# МАТЕМАТИЧЕСКИЕ МОДЕЛИ, МЕТОДЫ И АРХИТЕКТУРЫ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ: АНАЛИТИЧЕСКИЙ ОБЗОР ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ ИССЛЕДОВАНИЙ ПО РЕЗУЛЬТАТАМ МЕЖДУНАРОДНОГО СЕМИНАРА MMM-ACNS-2005

И. В. Котенко, М. В. Степашкин, Р. М. Юсупов

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<ivkote@comsec.spb.ru>, <stepashkin@comsec.spb.ru>, <yusupov@iias.spb.su>

УДК 681.3

*Котенко И. В., Степашкин М. В., Юсупов Р. М.* **Математические модели, методы и архитектуры для защиты компьютерных сетей: аналитический обзор перспективных направлений исследований по результатам международного семинара MMM-ACNS-2005** // Труды СПИИРАН. Вып. 3, т. 2. — СПб.: Наука, 2006.

**Аннотация.** *В статье дан аналитический обзор перспективных направлений исследований в области защиты компьютерных сетей, сделанный по результатам международного семинара «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2005), проведенного с 25 по 27 сентября 2005 года в Санкт-Петербурге. Освещена общая информация о семинаре, охарактеризованы приглашенные и секционные доклады, сделанные ведущими учеными в области защиты информации в таких перспективных направлениях исследований, как модели, архитектуры и протоколы для защиты информации, аутентификация, авторизация и управление доступом, анализ информационных потоков, скрытые каналы, политики безопасности и защита операционных систем, оценка уязвимостей, расследование инцидентов в сетях и обнаружение вторжений.* — Библ. 1 назв.

UDC 681.3

*Kotenko I. V., Stepashkin M. V., Yusupov R. M.* **Mathematical Models, Methods and Architectures for Computer Networks Security: the State-of-the-art Review of Perspective Directions of Research by Results of International Workshop MMM-ACNS-2005** // SPIIRAS Proceedings. Issue 3, vol. 2. — SPb.: Nauka, 2006.

**Abstract.** *The paper reviews the state-of-the-art of perspective research directions in the field of computer networks security fulfilled on basis of the International Workshop «Mathematical models, methods and architectures for computer networks security» (MMM-ACNS-2005), which took place from September, 25th till September, 27th 2005 in Saint-Petersburg. The common information on the workshop is presented, the invited and sectional reports of leading scientists in the field of information security in such perspective research directions as models, architectures and protocols for information security, authentication, authorization and access control, informational flow analysis, covert channels, security policy and operating system security, vulnerability assessment, network forensics and intrusion detection are described.* — Bibl. 1 items.

## 1. Введение

Третий международный семинар «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2005), проведенный с 25 по 27 сентября 2005 года в Санкт-Петербурге, — один из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей.

Первый и второй международные семинары MMM-ACNS-2001 и MMM-ACNS-2003, проведенные в 2001 и 2003 годах, продемонстрировали острый интерес исследовательских организаций и ученых всего мира к тематике использования формальных методов, моделей и построения перспективных архитек-

турных решений для обеспечения безопасности информационных ресурсов в компьютерных сетях.

Анализируя результаты MMM-ACNS-2001(2003, 2005), можно утверждать, что проведение подобного семинара в Санкт-Петербурге стимулирует разработку новых результатов и плодотворные обмены мнениями между различными школами в области защиты информации (как зарубежными, так и российскими), облегчает распространение новых идей и продвигает дух сотрудничества между исследователями в международном масштабе. Поэтому было решено регулярно (раз в два года) проводить этот семинар.

## 2. Общая информация о Международном семинаре

Семинар MMM-ACNS был организован Санкт-Петербургским институтом информатики и автоматизации РАН (СПИИРАН) и Университетом Бингхэмтона — государственным университетом штата Нью-Йорк (США). Финансовую поддержку семинара обеспечили Европейский офис аэрокосмических исследований и разработок (EOARD, США) и Офис военно-морских исследований (ONRGlobal, США). Международный программный комитет, включавший известных специалистов по теме семинара из 10 стран Европы, Австралии и Америки, выступал гарантом высокого научного уровня семинара.

Председателями организационного комитета конференции являлись Р.М. Юсупов (СПИИРАН) и И. Плониш (AFOSR, США), а председателями программного комитета — В.И. Городецкий (СПИИРАН), И.В. Котенко (СПИИРАН), В. Скормин (Университет Бингхэмтона, США).

