Тайм-лайн конференции

1 апреля, четверг. День заезда

16.00	Трансферт в пансионат «Солнечная поляна»
18.00 – 19.00	Заезд и регистрация участников, проживающих в пансионате
19.00 - 21.00	Вечеринка на свежем воздухе, знакомство участников конференции

2 апреля, пятница. Первый день работы конференции

8.30 – 9.30	Завтрак в пансионате	
9.30 – 10.00	Регистрация участников конференции	
10.00- 11.10	**Круглый стол «Состояние российского рынка информационной безопасности»** *Конференц-зал (Главный корпус)* *Подробнее на стр. 3*	
11.10 - 11.30	Кофе-брейк	
11.30 – 13.30	**Секция «Использование криптографических средств в системах электронного документооборота и для защиты персональных данных»** *Конференц-зал (Главный корпус)* *Подробнее на стр. 3*	
13.30 – 14.30	Обеденный перерыв	
14.30 – 16.30	**Секция «Криптография: теория и практика». Часть 1** *Большая аудитория (Б-Ц)* *Подробнее на стр. 4*	**Секция «Расследование инцидентов. Механизмы, технологии, проблемы, опыт»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 6*
16.30 – 16.50	Кофе-брейк	
16.50 – 18.30	**Секция «Криптография: теория и практика». Часть 2** *Большая аудитория (Б-Ц)* *Подробнее на стр. 4*	**Секция «Правда и вымысел о технологиях информационной безопасности»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 7*
19.30 – 22.00	Банкет в честь открытия конференции	

3 апреля, суббота. Второй день работы конференции

9.00 – 10.00	Завтрак в пансионате		
9.30 – 10.00	Регистрация участников конференции		
10.00 – 12.00	**Секция «Интернет и информационная безопасность»** *Большая аудитория (Б-Ц)* *Подробнее на стр. 9*	**Секция «Побочные каналы – атаки и противодействие»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 10*	**Соревнования РусКрипто CTF** *Подробнее на стр. 16*
12.00 – 12.20	Кофе-брейк		
12.20 – 13.30	**Круглый стол «Технологии безопасности электронных торговых площадок»** *Большая аудитория (Б-Ц)* *Подробнее на стр. 11*	**Круглый стол «Технологии защиты от вредоносных программ»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 11*	
13.30 – 14.30	Обеденный перерыв		
14.30 – 16.30	**Секция «Защита информации в распределенных компьютерных системах»** *Большая аудитория (Б-Ц)* *Подробнее на стр. 12*	**Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 13*	**Соревнования РусКрипто CTF** *Подробнее на стр. 16*
16.30 – 16.50	Кофе-брейк		
16.50 – 18.30	**Секция «Общие вопросы информационной безопасности»** *Большая аудитория (Б-Ц)* *Подробнее на стр. 14*	**Секция «Penetration testing internals»** *Малая аудитория (Б-Ц)* *Подробнее на стр. 15*	
18.30 - 19.30	Ужин в пансионате		
19.30 – 22.00	**Вечерняя rump-session. Награждение победителей конкурса докладов**		

4 апреля, воскресенье. День отъезда

9.00 -11.00	Завтрак в пансионате
12.00	Трансферт из пансионата в Москву

Первый день работы конференции

10:00 – 11:10	**Круглый стол «Состояние российского рынка информационной безопасности»** *Конференц-зал (Главный корпус)*

Модератор: *Александр Власов, издатель журнала Information Security.*

Участники: *Кузьмин Алексей Сергеевич, ФСБ РФ; Попов Владимир Олегович, компания «Крипто-Про»; Горелов Дмитрий Львович, компания «Актив»; Сычев Артем Михайлович, Россельхозбанк; Емельянов Геннадий Васильевич, Ассоциация Защиты Информации; Соколов Александр Васильевич, Ассоциация АП КИТ.*

Известные эксперты отрасли обсудят российский рынок информационной безопасности. Что изменилось за кризисный 2009 год? Какие прогнозы сбылись? Что ждать и чего опасаться в 2010 году?

11:30 – 13:00	**Секция «Использование криптографических средств в системах электронного документооборота и для защиты персональных данных».** *Конференц-зал (Главный корпус)*

Модератор: *Юрий Маслов, коммерческий директор, Крипто-Про.*

Технические, организационные и юридические аспекты использования криптографических средств в госорганах и коммерческих организациях. Требования регуляторов и практика использования. В секции примут участие сотрудники ФСБ РФ, представители крупнейших российских компаний, разрабатывающих и внедряющих СКЗИ.

Использование СКЗИ в системах электронного документооборота и для защиты персональных данных.
Юрий Маслов*, коммерческий директор, ООО «Крипто-Про».*
Практика применения систем криптографической защиты информации. Технические и юридические аспекты. Нюансы использования технологий и соблюдение требований российского законодательства.

EDSIGN и ЭЦП – бумажные документы без бумаги.
Василий Овчинников*, эксперт, Электронные Офисные Системы.*
В докладе рассматривается проблема популяризации механизмов криптографической защиты информации применительно к механизму электронной цифровой подписи.

