты с поддержкой такой аутентификации. В завершение будут проанализированы перспективы использования российских криптографических алгоритмов в данной технологии.

Вирус подмены страниц: изменение поведения веб-сервисов без ведома их создателей

Александр Матросов, аналитик, Яндекс

В докладе рассматривается неконтролируемое, скрытое от создателей воздействие на веб-сервисы посредством выполнения вредоносного кода на стороне пользователя. До сих пор считалось, что выбор пользователем сервиса зависит от характеристик самого сервиса и скорости «доставки». Теперь вредоносные системы способны влиять на свойства продукта, воспринимаемого пользователем. Легкость монетизации подобных систем ведет к их широкому распространению и многообразию форм, в которых они представлены. Так как создатели сервисов не имеют средств регистрации подобных угроз, а иногда и не знают о них, вредоносные системы могут достигать огромной распространенности, прежде чем их влияние начнут учитывать.

10:30 – 11:30 Секция «Криптография: теория и практика»

Малый зал №2

Классическая секция конференции «РусКрипто». С докладами выступят признанные эксперты в области криптографии, директора Ассоциации «РусКрипто», ведущие специалисты компаний-разработчиков.

Модераторы:
Жуков Алексей Евгеньевич, к.ф.-м.н. доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто»
Попов Владимир Олегович, к.ф.-м.н., компания «Крипто-Про»

Обратимые конечные автоматы в криптографии

Жуков Алексей Евгеньевич, к.ф.-м.н. доцент МГТУ им. Баумана, директор ассоциации «РусКрипто»

В работе рассматриваются задачи, связанные с обратимостью конечных автоматов, делается обзор полученных результатов и открытых проблем.

О практическом применении White-Box криптографии

Дмитрий Щелкунов, к.т.н, компания «Актив»

В докладе будет приведен ряд механизмов, применяемых в White-Box криптографии. Показано, что алгоритм блочного шифрования AES малопригоден для создания стойких White-Box схем.

Исторический обзор «Эволюция алгоритма DES»

Сергей Панасенко, к.т.н, МСР, фирма «Анкад»

Доклад посвящен алгоритму шифрования DES, который долгое время был стандартом симметричного шифрования США, и различным вариантам данного алгоритма, предложенным криптологами с целью усиления алгоритма.

Восстановление анонимности при использовании протоколов DAA

Вадим Федюкович, GlobalLogic Ukraine

Анонимность пользователя сервиса является одной из основных целей, преследуемых в рамках инициативы Trusted Computing и механизма удаленной проверки целостности платформы пользователя. Уникальный протокол регистрации и алгоритм создания подписи, предложенные в рамках этой инициативы, должны обеспечивать анонимность пользователя, в том числе в процессе проверки созданных им подписей. В работе показана стратегия для произвольных Эмитен-

та и Проверяющего, позволяющая нарушить условие анонимности честного Пользователя, а также предложена дополнительная проверка регистрационных данных, позволяющая обнаружить попытку нарушения анонимности и отклонить такие регистрационные данные.

Теоретико-автоматные аспекты криптографии

Бабаш Александр Владимирович, д. ф.-м.н., профессор кафедры Информационной безопасности РГСУ

В докладе излагается класс методов синтеза и анализа шифрующих автоматов.

11:50 – 13:40

Секция «Криптография: теория и практика»

Малый зал №2

Продолжение работы.

Мифы и реальность квантовой криптографии

Хайров Игорь Евгеньевич, проректор по информационной безопасности, АИС

В настоящее время квантовая криптография воспринимается многими как панацея от многих бед. Однако возникает много вопросов, в частности: так ли надежна квантовая криптография, насколько общество готово принять данную технологию и каковы ее перспективы. Что такое квантовая криптография и основные принципы, на которых она построена. Современное состояние вопроса в области квантово-криптографической защиты информации в России и за рубежом. Практическое применение квантовой криптографии. Насколько надежна квантовая криптография. Возможные методы съема информации с квантово-криптографического канала.