В ходе подготовки к семинару было получено 85 статей из 20 стран. Наибольшее количество статей поступило из России, Кореи, США, Испании и Китая. Каждая из статей была тщательно проанализирована тремя–четырьмя рецензентами. В результате международным программным комитетом было отобрано 37 лучших докладов, представляющих 15 стран, в том числе Россию, США, Австрию, Китай, Францию, Корею, Италию, Испанию, Канаду, Германию, Грецию, Венгрию, Японию, Польшу и Тунис (рис. 1). Из этих докладов 25 было выбрано для полных презентаций и 12 — для коротких.

Кроме того, для участия в семинаре были персонально приглашены наиболее известные в мире специалисты в области защиты информации. В частности, с приглашенными докладами выступили такие ученые, как Наранкер Дулей (Имперский Колледж Лондона, Великобритания), Мин-Ю Хуанг (компания Боинг, США), Сушил Джаджодиа (Университет Джорджа Мейсона, США), Давид Николь (Иллинойский университет, США) и Виктор Скормин (Университет Бингхэмтона, США).

Кроме приглашенных докладов, программа семинара включала работу *шести секций*: (1) математические модели, архитектуры и протоколы для защиты информации; (2) аутентификация, авторизация и управление доступом; (3) анализ информационных потоков, скрытые каналы и управление в доверенных системах; (4) политики безопасности и защита операционных систем; (5) моделирование угроз безопасности, оценка уязвимостей и расследование инцидентов в сетях; (6) обнаружение вторжений.

На семинаре была проведена *панельная дискуссия* (рис. 2), посвященная обсуждению состояния и актуальных направлений исследований в области анализа уязвимостей и обнаружения вторжений. В панельной дискуссии приняли участие М.-Ю. Хуанг (компания Боинг, США) — ведущий дискуссии,



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В. Городецкий (СПИИРАН, Россия), А. Грушо (Российский Государственный Гуманитарный Университет, Россия), С. Джаджодиа (Университет Джорджа Мейсона, США), Н. Дулей (Имперский Колледж Лондона, Великобритания), П. Зегжда (Санкт-Петербургский Государственный Технический Университет, Россия), И. Котенко (СПИИРАН, Россия), Д. Николь (Иллинойский университет, США), В. Скормин (Университет Бингхэмтона, США) и С.-К. Чин (Сиракузский университет, США).

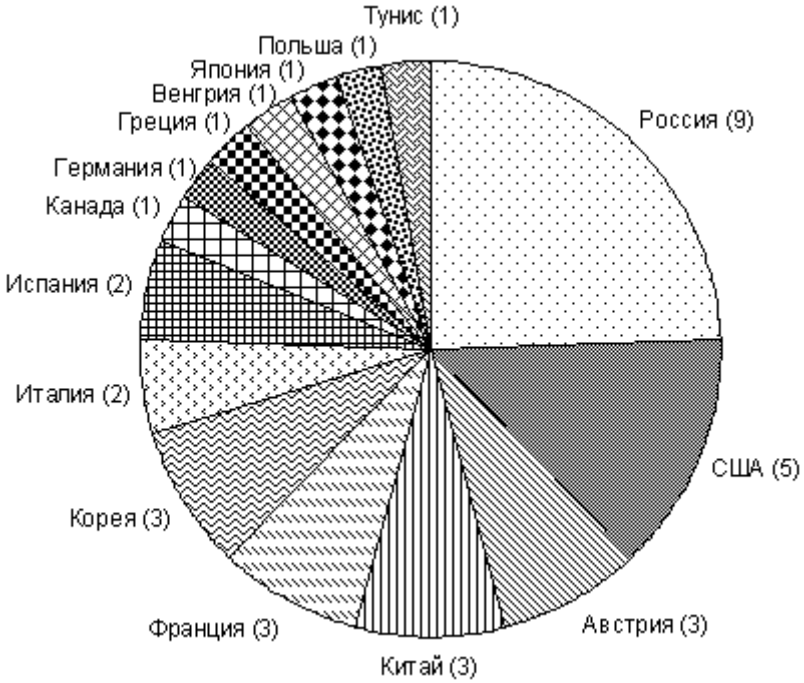


Рис. 1. Статистика по принятым докладам
(в скобках указано количество докладов от каждой страны).