Некоторые аспекты использования криптографических средств при предоставлении государственных электронных услуг.
Дмитрий Гусев*, зам. генерального директора, ИнфоТеКС.*
В докладе представлен взгляд российской компании, разрабатывающей средства криптографической защиты информации, на то, как должен развиваться рынок СКЗИ для массовых государственных проектов. Что мешает и что может дать толчок более быстрому развитию этого сегмента рынка информационной безопасности.

Технологии ЭЦП и шифрования для средних и мелких проектов. Как сделать сложное простым?

***Дмитрий Горелов**, коммерческий директор, компания Актив.*

Существует масса причин, из-за которых технологии ЭЦП внедряются медленно или не внедряются совсем. Зачастую это объясняется отсутствием квалифицированных специалистов. И если крупные компании способны решить эту проблему, то как быть со средним или мелким бизнесом? Как развертывать эти технологии в территориально распределенных компаниях?

Что изменилось после выхода приказа ФСТЭК №58?

***Михаил Линьков**, главный инженер, Центр Безопасности Информации.*

В докладе освещаются основные изменения в проводимых мероприятиях по защите персональных данных, связанные с утверждением Положения о методах и способах защиты информации в информационных системах, обрабатывающих персональные данные (Приказ ФСТЭК России №58 от 5 февраля 2010 года).

Использование ЭЦП в электронном документообороте: текущее состояние и ближайшие перспективы.

***Григорий Поваров,** заместитель генерального директора, СКБ Контур*

К настоящему моменту использование ЭЦП во взаимоотношениях государства и бизнеса достигло впечатляющих результатом. Отдельные изменения нормативной базы могут способствовать выходу электронного юридически значимого документооборота на новый уровень. Однако для этого необходимо устранить ряд сдерживающих ограничений.

14:30 – 18:30 Секция «Криптография: теория и практика»

Большая аудитория (Бизнес-центр)

***Модераторы:** Жуков Алексей Евгеньевич, к.ф.-м.н. доцент МГТУ им. Баумана, директор Ассоциации «РусКрипто»; Кузьмин Алексей Сергеевич, ФСБ РФ; Попов Владимир Олегович, к.ф.-м.н., Крипто-Про, директор Ассоциации «РусКрипто».*

Классическая секция конференции «РусКрипто». Текущие и разрабатываемые российские криптографические стандарты. Нюансы реализации и технологии использования. Реальные и мнимые уязвимости. Работа Технического Комитета № 26. Теоретическое обоснование стойкости криптографических алгоритмов. Криптографические протоколы. Использование российских стандартов в международных криптографических протоколах.

Последние инициативы NIST в области криптографии.

***Жуков Алексей Евгеньевич**, к.ф.-м.н., доцент МГТУ им. Н.Э. Баумана.*

Обзорный доклад о новом в международной криптографии.

Перспективы появления и применения квантовых компьютеров в криптографии.

***Кузьмин Алексей Сергеевич**, ФСБ РФ.*

Мифы и реалии квантовой криптографии.

***Хайров Игорь Евгеньевич**, к.т.н., проректор, Академия Информационных Систем.*

Как таковой квантовой криптографии не существует. Существует множество алгоритмов квантового распределения ключевой информации, а в качестве криптографических преобразований используются классические симметричные алгоритмы. Задается много вопросов, связанных с перспективностью и надежностью квантово-криптографических технологий. Как

известно, в соответствии с фундаментальными законами квантовой физики невозможно клонировать неизвестное квантовое состояние микрочастицы без внесения в него изменений. Однако те же самые законы не запрещают копировать квантовую частицу. Соответственно, возникает вопрос, являются ли квантовокриптографические технологии панацеей в области криптографической защиты информации?

Алгоритм пороговой электронной цифровой прокси подписи без раскрытия секретного ключа.

***Евгений Толюпа**, ЯрГУ им. П.Г. Демидова.*

В работе предложен алгоритм электронной цифровой прокси подписи, позволяющей оригинальному подписчику делегировать группе участников возможность подписывать сообщения от его имени. Оригинальному подписчику не требуется передавать группе значение секретного ключа. При подписании сообщения группа не восстанавливает информацию, полученную от оригинального подписчика.

Однородные двумерные булевы клеточные автоматы и их свойства применительно к генерации псевдослучайных последовательностей.

***Борис Сухинин**, МГТУ им. Н.Э. Баумана.*

Псевдослучайные последовательности (ПСП) широко используются в различных областях науки и техники – от теории игр и моделирования физических процессов методом Монте-Карло до криптографии. В работе исследуется ряд свойств однородных двумерных булевых клеточных автоматов, а также предлагается новый метод генерации псевдослучайных последовательностей, основанный на использовании этих автоматов. Выходные последовательности таких генераторов имеют хорошие статистические свойства, а аппаратная реализация предложенных алгоритмов на типовых ПЛИС обладает очень высоким быстродействием – до 25 Гбит/с на частоте 100 МГц.

Основные направления деятельности Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации».