Новые алгоритмы стеганографии и стегоанализа, базирующиеся на идеях и методах теории информации

А. Н. Фионов, д.т.н., СибГУТИ

Идеи и методы теории информации, прежде всего, универсального кодирования источников, применены к задачам стеганографии и стегоанализа. Получена простая конструкция идеальной (в теоретико-информационном смысле) стегосистемы, исследованы алгоритмы построения стегосистем с учётом статистики контейнеров, предложен новый подход к стегоанализу графических файлов.

Поточный алгоритм шифрования с использованием периодических функций

Сизов Владимир Петрович, ЗАО «Бионт»

Алгоритм шифрования отличается от остальных алгоритмов тем, что вычисления производятся с определённой точностью, на основе тригонометрических функций. Особенность алгоритма состоит в том, что при увеличении точности вычислений период гаммирования может достигнуть сколь угодно большого значения.

Параллельные алгоритмы для дискретного логарифмирования

Игорь Сидоров, ТТИ ЮФУ

В докладе рассматриваются разработанные в ТТИ ЮФУ параллельные алгоритмы, предназначенные для решения задачи дискретного логарифмирования. Приводятся краткие описания алгоритмов и оценки их эффективности.

15:00 – 16:20

Блок докладов «Как обманывают клиентов производители средств защиты»

Большой зал

Рынок информационной безопасности подчиняется тем же законам, что и многие другие сегменты. И производители средств защиты используют различные уловки для того, чтобы завлечь в свои сети доверчивых потребителей. Замалчиваемая правда, подмена понятий, использование непонятных терминов и жаргонизмов и даже откровенная ложь — все эти методы прочно обосновались в арсенале многих игроков рынка ИБ. На секции будут рассмотрены типичные и распространенные способы введения в заблуждение покупателей и вопросы, которые можно задать недобросовестным продавцам, чтобы вывести их на чистую воду.

Модератор: Алексей Лукацкий, бизнес-консультант, Cisco Systems

Почему ИБ-компании, зная правду, врут в глаза своим клиентам?

Алексей Лукацкий, бизнес-консультант, Cisco Systems

Парадоксально, но фактмногие компании, которые занимаются безопасностью, своей основной целью считают не безопасность своих клиентов. На первом месте для них деньги и только деньги, а безопасность — только инструмент зарабатывания. Для этого все цели хороши. Можно утверждать, что DLP-решения обнаруживают утечки данных. Можно утверждать, что антивирус обнаруживает все, даже неизвестные вирусы. Можно утверждать, что число атак растет по экспоненте и без средств сетевой безопасности не обойтись. Можно утверждать, что предлагаемая система защиты невзламываема. Можно утверждать, что система корреляции поддерживает все известные средства защиты. Можно ссылаться на сертификат, как свидетельство вседозволенности. А можно развенчать все эти, а также другие мифы, звучащие из уст ИБ-компаний? Попытаемся.

Торговля страхом и ложь во спасение: как и зачем ИБ обманывает бизнес

Алексей Смирнов, независимый эксперт

Что такое «торговля страхом» и что такое «ложь во спасение». Первое — примерно понятно и в особых объяснениях не нуждается: попытка заработать денег на вымышленных или преувеличенных угрозах. Что же является «позитивной» стороной обмана? Иногда приходится «пугать», потому что объяснить реальную опасность неспециалисту сложно, да и не всегда он настроен слушать. Иногда ложь необходима для развития перспективных технологий - да, проблемы данного конкретного заказчика порой решаются проще, но мы должны думать не только о его проблемах, но и о более глобальных задачах. В конце концов, каждый из нас, кто по-настоящему любит свою работу — творец, и бывает так, что совершенно не из меркантильного интереса мы строим систему «на вырост», хотя с точки зрения бизнеса достаточным, а значит и более оправданным было бы дешевое и «некрасивое» решение, даже с учетом его короткого жизненного цикла и необходимости последующего рефакторинга.