Рис. 2. Во время проведения панельной дискуссии (слева направо — Н. Дулей, С.-К. Чин, С. Джаджодиа, В. Скормин, Д. Николь, П. Зегжда, А. Грушо, В. Городецкий, И. Котенко).



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

*Труды семинара опубликованы* в престижном международном научном издании, «Lecture Notes in Computer Science», издательство «Шпрингер», Германия, том 3685 под редакцией В. Городецкого (Россия), И. Котенко (Россия) и В. Скормина (США) [1].

Краткий обзор научного содержания приглашенных докладов, а также секционных докладов приводится ниже.

## 3. Содержание приглашенных докладов

На семинаре было представлено пять приглашенных докладов.

*Н. Дулей* (*Naranker Dulay, Имперский Колледж Лондона, Великобритания*) представил доклад на тему **«Самоуправляемые ячейки для повсеместных систем»** (в соавторстве с *Э. Лупу*, *М. Сломаном*, *Д. Свентеком*, *Н. Бадр* и *С. Хипс*). Актуальность и важность данного доклада подтверждается тем, что совершенствование повсеместных (ubiquitous) вычислительных инфраструктур может значительно расширить роль вычислений в повседневной жизни людей на основе быстрого распространения персональных беспроводных устройств и, что особенно важно, использования беспроводных вычислительных устройств, встраиваемых в различные среды: здания, дороги, транспортные средства, ландшафт, домашние приборы, одежду, упаковку потребительских товаров, и даже в виде имплантантов в растения, животных и людей. Использование повсеместных вычислений (ubiquitous computing) требует обеспечения поддержки управления персональными беспроводными устройствам и датчиками. В докладе автор раскрыл основанную на политиках (как множестве правил функционирования) общую архитектуру систем повсеместных вычислений, которая позволяет обеспечивать управление на различных уровнях, базируясь на понятии самоуправляемых ячеек (self-managed cells). Такие ячейки подразумевают использование управляемых политикой агентов, которые осуществляют разграничение доступа пользователей на основе контекста и доверия, а также адаптацию системы к изменяющимся условиям функционирования. Ячейки могут самоорганизовываться на основе механизмов объединения (федерации) и вложения. Основные перспективы использования такого подхода связаны с возможностью организации эффективного управления информационными ресурсами со стороны повсеместных систем, в том числе реализации функций обнаружения, фиксации, обработки и отображения (публикации) информации. Следует отметить, что эта информация может быть недолговечной, мобильной, фрагментированной и объемной и т.п., что затрудняет ее обработку.

Автор проанализировал такие понятия и компоненты управления информационными ресурсами как самоуправляемые ячейки (self-managed cells), «сторожевые» ячейки (cell watchdog), сервис события (event service), сервис обнаружения (discovery service), сервис политики (policy service), сервис домена (domain service), сервис контекста (context service), сервис доверия (trust service), язык политики ячейки (cell policy language), взаимодействие между ячейками (inter-cell interactions) и самоорганизация ячеек (self-organization).

В своем докладе Н. Дулей указал на существование множества неразрешенных проблем в данном направлении исследований, связанных, например, с решением следующих вопросов: (1) как обеспечить, чтобы протоколы оптимизировали расход потребляемой электроэнергии; (2) как удостовериться, что устройство управляется соответствующей ячейкой и не «захвачено» нелегитимной ячейкой (злоумышленником); (3) как представлять управляющую информацию



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

и политики конечным пользователям и выявлять параметры настройки политики; (4) какие паттерны проектирования лучше использовать для управления ячейками; (5) как специфицировать и реализовать политики, позволяющие управлять доступом к личной информации; (6) какие механизмы использовать для обеспечения защиты личной информации и предотвращения слежки.

В докладе *М.-Ю. Хуанга* (*M.-Y. Huang, компания Боинг, США*) **«Критические проблемы информационной безопасности для современных крупномасштабных инфраструктур»** основное внимание было уделено развитию положения о том, что в настоящее время цели обеспечения информационной безопасности связаны, главным образом, не с защитой информации от несанкционированного доступа, а с тем, как обеспечить надежный доступ легитимных пользователей к необходимым ресурсам. В современных военных и коммерческих системах различные пользователи (партнеры, поставщики, клиенты) постоянно обращаются к информационной инфраструктуре с использованием телекоммуникационных сетей. Каждый легитимный пользователь должен получить доступ непосредственно к требуемым данным и ресурсам. Безопасное и эффективное управление доступом в этом контексте является базисом сдвига к парадигме выполнения бизнес-операций следующего поколения, которая создает новые возможности для развития деловых операций и приводит к увеличению его эффективности. Те, кто не в состоянии сделать этот переход, будут вынуждены столкнуться со значительными проблемами в конкурентной борьбе. Информационная безопасность в текущих условиях, по существу, является двигателем бизнеса.