***Анатолий Лунин**, эксперт ГОСТ Р, заместитель ответственного секретаря ТК26.*

В обзорном докладе будут освещены основные проекты, выполняемые в рамках ТК26, в направлении национальной, региональной и международной стандартизации. Среди них - текущие и разрабатываемые российские стандарты, а также стандарты СНГ, признание российских криптографических алгоритмов в качестве международных стандартов.

Перспективный алгоритм хеширования.

***Матюхин Дмитрий Викторович**, ФСБ РФ; **Владимир Рудской**, МГУ им. М.В. Ломоносова.*

В докладе будут изложены принципы построения, общая схема и эксплуатационные характеристики новой функции хеширования, которая может быть использована в качестве основы для обновления национального стандарта ГОСТ Р 34.11-94.

Об использовании криптографических алгоритмов ГОСТ в протоколе DNSSec.

***Василий Долматов**, КриптоКом.*

В докладе рассказывается о процессе добавления в интернет-стандарт на протокол DNSSec поддержки российских криптоалгоритмов.

Вопросы реализации протоколов криптографической защиты информации. Российские ГОСТ-ы и IPSEC, TLS, EFS, ФКН.

***Попов Владимир Олегович**, к.ф.-м.н., Крипто-Про, директор Ассоциации «РусКрипто».*

Существующие требования ФСБ России накладывают дополнительные условия на реализацию защищенных криптографических протоколов. В докладе будут рассмотрены вопросы как правильно встраивать российскую криптографию в перечисленные и в перспективные протоколы.

О нулевой практической значимости «Атаки определения ключа полнораундового блочного шифра ГОСТ с нулевой трудоемкостью и памятью».

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

В докладе показывается, что вариант метода бумеранга с использованием связанных ключей, рассмотренный в работе E. Fleishmann et al., указанной в названии доклада, эквивалентен полному перебору ключей алгоритма шифрования ГОСТ 28147-89. Далее предлагаются модифицированные варианты метода. В заключение демонстрируется, что практические приложения рассматриваемого метода крайне ограничены, и он не является принципиальным препятствием для использования алгоритма ГОСТ 28147-89.

О криптографической стойкости функции хеширования ГОСТ Р 34.11-94.

***Матюхин Дмитрий Викторович**, ФСБ РФ.*

В докладе будут рассмотрены некоторые характеристики предложенного F.Mendel и соавторами на конференции CRYPTO 2008 метода построения коллизии хеш- функции ГОСТ Р 34.11-94, не указанные авторами метода. Речь пойдет об объеме памяти метода, способах его модификации в условиях ограниченной памяти и минимальном объеме памяти, при котором трудоемкость метода меньше универсальной "корневой" оценки, справедливой для любой хеш-функции.

Атаки на основе метода связанных ключей.

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

В последние годы все больше строится атак на блочные и поточные алгоритмы шифрования на основе метода связанных ключей. Примером этого служат предложенные атаки на основе методов связанных ключей и бумеранга на алгоритмы AES и ГОСТ 28147-89. В обзорном докладе рассматриваются некоторые алгоритмы блочного шифрования, уязвимые относительно атак на основе метода связанных ключей. Описываются некоторые слабые алгоритмы развертывания ключа.

14:00 – 16:00 Секция «Расследование инцидентов. Механизмы, технологии, проблемы, опыт»

Малая аудитория (Бизнес-центр)

***Модератор:** Илья Сачков, генеральный директор, Group-IB.*

Многие продукты в области ИБ могут быть использованы для сбора и анализа информации об инцидентах. Как и при помощи каких технологий расследуются инциденты нарушения информационной безопасности. Forensic-клиенты для корпоративных служб безопасности и правоохранительных органов. Также будут рассмотрены правовые аспекты расследования инцидентов. В секции примут участие представители соответствующих подразделений правоохранительных органов и специалисты служб безопасности, специализирующиеся на расследовании инцидентов.

Извлечение информационных улик из мобильных телефонов, смартфонов и КПК.

***Николай Голубев**, Oxygen Software.*

Современный мобильный телефон хранит массу информации - от списка контактов до истории перемещений своего владельца. Во всем мире этим данным находят все большее применение – от доказательства в суде до контроля компании над использованием служебных телефонов сотрудниками.

Расследование распределенных атак на отказ в обслуживании(DDoS): новые подходы.

***Илья Сачков**, CISM, генеральный директор, Group-IB.*

DDoS атаки – один из самых популярных и опасных видов компьютерных преступлений. Малое количество успешно раскрытых уголовных дел и ощущение безнаказанности делает данный вид атак наиболее прибыльным. В докладе будут показаны новые методы по расследованию данного вида атак, а также освещены правовые вопросы.

Алгоритмические и инженерные аспекты анализа защищенных данных.

***Алексей Чиликов**, к. ф.-м. н., руководитель отдела исследований, компания Passware.*

Защищенные и зашифрованные данные нередко становятся серьезным препятствием при расследовании инцидентов информационной безопасности. В докладе представлена информация о математических и инженерных задачах, возникающих при восстановлении защищенных данных и современных подходах к решению таких задач.