Информационная безопасность и внешние консультанты

Михаил Хромов, Начальник Аналитического отдела Управления ИБ, ЛУКОЙЛ-ИНФОРМ

Призыв не дать себя обмануть при аутсорсинге разработки внутренней нормативной базы по обеспечению информационной безопасности выглядит простой банальностью, но опасность скрыта вовсе не там, где ее принято полагать. Наибольшие риски, возникающие при принятии решения о привлечении внешних консультантов к дизайну процессов ИБ Вашей организации, связаны не с невыполнением ими своих обязательств по договору и не с получением от них неправильных советов за свои кровные. Самое худшее, что может с Вами произойти - это приобретение т.н. «best practices». К сожалению, то не обладая опытом организации этого процесса в своей собственной фирме, то стремясь сэкономить силы на разработку, но чаще всего из совершенно искреннего стремления предложить клиенту самое лучшее и передовое, именно их-то Вам скорее всего и продадут. В этом случае Вы не просто зря потратили деньги - Вы получаете на содержание монстра, которого вряд ли сможете прокормить. И очень вероятно, что поздновато это распознаете.

15:00 – 16:20

Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»

Малый зал №2

Технологии обфускации, виртуализации программного кода бурно развиваются. Что нового появилось в этих технологиях? Теория и практика. Динамический и статический анализ, новые подходы.

Модератор: Дмитрий Горелов, коммерческий директор, компания «Актив»

Анализ уязвимостей драйверов

Никита Тараканов, Александр Анисимов, Positive Technologies

Современные системы часто используют дополнительные системные драйверы для расширения функциональных возможностей. Но зачастую при разработке такого критичного компонента как драйвер ОС разработчики пренебрегают правилами проектирования и разработки с учетом требований безопасности, что приводит к возникновению уязвимостей. Уязвимости драйверов позволяют неограниченно повышать свои привилегии и получать доступ к ядру операционной системы. Типичные ошибки и уязвимости программ, использующих дополнительные драйверы, примеры реально обнаруженных уязвимостей в антивирусах, виртуальных машинах, средствах защиты уровня узла. Утилиты и методы поиска уязвимостей и подходы к защите.

Беззащитная защита. Часть 1: Технологии обхода антивирусов

Алиса Шевченко, eSage lab

В данном докладе будут рассмотрены различные техники, встраиваемые в современные вредоносные программы с целью воспрепятствовать работе антивирусной защиты либо обойти ее, их эволюция с течением времени и детали реализации. По результатам систематизации и анализа фактического материала будут сделаны выводы, применимые к задаче разработки любого типа защитного ПО: как мыслит и действует злоумышленник с целью обхода защиты, в чем причины провала защит в контексте их архитектуры и реализации, и каковы принципы разработки эффективной защиты.

Беззащитная защита. Часть 2: Уязвимости в драйверах режима ядра современных антивирусных продуктов: анализ, эксплойтинг и защита.

Дмитрий Олексюк, eSage lab

В рамках этого выступления докладчик глубоко рассмотрит тему поиска и эксплуатации уязвимостей в драйверах режима ядра для windows, а так же автоматизации их выявления. Главным образом, внимание будет акцентироваться на драйверах популярных антивирусных программ, проактивных защит и пакетов ПО класса internet security. Завершающая часть доклада будет посвящена вопросам проектирования и написания свободного от уязвимостей кода: на примере исходных текстов будут показаны типичные ошибки, допускаемые разработчиками, и рассказано о том, как их нужно избегать. Кроме этого, будет представлена методология тестирования, которая способна выявить большую часть уязвимостей, освещенных в докладе.