В докладе был представлен широкий диапазон критических проблем информационной безопасности, возникающих в современной бизнес-среде, и обсуждены потенциальные архитектурные и технологические направления, связанные с применением больших и распределенных инфраструктур. Автор сделал вывод, что механизмы обеспечения информационной безопасности, не берущие в расчет важные аспекты используемой парадигмы деловых операций, ведут к очень рискованному бизнесу. Причиной неудач в защите информации в значительной степени является использование устаревших механизмов и неспособность распознать и учесть революционные требования к реализации механизмов информационной безопасности.

*С. Джаджодиа* (*S. Jajodia, Университет Джорджа Мейсона, США*) сделал доклад **«Топологический анализ уязвимостей на основе правил»**, подготовленный в соавторстве с *В. Сваруп* и *Д. Памула*. Доклад был посвящен задаче исследования уязвимостей компьютерных сетей и построения графов атак. Эта задача важна для определения возможностей нарушителя в данной конфигурации сети и выявления «узких мест» в защите. Было отмечено, что нарушитель, как правило, проникает в компьютерную сеть, исследует и изменяет ее конфигурацию, используя многочисленные уязвимости. Например, он может выполнить последовательность действий, которые вначале направлены на исследование уязвимых систем в сети, затем использует одну из обнаруженных уязвимостей для получения привилегий пользовательского уровня, затем эксплуатирует другую уязвимость для получения привилегии уровня администратора сети, и, наконец, компрометирует систему, используя полученные привилегии.

Графы атак представляют собой последовательности реализации известных атак, которые нарушители могут использовать для компрометации компьютерных сетей. В настоящее время предложены различные методики для авто-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

матической генерации графов атак по заданной конфигурации компьютерной сети. Для генерации графов атак эти методики применяют средства проверки на модели (model checkers), недостатком которых является низкая масштабируемость, или основываются на предположении о монотонности (когда последующее действие не может отменить предыдущее), которое не позволяет представить реальные ситуации. В докладе автор предложил методику анализа уязвимостей, которая является более масштабируемой, чем решения, базирующиеся на средствах проверки на модели, и более выразительны, чем решения, основанные на предположении о монотонности. В своем подходе он представил индивидуальные атаки, как правила перехода системы из одного состояния в другое и определил непересекающиеся (noninterfering) наборы этих правил, приводящие к достижению определенной цели (например, получению доступа к определенной информации). Автор предложил эффективные алгоритмы генерации таких наборов правил. Было подчеркнуто, что эти алгоритмы остаются эффективными и для произвольных немонотонных наборов правил. Таким образом, предложенный подход позволяет представлять ситуации, в которых выполнение средств компрометации (эксплоитов) со стороны нарушителей имеет побочный эффект временного сокращения возможностей нарушителя.

Четвертый приглашенный доклад, названный **«Модели и анализ активной защиты от сетевых червей»**, был представлен *Д. Николь* (*D. Nicol, Иллинойский университет, США*) в соавторстве с *М. Лилдженстам*. Разработка мер защиты против сетевых червей и саморазмножающихся вирусов, обладающих способностью быстрого распространения в сети Интернет, в последнее время стала чрезвычайно актуальной задачей. До настоящего времени большинство предложенных методов защиты являлись пассивными, так как они были предназначены для блокирования или замедления распространения сетевых червей, или реализации их обнаружения и фильтрации. Активная защита сводится к противодействию сетевым червям за счет устранения или изоляции зараженных хостов, и/или автоматического и активного исправления «дыр» (на базе установки пакетов программных коррекций) в программном обеспечении уязвимых, но еще не инфицированных хостах. Понятие активной защиты затрагивает важные юридические и этические аспекты, которые могут привести к запрету их реализации для широкого использования в Интернет. Однако следует отметить, что активная защита может иметь непосредственное применение в специализированных сетях, принадлежащих отдельным компаниям или правительственным учреждениям.