Исследование вредоносных программ с точки зрения расследования инцидентов.

***Александр Матросов**, Руководитель Центра вирусных исследований и аналитики, ESET.*

В докладе будут рассмотрены вопросы, связанные с исследованием вредоносных программ и проведением экспертизы вредоносного кода. Эта тема становится все более актуальной, при этом практически не освещена в открытых источниках. Как проводится экспертиза вредоносного кода? Какую информацию можно извлечь в процессе исследования? Как она может повлиять на процесс расследования конкретного инцидента?

16:20 – 18:00

Секция «Правда и вымысел о технологиях информационной безопасности»

Малая аудитория (Бизнес-центр)

***Модератор:** Алексей Лукацкий, бизнес-консультант, Cisco Systems.*

На секции представлены дискуссионные доклады. Информационная безопасность – актуальная потребность или давление регулирующих органов? Реальные и мнимые угрозы уязвимости. Что могут и где бессильны технологии информационной безопасности? Чем и как пугают потенциальных и реальных клиентов системные интеграторы в области безопасности?

Мифы виртуализации.

***Мария Сидорова**, главный редактор, VMwareSecurityGroup.ru.*

Заблуждения и стереотипы относительно обеспечения информационной безопасности инфраструктур виртуализации. Правда ли, что решения виртуализации сами по себе позволяют повысить уровень обеспечения информационной безопасности?

Чем закончится DLP hype?

***Владимир Иванов**, Заместитель директора департамента эксплуатации, Яндекс.*

Принято считать, что отношение пользователей к новым продуктам определяется Hype Cycle, предложенным компанией Gartner в 1995 году. В существующем виде технологии, нацеленные на обеспечение защиты от утечек данных, появились несколько лет назад. Казалось бы, этого достаточно для того, чтобы и период надутых ожиданий, и период первых разочарований закончился, а технология могла бы выйти на плато продуктивности. Так ли это? Смогла ли DLP стать the next big thing?

Заказной тест на проникновение – механизм обеспечения ИБ?

***Василий Томилин**, ведущий специалист, Cisco Systems.*

Пентесты стали достаточно популярны. Можно ли рассматривать пентест как механизм обеспечения ИБ? Результаты такого однократного тестирования на проникновение, безусловно, могут послужить базой для продажи услуг ИБ, для получения нового заказчика или в качестве элемента конкурентной борьбы. В то же время, сам по себе факт проникновения едва ли позволит повысить уровень защищенности ИТ-инфраструктуры организации.

Заблуждения банковской безопасности.

***Алексей Лукацкий**, бизнес-консультант по безопасности, Cisco Systems.*

Банки считаются достаточно продвинутыми в области защиты банковской тайны и финансовых средств, доверенных им клиентами. Но так ли это на самом деле? Не вводят ли они в заблуждение своих клиентов, формируя в них чувство ложной защищенности? Настолько ли надежны виртуальные клавиатуры, одноразовые коды для осуществления транзакций, SMS-аутентификация, USB-токены с неизвлекаемыми криптоключами, как об этом говорится на сайтах банков?

Второй день работы конференции

10:00 – 12:00	**Секция «Интернет и информационная безопасность»** *Большая аудитория (Бизнес-центр)*

Модератор: *Сергей Гордейчик, технический директор, Positive Technologies*.
Секция посвящена актуальным аспектам информационной безопасности, связанных с использованием Интернет и сетевых технологий. Сетевые атаки на рабочие станции и серверы приложений, современные механизмы защиты Интернет-систем, защита корпоративных и Интернет-систем, использующих Web-технологии.

Web Application Security Consortium. Перспективы развития.

Сергей Гордейчик*, технический директор Positive Technologies, член совета директоров Web Application Security Consortium.*
Web Application Security Consortium (WASC) - международная организация, объединяющая профессионалов в области безопасности веб-приложений, деятельность которой направлена на консолидацию и распространение передового опыта в области безопасности прикладных систем, использующих Web-технологии. В рамках доклада будет приведен обзор текущих и перспективных проектов WASC, анализ примеров использования разработанных документов и таксономий в реальных проектах.

Обнаружение уязвимостей в механизме авторизации веб-приложений.

Андрей Петухов*, Лаборатория Вычислительных Комплексов, факультет ВМиК МГУ.*
В настоящее время существует широкий класс уязвимостей, для которого не найдено удовлетворительных автоматизированных методов обнаружения — это уязвимости авторизации. В рамках доклада рассматриваются подходы к автоматизации обнаружения уязвимостей веб-приложений, связанных с авторизацией методом «черного ящика».

События безопасности, сопровождающие покушения на хищения финансовых средств клиентов в системах дистанционного банковского обслуживания.

Артем Сычев*, начальник управления информационной безопасности, Россельхозбанк.*
В рамках доклада рассматриваются прямые и косвенные признаки проведения атак, направленных на хищения финансовых средств клиентов в системах дистанционного банковского обслуживания.

Анализ эффективности средств защиты на примере систем обнаружения атак.