Обзор мирового рынка программных средств защиты от копирования

Василий Букасов, МИФИ

Дайджест всего самого нового и интересного на рынке софтверных протекторов. Тенденции, технологии, новые подходы к защите программного обеспечения. Обзор удачных решений, анализ недостатков полярных систем. Online-продажи, механизмы лицензирования, технологии, которые используют крупнейшие софтверные компании.

16:40 – 18:40

Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»

Малый зал №2

Продолжение работы.

Автоматическое обнаружение дефектов при помощи межпроцедурного статического анализа исходного кода

В.С. Несов, ИСП РАН

Статический анализ программ позволяет находить уязвимости и критические ошибки, трудно обнаруживаемые другими средствами. В докладе описывается метод масштабируемого межпроцедурного статического анализа и основанная на нем система автоматического поиска дефектов в реальных программах на языке Си. Приводятся результаты поиска таких дефектов, как переполнение буфера и разыменование нулевого указателя, в свободно распространяемых программах.

Автоматизация динамического анализа бинарного кода

В.А. Падарян, А.И. Гетьман, ИСП РАН

Рассматривается программная среда, позволяющая выполнять динамический анализ защищенного бинарного кода с целью получения описания интересующего алгоритма. Среда реализует оригинальную методику анализа и предоставляет пользователю развитый набор программных средств, объединенных в рамках единого графического интерфейса. Описываются некоторые особенности среды, такие как архитектурно независимое API, используемое для работы средств анализа, расширение пользовательского интерфейса скриптовым языком.

Восстановление типов данных в программах на основе информации, собранной во время выполнения

К.Н. Трошина, ИСП РАН

Задача восстановления типов данных — одна из наименее проработанных и трудных задач обратной инженерии. Полное и точное восстановление типов данных на основе только информации по ассемблерному листингу не всегда возможно. В представленной работе рассмотрены методы сбора и анализа информации об обращениях к памяти во время работы приложения. Рассмотрен метод восстановления высокоуровневых типов данных по ассемблерному листингу и собранному профилю обращений к памяти.

16:40 – 18:40

Научная секция «Защита информации в распределенных компьютерных системах». Часть 1

Большой зал

Тематика докладов будет посвящена следующим направлениям научных исследований и разработок: адаптивные механизмы защиты информации; идентификация, аутентификация; межсетевые экраны, виртуальные защищенные каналы; скрытые каналы; интеллектуальный анализ данных, биологические подходы для защиты информации; обманные системы и ловушки; защита от внутренних злоумышленников; защита информации на основе репутации и др.

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

Сетевые «кошки-мышки»: войны адаптивных программных агентов

Котенко Игорь Витальевич, д.т.н., СПИИРАН

В докладе, на примере защиты от компьютерных атак «распределенный отказ в обслуживании» в сети Интернет, предлагается подход к исследованию адаптивных и кооперативных механизмов функционирования команд интеллектуальных агентов. Предлагаемый подход основан на представлении сетевых систем в виде комплекса команд взаимодействующих агентов, которые могут быть в состоянии антагонистического противостояния, безразличия или кооперации. Агрегированное поведение системы выражается в локальных взаимодействиях агентов.

Адаптивная система VPN в распределенных компьютерных сетях

Игнатов Владимир Владимирович, старший вице-президент, Инфотекс

Обсуждается построение виртуальных защищенных сетей (VPN) с использованием Peer to Peer (P2P) технологий для организации прозрачного взаимодействия компьютеров, расположенных в произвольных точках распределенной компьютерной сети, с криптографической защитой трафика этих компьютеров от источника до получателя информации.

Подход к защите программ на основе механизма удаленного доверия

Десницкий Василий Алексеевич, СПИИРАН

Доклад посвящен разработке и анализу модели защиты программ на основе механизма удаленного доверия. Цель данного подхода – обнаружение несанкционированных модификаций клиентской программы, выполняющейся в потенциально враждебном окружении. Механизм ориентирован, в первую очередь, на защиту приложений, для корректного функционирования которых требуются сетевые коммуникации с удаленными клиентами или серверами.