В своем докладе Д. Николь предложил использовать моделирование для анализа эффективности активных методов защиты от сетевых червей и саморазмножающихся вирусов. Используя дискретные стохастические модели, он доказал, что механизмы защиты можно строго упорядочить в терминах их возможностей по противодействию. Используя континуальные монотонные модели, автор рассмотрел показатели эффективности защиты в терминах числа хостов, защищенных от внедрения злонамеренного программного кода, полной сетевой пропускной способности, использованной червем и механизмами защиты, а также пикового коэффициента сканирования, который допустим для заданной сети в процессе противодействия сетевым червям. Автор получил количественные границы необходимой производительности механизмов защиты. Эти результаты могут рассматриваться как математический базис для анализа механизмов активной защиты от сетевых червей. Автор рассмотрел четыре та-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ких механизма: (1) установка пакетов программных коррекций на неинфицированных хостах, (2) увеличение популяции компонентов активной защиты на основе использования неинфицированных хостов, восприимчивых к червям, (3) подавление зараженных хостов, обнаруженных на основе сканирования, и (4) подавление зараженных хостов, обнаруженных на основе сканирования и анализа сетевого трафика. Используя обобщенную дискретную стохастическую модель, автор показал, что введение каждого дополнительного механизма защиты (в том порядке, который был приведен выше) приводит к последовательному увеличению эффективности защиты от сетевых червей. Способность изучать поведение червей на основе таких методов ведет к лучшему пониманию решений по защите. Д. Николь отметил, что в данной области исследований еще многое необходимо сделать. Несмотря на важность полученных результатов, в докладе не была освещена весьма важная проблема автоматического обнаружения момента инициирования червя. Автор исследовал только эффективность защитных мер, активизируемых после обнаружения распространения червя.

Приглашенный доклад **«Предотвращение информационных атак посредством обнаружения в реальном времени саморепликации в компьютерном коде»**, представленный *В. Скормином* (*V. Skormin, Университет Бингхэмтона, США*) и подготовленный в соавторстве с *Д. Саммервиллем*, *А. Волынкиным* и *Д. Моронски*, посвящен решению актуальной задачи обнаружения неизвестных вирусов. Авторы утверждают, что потенциальное количество механизмов саморепликации кода конечно, и именно поэтому, если обладать способностью их автоматического обнаружения, можно разработать некоторое универсальное программное средство для обнаружения вирусов. Причина выбора механизма саморепликации в качестве критерия обнаружения состоит в том, что незлонамеренные коды, как правило, не используют механизмы самораспространения, в то время как саморепликация является крайне важной для реализации широкого спектра компьютерных вирусов и червей.

В докладе представлен подход к реализации превентивной защиты, как от известных, так и от неизвестных злонамеренных исполняемых кодов. В отличие от широко применяемых подходов, предлагаемый подход не использует сканирование кода на наличие сигнатур известных вирусов. Вместо этого он базируется на обнаружении попыток выполнимого кода самореплицироваться в течение времени выполнения. Этот подход является расширением ранее разработанного авторами метода обнаружения неизвестных вирусов в кодах, базирующихся на скриптах.

Одно из основных преимуществ предложенного подхода — его способность обнаруживать неизвестные вирусы с очень низким процентом ложных тревог. Кроме того, обнаружение выполняется независимо от используемого стиля, языка программирования и компилятора на очень низком уровне в операционной системе, где могут быть проверены наиболее важные действия. Это препятствует снижению производительности системы обнаружения, обусловленному обработкой бесполезных системных вызовов, которые могут быть достигнуты на более высоком и более уязвимом уровне, но позволяет осуществлять контроль всех процессов, обращающихся к основным функциям операционной системы. Обнаружение осуществляется монитором времени выполнения, который реализует непосредственное обнаружение и завершение любого количества подозрительных процессов, выполняющихся в текущее время в системе.



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Хотя в описываемой работе сделана попытка разработки метода, позволяющего обнаруживать и учитывать все существующие способы саморепликации, могут существовать некоторые новые методики реализации вирусов, которые обходят предложенные методы обнаружения. Автор заявил о том, что он знает об осуществимости многопроцессной саморепликации, которая может быть реализована высококвалифицированными нарушителями, и намеревается разработать методы ее обнаружения в будущих исследованиях. Тем не менее, необходимо отметить, что большинство компьютерных атак использует менее сложные методы программирования, и поэтому предложенная технология обнаружения может быть с успехом применена.