Владимир Лепихин*, заведующий лабораторией сетевой безопасности, Информзащита.*
Вопрос оценки реальной эффективности средств защиты в настоящее время актуален как никогда. Усложнение систем в купе с усилением маркетинговой активности практически не оставляет шансов понять, что и насколько эффективно делает тот или иной продукт. В докладе приведены результаты сравнения систем обнаружения атак на основе оригинальной методики, позволяющей оценить эффективность выполнения целевой функции продуктами данного класса.

Особенности обеспечения информационной безопасности в системах SCADA.

***Андрей Комаров**, технический директор, компания ITDefence.*

Доклад посвящен анализу существующих технологий и практик для контроля безопасности критически важных инфраструктур, использующих технологии SCADA. Рассматриваются существующие технологические подходы, разработки ФСТЭК РФ и Совета Безопасности, а также практики выявления подобных систем с помощью традиционных каналов связи, особенностей получения несанкционированного доступа и методики предотвращения вторжений, специфичных для этой сферы.

Тестирование уязвимостей приложений в рамках сертификации по PA-DSS.

***Марат Вышегородцев**, специалист, Информзащита.*

Безопасность прикладных систем является сложной и актуальной задачей. Одним из методов повышения защищенности является использование требований стандарта PA-DSS как составной части PCI DSS. В докладе рассматриваются основные требования стандарта, подходы к проведению работ. Обсуждаются основные виды уязвимостей, методики тестирования и примеры из практики анализа защищенности платежных приложений.

10:00 – 12:00 Секция «Побочные каналы – атаки и противодействие»

Малая аудитория (Бизнес-центр)

***Модератор:** Алексей Чиликов, к.ф.-м.н., руководитель отдела исследований, Passware.*

Атаки на аппаратные реализации криптоалгоритмов при помощи побочных каналов – одно из наиболее активно развивающихся направлений современной криптографии. В рамках секции будет представлен обзор последних достижений мировой науки в этой области, а также новые научные результаты. Специалисты-практики поделятся своим опытом проектирования и разработки защищенных систем.

Исторический обзор технологий атак по побочным каналам.

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

Вводный доклад в тематику секции. Термины, история. Достижения прошлого. Научные и практические вопросы.

Новая атака методом анализа сбоев на реализации криптоалгоритмов для эллиптических кривых.

***Олег Тараскин**, преподаватель, МИФИ.*

Представлена новая схема атаки методом анализа сбоев (fault attack) на некоторые реализации криптоалгоритмов для эллиптических кривых. Рассматривается вопрос о применимости данной атаки к различным реализациям алгоритмов и возможных мерах противодействия.

Защита ключевой информации от утечки по каналу ПЭМИН.

***Александр Шарамок**, к.т.н., начальник отдела, Фирма «АНКАД».*

Рассмотрен вопрос защиты ключевой информации от утечки по каналу ПЭМИН. Для решения

этого вопроса в преобразованиях, использующих сложение по модулю 2**n, предложен способ сложения двух чисел, представленных в позиционной системе счисления, одно из которых маскировано путем поразрядного сложения с маской по модулю основания системы счисления. При сложении снятие маски осуществляется без получения разрядов маскированного операнда в «чистом» виде.

Fault-атаки на алгоритм HMAC.

***Алексей Чиликов**, к. ф-м. н., руководитель отдела исследований, Passware .*

Предложена атака на основе анализа сбоев (fault-атака) на алгоритм HMAC. Рассмотренная атака применима к вариантам HMAC, основанным на широко распространенных алгоритмах хеширования (SHA-1/SHA-0/MD5/MD4) и приводит к успешному раскрытию ключевой информации. Проведен анализ сложности указанной атаки, подтвержденный результатами компьютерного моделирования. Обсуждается вопрос о возможностях ее практического применения против устройств, аппаратно реализующих указанные алгоритмы.

12:20 – 13:30 Круглый стол «Технологии безопасности электронных торговых площадок»

Большая аудитория (Бизнес-центр)

***Модератор:** Илия Димитров, исполнительный директор, Ассоциация электронных торговых площадок.*

Электронные закупки стали неотъемлемой частью современного бизнес-пространства. В этом году все государственные закупки перейдут в электронную форму. Участники круглого стола обсудят технологии обеспечения безопасности и нюансы использования криптографии при работе торговых площадок. В работе примут участие представители крупнейших электронных торговых площадок и удостоверяющих центров.

12:20 – 13:30 Круглый стол «Технологии защиты от вредоносных программ»

Малая аудитория (Бизнес-центр)

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

Современная модель угроз. От чего должен защищать антивирус? Что будет происходить с угрозами в ближайшем будущем? Технологии защиты как ответ на существующие угрозы, эволюция технологий (проактивность, «облачные» репутационные технологии, sendbox, интеграция). Влияние глобальных трендов на ИТ-рынке (виртуализация, XaaS). Участвуют эксперты компаний TrendMicro, Лаборатория Касперского, ВирусБлокАда, S.N.Safe&Software, McAfee.