Методы защиты от вредоносных web-сайтов на основе оценок репутации

Чечулин Андрей Алексеевич, Центр специальной системотехники

В докладе проводится анализ существующих методов оценки репутации и предлагается подход к оценке репутации Web-сайтов, формируемый на основе многофакторного анализа его характеристик, получаемых из различных источников.

10:00 – 12:00	**Секция «Свободное ПО и информационная безопасность»** *Большой зал*

Свободное программное обеспечение все шире используется как на серверах, так и на рабочих станциях в решениях, требующих обеспечения информационной безопасности. У российских и зарубежных компаний есть опыт создания и сертификации решений на базе СПО для работы с конфиденциальной информацией и с гостайной.

Модератор: Алексей Смирнов, генеральный директор, ALT Linux

Инвестиции в безопасность свободного ПО

Котов С.Л., Рожнов М.М., ГИЦ ПС ВТ

Рассматриваются технические и экономические аспекты возврата инвестиций в свободное ПО путем проведения сертификационных испытаний.

ALT Linux: Пятая платформа

Виталий Кузнецов, руководитель проектов, компания ALT Linux

Новая платформа разработки продуктов ALT Linux рассматривается как основа бизнеса по созданию безопасных решений ALT Linux и его партнёров - отечественных разработчиков свободного и проприетарного ПО.

Интегрированные защищённые решения на базе свободного ПО и ПО IBM

Васюков Алексей Викторович, консультант, VDEL

В докладе рассматривается опыт создания интегрированных типовых решений для серверов и рабочих станций, включающих полный стек программного обеспечения от операционной системы до бизнес-приложений, и сертификации данных типовых решений в соответствии с руководящими документами ФСТЭК.

Контейнеры и управление ресурсами в OpenVZ Linux ядре

Кирилл Колышкин, OpenVZ

В докладе рассматриваются Linux-контейнеры, реализованные в OpenVZ (и частично в основном ядре Linux), их функциональность, особенности, отличия от других систем виртуализации, характерные примеры использования. Особое внимание уделяется подсистеме управления ресурсами, делающей возможным мирное сосуществование множества контейнеров под одним ядром. Рассмотрены некоторые типичные для Linux DoS-атаки; показано, как подсистема управления ресурсами в OpenVZ позволяет их предотвратить.

W3AF – система для проведения аудита безопасности веб-приложений с открытым исходным кодом

Тарас Иващенко, специалист отдела аудита, Информзащита

В докладе рассматривается W3AF (Web Application Attack and Audit Framework) - пожалуй, одно из самых мощных современных средств для аудита безопасности и эксплуатации уязвимостей веб-приложений, его архитектура и особенности, отличия от конкурентов (в том числе проприетарного программного обеспечения). Наглядно демонстрируются приемы работы с W3AF, в частности, сессия поиска и эксплуатации уязвимостей.

10:00 – 11:00	**Научная секция «Защита информации в распределенных компьютерных системах». Часть 2** *Малый зал №2* Продолжение работы.

AURA: программная платформа высокоскоростного анализа сетевого трафика для задач информационной безопасности

Денис Гамаюнов, Казачкин Дмитрий, лаборатория Вычислительных комплексов, факультет ВМК МГУ им. М.В.Ломоносов;

Доклад посвящен специализированной программной платформе высокоскоростного анализа сетевого трафика для задач информационной безопасности. Обсуждается актуальность задачи, архитектура платформы на основе математического аппарата альтернирующих автоматов. Представлены результаты тестирования на нагруженных сетевых каналах.

Использование частотного анализа встречаемости инструкций для обнаружения полиморфного исполнимого кода в сетевом трафике

Эдуард Торощин, лаборатория Вычислительных комплексов, факультет ВМК МГУ им. М.В.Ломоносова

В докладе рассматривается проблема обнаружения вредоносного исполнимого кода в сетевом трафике. Описан новый метод обнаружения NOP-зон на основе анализа частоты встречаемости инструкций IA32. Представлены результаты экспериментов, демонстрирующие высокую точность и близкий к 0 уровень ложных срабатываний на типовых «нормальных» данных.