14:30 – 16:30	**Секция «Защита информации в распределенных компьютерных системах»** *Большая аудитория (Бизнес-центр)*

Модератор: *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 адаптивные механизмы защиты информации, моделирование атак и механизмов защиты, идентификация и аутентификация, интеллектуальный анализ данных и биологические подходы для защиты информации, обнаружение атак и вредоносного программного обеспечения, обманные системы и ловушки, защита от внутренних злоумышленников, защита информации на основе репутации и классификации объектов в Интернет и др.

Раннее обнаружение эпидемий сетевых червей в высокоскоростных каналах передачи данных.

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

Предложен метод раннего обнаружения эпидемий сетевых червей на основе анализа частоты встречаемости участков вредоносного исполняемого кода в сетевом трафике. Идея метода заключается в выявлении таких участков исполняемого кода архитектуры x86, частота встречаемости которых в наблюдаемом канале изменяется в соответствии с простой эпидемиологической моделью. Предложенный метод обладает линейной вычислительной сложностью, а экспериментальные исследования на программном прототипе демонстрируют пропускную способность порядка 1Гбит/с на типовом оборудовании.

Комбинирование методов Data Mining для статического детектирования Malware.

Дмитрий Комашинский*, Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Одним из возможных вариантов оптимизации показателей предиктивной функции эвристических средств детектирования Malware, основанных на методах Data Mining, является применение комбинирования отдельных решающих экспертов (классификаторов). В настоящей работе этот вопрос рассматривается в контексте объединения отдельных существующих и доказавших свою потенциально высокую эффективность методов статического детектирования Malware.

Гранулярный контроль безопасности поведения приложений со стороны ядра Linux.

Федор Сахаров*, Лаборатория вычислительных комплексов, факультет ВМК МГУ имени М.В.Ломоносова.*

Рассматривается задача автоматического контроля безопасного выполнения приложений под управлением операционной системы Linux с целью раннего обнаружения атак, изменяющих поток выполнения программы или поток данных. В качестве решения данной задачи предлагается комбинированный подход с использованием Security Enhanced Linux (SELinux) и механизма отслеживания контрольных точек в исполняемом коде приложений.

Защита от сетевых атак на основе комбинированных механизмов анализа трафика.

***Андрей Чечулин**, Центр специальной системотехники.*

Актуальной задачей в области обеспечения безопасности информационных ресурсов является защита от сетевых атак. Для решения данной проблемы предлагается использовать подход к защите от сетевых атак, основанный на использовании семейства отдельных (атомарных) методов (алгоритмов) анализа трафика и многоуровневого комбинирования алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, а также мета-классификатора, осуществляющего принятие решения о вредоносности трафика по данным от каждого алгоритма.

Блокирование Web-сайтов с неприемлемым содержанием на основании выявления их категорий.

***Юлия Зозуля**, Лаборатория проблем компьютерной безопасности, СПИИРАН.*

Представляемая работа посвящена разработке общего подхода и реализующего его начального прототипа, предназначенных для решения актуальной в настоящее время (например, для систем родительского контроля) задачи категорирования веб-сайтов для систем блокирования веб-страниц с неприемлемым содержимым. Согласно предлагаемому подходу пользователь (например, родитель) может определить список категорий, по которым будет оцениваться каждый посещаемый веб-сайт. В соответствии с выбранными категориями странице ставится оценка с учетом информации из разных источников. Оценка сайта заносится в базу данных, а затем используется и обновляется при последующем доступе к этому или другим сайтам.

Агентно-ориентированное моделирование бот-сетей.

***Алексей Коновалов**, Аркадия.*

В работе рассматривается предложенный общий подход и реализуемая программная среда, предназначенные для моделирования бот-сетей и механизмов защиты от их воздействия. Моделируются жизненный цикл бот-сети, а также антагонистический по отношению к нему процесс сдерживания его развития на основе применения механизмов защиты от воздействия бот-сети. Исследуются сценарии формирования бот-сети, сценарии различных инфраструктурных атак, выполняемых с помощью бот-сетей (в том числе реализации DDoS-атаки), а также сценарии защиты от них. Модели бот-сети и механизмов защиты от воздействия бот-сети задаются в виде модели противоборства команд интеллектуальных агентов атаки и защиты.

14:30 – 16:30 Секция «Реверсинг. Анализ исполняемого кода и технологии защиты»

Малая аудитория (Бизнес-центр)

***Модератор:** Дмитрий Щелкунов, к.т.н., КФ МГТУ им. Н.Э. Баумана.*

Секция посвящена вопросам ИБ, связанным с выполнением программного кода на недоверенных платформах: технологиям защиты и взлома программного обеспечения, технологиям обфускации и деобфускации, вопросам DRM и тем задачам, которые нельзя решить, используя только криптографические методы.

White-Box криптография, обфускация и защита ПО. Основные направления развития.

***Дмитрий Щелкунов**, к.т.н., КФ МГТУ им. Н.Э. Баумана.*

Рассматривается текущее состояние проблем White-Box криптографии и обфускации, а также роль этих технологий в защите ПО. Описывается оригинальный подход, позволяющий повысить стойкость White-Box реализаций. Показано, что для создания стойких White-Box схем необходима автоматическая генерация соответствующего блочного шифра. Рассмотрена возможность применения механизмов White-Box криптографии для обфускации программ. Кратко описываются возможности инструмента Guardant 3a-code.

Методика восстановления формата данных.

***Александр Гетьман**, стажер-исследователь, Вартан Падарян, старший научный сотрудник, ИСП РАН.*

В докладе рассматривается методика автоматизированного восстановления формата данных, базирующаяся на динамическом анализе бинарного кода. Описанный подход позволяет восстановить иерархическую структуру изучаемых данных и выявлять определенную семантику полей. Важной особенностью подхода является его применимость к анализу защищенных приложений.

Моделирование семантики машинных инструкций.

***Вартан Падарян**, старший научный сотрудник, Соловьев М.А. , ИСП РАН.*

Рассматривается система моделирования операционной семантики машинных инструкций. Основной областью применения системы является динамический анализ бинарного кода с целью восстановления алгоритмов. Система включает в себя алгоритмы построения моделей отдельных машинных инструкций на основе спецификаций целевых машин и поддерживает интерпретацию операционной семантики, выраженной в этих моделях.

Враг внутри PDF.

***Сергей Рублев**, эксперт по информационной безопасности.*

В последние годы PDF-документы стали неотъемлемой частью нашей повседневной работы в сети Интернет, однако простой клик по файлу .pdf может привести к очень серьезным последствиям. В докладе рассматривается как общие вопросы структуры и разметки PDF-документов, так и вопросы, связанные с безопасностью PDF: возможности активного содержания документа, внедрение вредоносного кода. Также уделяется внимание средствам противодействия вредоносному содержимому PDF-файлов.

16:50 – 18:30 Секция «Общие вопросы информационной безопасности».

Большая аудитория (Бизнес-центр)

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

Технические и методические доклады, посвященные технологиям информационной безопасности. Опыт реальных проектов и перспективные разработки.

Электронная почта – схемы надежной защиты сервера и трафика.

Карен Абрамянц, MCNPS, MCSA, преподаватель, Академия Информационных Систем.

В современных организациях при обмене информацией огромную роль играет система элек-

тронной почты. Следует понимать, что посредством электронной почты могут рассылаться вредоносные файлы, фишинг-ссылки и просто спам-сообщения. Такие виды корреспонденции несут угрозу безопасности как корпоративной информационной системы в целом, так и данных отдельных сотрудников в частности, а просмотр спам-сообщений может способствовать неэффективной трате рабочего времени сотрудников. При этом сам почтовый сервер организации может быть подвержен атакам со стороны внешних сетей. В докладе рассмотрены эффективные методы защиты почтового сервера и фильтрации корреспонденции, предлагаемые различными вендорами на сегодняшний день.

Практика выбора IPC для защиты от внутренних угроз.

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

Защита корпоративной информации от внутренних угроз в последние годы переросла из модного тренда для избранных компаний во вполне самостоятельное направление информационной безопасности. Топ-менеджеры постепенно начинают пересматривать свое отношение к финансированию и рассматривать защиту данных от внутренних угроз не только как источник расходов, но и как конкурентное преимущество компании.

Современные руткит/антируткит технологии.

***Дмитрий Варшавский**, ведущий программист, ВирусБлокАда.*

Вредоносные программы типа «rootkit». Программы поиска аномалий типа «antirootkit». Почему данные технологии сегодня актуальны? Варианты присутствия вредоносного кода. Сокрытие и модификация системных объектов. Внедрение в файловую систему, модификация загрузочной области. Стек драйверов ОС: фильтрация и скрытые обработчики. Примеры и методы обнаружения аномалий.

Особенности реализации прозрачного шифрования файлов в КриптоПро EFS.

***Павел Смирнов**, Крипто-Про.*

Рассматривается архитектура средства защиты конфиденциальной информации КриптоПро EFS, сходства и отличия реализации шифрования файлов на диске в шифрующей файловой системе Microsoft EFS и КриптоПро EFS, дополнительные возможности КриптоПро EFS, пути дальнейшего развития продукта.

Построение систем защищенного взаимодействия.

***Алексей Голдбергс**, Сергей Симаков, Microsoft.*

В докладе рассматриваются задачи и решения вопросов организации защиты обмена информацией в крупных территориально-распределенных организациях с использованием средств строгой аутентификации, федеративных отношений и минимального раскрытия персональной информации.

16:50 – 18:30 Секция «Penetration testing internals»

Малая аудитория (Бизнес-центр)

***Модератор:** Сергей Размахнин, руководитель группы департамента информационной безопасности, МТС.*

Секция посвящена технологиям сетевых атак, тестирования на проникновение и другим «экстремальным» методикам оценки защищенности информационных систем.

Тестирование на проникновение, что за??!