Обнаружение вредоносного программного обеспечения на базе методов интеллектуального анализа данных

Шоров Андрей Владимирович, «Аркадия»

Доклад о применении методов интеллектуального анализа данных (Data Mining) для построения средств эвристического детектирования.

11:00-12:00	**Секция «Доклады победителей конкурса докладов»** *Малый зал №2*

Секция, состоящая из докладов студентов и аспирантов, победивших в традиционном конкурсе докладов, ежегодно проводимом ассоциацией «РусКрипто».

О невозможных дифференциалах алгоритма шифрования Zodiac

Андрей Котов, МИФИ

Исследование линейных совершенных шифров и их современных аналогов

Светлана Коновалова, УрГУПС

Протокол электронной торговли без арбитра

Николай Мацук, МИФИ

День третий. 5 апреля, воскресенье

10:00 – 15:00	**Студенческий день** *Малый зал №1*
Мероприятие предоставит возможность студентам выступить с мини докладами, а также обменяться уже существующими наработками. Участники – студенты последних курсов, аспиранты и их преподаватели.	
12:30 – 13:30	**Подведение итогов, закрытие конференции** *Большой зал*

Пансионат «Липки»

В стоимость проживания входит:

- проживание в пансионате;
- 3-разовое питание «шведский стол»;
- пользование бассейном (с 08-00 до 22-00).

При отсутствии мед.справки стоимость медосмотра – 70руб.

Для участников конференции, **не проживающих** в пансионате, стоимость питания составляет:

- Завтрак – 200руб/чел.
- Обед – 250руб/чел.
- Ужин – 200руб/чел.

Оплатить питание вы можете у представителей Оргкомитета конференции.

Система оплаты

На территории пансионата действует безналичная система оплаты. При регистрации на каждого гостя оформляется карта, которая является ключом от номера. На эту карту вы можете положить деньги и в дальнейшем расплачиваться с ее помощью на территории пансионата (дополнительные услуги, бары, рестораны и т.д.).
ВНИМАНИЕ! Наличные деньги к оплате на территории пансионата не принимаются!

Дополнительные услуги

- Бильярд «Русская пирамида» - 350руб./1час;
- Бильярд «Американский пул» - 300руб./1час;
- Пользование бассейном (с 22.00 до 06.00) – 300руб./1час;
- Сауна на 6 мест с 08.00 до 24.00 – 1200руб./1час,
  с 24.00 до 08.00 – 1550руб./1час;
- Сауна на 4 места с 08.00 до 24.00 – 750руб./1час,
  с 24.00 до 08.00 – 950руб./1час;
- Русско-финская, русско-турецкая бани, инфракрасная кабина (до 10 мест) – 3150/1 час (каждое дополнительное место – 315руб./1час);
- Джакузи, комната отдыха (до 6 мест) – 1050руб./1 час (каждое дополнительное место – 105руб./1час);
- Конный прокат:
  – Верховая езда – 800руб./1 час,
  – Карета (4 человека) – 1200руб./1 час;
- Теннисный корт – 450руб./1 час;
- Спортивный зал – 450руб./1 час;

- Тренажерный зал – 100руб./1 час;
- Стол для «пинг-понга» (с ракетками) – 150/1 час;

Расчетный час

Заезд - 2апреля 2009 года в 17-00, выезд - **5 апреля в 15-00**.

Организованный выезд из пансионата

Участников конференции будет ожидать автобус **5 апреля в 15.30** на парковке рядом с выездом с территории пансионата «Липки».

Адрес пансионата «Липки»

Московская область, Одинцовский район, Аксининская сельская администрация, д. Липки.