***Дмитрий Евтеев**, эксперт по безопасности, Positive Technologies.*

Тестирование на проникновение (тесты на преодоление защиты, penetration testing) является популярной во всем мире услугой в области информационной безопасности. Практический опыт предоставления данной услуги показывает, что вокруг тестов на проникновение сложилось большое количество мифов и неоднозначных трактовок. В рамках доклада рассматриваются основные вопросы, связанные с проведением тестов на проникновение с организационной, методической и технической точки зрения. Приводятся примеры реальных работ и их использования в рамках стратегии развития ИБ компаний.

Обзор уязвимостей баз данных на примере Oracle, IBM DB2.

***Юрий Гуркин**, генеральный директор, GLEG.*

Характерные типы уязвимостей баз данных: уязвимости в сетевых сервисах, позволяющие получить контроль над системой или базой данных, или вызвать отказ в обслуживании, уязвимости в процедурах PL/SQL, позволяющие получить привилегии SYS. Рассматриваются методы эксплуатации данных типов уязвимостей, в частности SQL Injections с использованием Java. Обзор состояния защищенности последних версий баз данных с примерами новых уязвимостей (0-day) в IBM DB2, Oracle.

Атаки на клиентов. Технология JIT-SPRAY. Написание универсального шеллкода.

***Алексей Синцов**, аудитор ИБ, Digital Security.*

С учетом последних техник защиты, таких как DEP, ASLR и защита от HeapSpray в браузере IE 8, атаки на клиентов с использованием популярных уязвимостей стали затруднены, а в некоторых случаях невозможны. Существует новый метод Jit Spray, предложенный на BlackHat DC 2010, который позволяет обойти защиту ASLR и DEP при атаке на браузер клиента. Однако публичного рабочего эксплоита до сих пор предложено не было. В докладе особое внимание уделено особенностям разработки универсального шеллкода для реализации данного метода.

10.00 – 18:30

Соревнования РусКрипто CTF 2010

Первая аудитория (Бизнес-центр)

В этом году впервые в рамках ежегодной конференции РусКрипто состоится соревнование по правилам CTF (Capture the Flag). В соревновании примут участие студенческие команды из различных ВУЗ'ов, которые будут пробовать свои силы в анализе уязвимостей сетей.

В числе основных задач, поставленных перед участниками, будут обнаружение и устранение уязвимостей в предложенных сетях, а также использование идентичных уязвимостей в сетях противников для захвата секретной информации. При этом организаторы соревнования в реальном времени будут вносить изменения, добавляя новые уязвимости.

Участники РусКрипто CTF 2010: ХакерДом (УГУ им. А.М.Горького, Екатеринбург), CIT (ИТМО, Санкт-Петербург), SiBears (Томский государственный университет, Томск), Bushwhackers (МГУ, Москва), [Censored] (РГУ им И. Канта, Калининград), Huge Ego Team (МИФИ, Москва).

Пансионат «Солнечная поляна»

В стоимость проживания входит:
- проживание в пансионате;
- первая медицинская помощь;
- парковка на охраняемой территории.

В стоимость организационного взноса участника входит:
- участие в конференции с 1 по 4 апреля;
- материалы конференции;
- питание по программе;
- банкет;
- трансферт в день заезда/выезда.

Общие правила для участников:
- ✓ Пропуск на все мероприятия конференции осуществляется только по предъявлению бэйджа участника конференции,
- ✓ Питание согласно программе конференции - при предъявлении соответствующей карточки на питание.

Бэйджи и карточки на питание выдаются на регистрации участников при заселении в пансионат 1 апреля или в день открытия конференции 2 апреля в 9.30 в холле главного корпуса пансионата «Солнечная поляна». При отсутствии бэйджа участника или карточки на питание претензии не принимаются.

Питание (завтраки, обеды, ужин) будут проходить в ресторане Главного корпуса пансионата согласно программе конференции.

Дополнительные услуги пансионата (по предварительному заказу через Администрацию пансионата)
- Бассейн (расположен в Гостевом корпусе);
- Сауны (три сауны вместимостью от 4 до 6 человек);
- Турецкая баня;
- Массаж;
- Бильярд;
- Прокат лошадей хобби-класса;
- Прокат спортивного инвентаря;
- Интерактивный лазерный тир и другие услуги.

Расчетный час
Заезд – 1 апреля 2010 года в 18-00, выезд - 4 апреля в 12-00.

Организованный выезд из пансионата
Участников конференции будет ожидать автобус **4 апреля в 11.45** на парковке рядом с выездом с территории пансионата «Солнечная поляна».

Адрес пансионата «Солнечная поляна»:
Московская область, Одинцовский р-н, г. Звенигород, дер. Волково.

Беседка с камином:

1 апреля, четверг

19.00 – Вечеринка на свежем воздухе.

Главный корпус пансионата:

2 апреля, пятница

10.00 - 13.00 – Деловая программа конференции.
19.00 – Банкет в ресторане корпуса.

Регистрация участников будет проходить в фойе Главного корпуса.

Питание согласно программе конференции будет проходить в ресторане Главного корпуса.

Бизнес центр:

2 апреля (с 14.00) и 3 апреля – Деловая программа конференции.