Во время презентации В. Скормином было продемонстрировано программное средство, реализующее предложенную методику для операционных систем семейства Microsoft Windows.

## 4. Секция «Математические модели, архитектуры и протоколы для защиты информации»

На секции было представлено четыре доклада и два сообщения.

*К. Деко* (*C. Daicos, Королевский Военный Колледж Канады, Канада*) в соавторстве со *С. Найтом* (S. Knight) представил доклад **«Пассивная методика наблюдения за внешними Web-ресурсами для частных сетей»**. В этой работе предлагается методика контент-анализа, названная «Формирование цепочки связей», которая предназначена для поддержки процесса формирования сетевых сеансов (sessionization). Результатом выполнения методики являются большие части сеансов, называемые фрагментами сеанса.

Автор показал, что пассивное внешнее наблюдение в частных сетях за коммуникациями, ведущимися с хостов, пользователи которых просматривают Web-ресурсы, является возможным, несмотря на эффекты анонимизации, выполняемые NAT и прокси-серверами на шлюзах. Эти устройства эффективно скрывают источник сетевых потоков, и удаляют множество идентификационных атрибутов, затрудняя процесс группировки пакетов сетевого трафика во взаимно непересекающиеся наборы пакетов, характеризующие работу отдельных пользователей и хостов (и называемые сеансами). Сеансы позволяют иметь полную картину работы каждого пользователя сети. Без их выделения пассивное внешнее наблюдение не приносит большой пользы.

Предлагаемая методика основана на знании того, что большинство загружаемых Web-ресурсов представляет собой композицию web-страниц, получаемых пользователем с различных сайтов. Посредством перемещения по гиперсвязям в теле HTTP-сообщений, собранных пассивными методами, Web-трафик сети может быть объединен во фрагменты сеансов, и использоваться аналитиками-людьми для выделения сеансов индивидуальных пользователей.

Представленная в докладе реализация методики показала возможность ее использования.

*Д.Э. Джонсон* (*J.E. Johnson, Университет Штата Южная Каролина, США*) в докладе **«Сети, моноиды Маркова и обобщенная энтропия»** представил теоретический взгляд на анализ вероятностных параметров информационных потоков, возникающих между узлами компьютерной сети. Он использовал понятие матрицы инцидентности и проанализировал ее свойства, применяя аппарат абстрактной алгебры и энтропии. Автор показал, что матрица инцидентности может быть использована для получения непрерывного преобра-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

зования Маркова, которое может интерпретироваться как создание необратимого потока сообщений между узлами соответствующей сети.

В докладе *М. Смирнова* (*M. Smirnov, Институт Фраунхофера Фокус, Германия*) **«Доверие посредством потоков работ в автономных коммуникациях»** рассмотрена задача проектирования систем автономных коммуникаций, известных также как одноранговые системы связи или системы “peer-to-peer” коммуникаций. В таких системах существует множество взаимозависимостей между различными интересами и требованиями, что чрезвычайно усложняет задачу их проектирования. Один из перспективных подходов к решению этой задачи — не пытаться решать все возможные проблемы на стадии проектирования, а ввести в систему такие возможности, которые облегчат решение возникающих проблем во время ее функционирования. Автономные сетевые элементы в одноранговой среде должны сотрудничать друг с другом при осуществлении доступа к средствам коммуникации и доставки информации. В докладе показано, как эти элементы могут прийти к взаимному доверию и самоорганизовываться на основе обмена планами потоков работ по обработке информации. На основе учета эффективности работы локально определенного семейства сетевых элементов введена так называемая модель этикета. Большая часть доклада была посвящена описанию процесса проектирования модели этикета на основе использования протокола поведения сетевых элементов и рассмотрению примера их коммуникации.

Доклад *Б. Тсоумаса* (*Bill Tsoumas, Афинский Университет Экономики и Бизнеса, Греция*) **«Онтологический подход к управлению безопасностью информационных систем»**, подготовленный совместно со *С. Дритсасом* (S. Dritsas) и *Д. Гритцалисом* (D. Gritzalis), посвящен рассмотрению онтологического подхода к решению задач безопасности. Использование данного подхода обосновывается сложностью современных информационных систем.

Предлагаемый подход предназначен для поддержки совместного и многократного использования знаний по обеспечению безопасности явным и согласованным способом. В докладе представлена основанная на знаниях и онтологии архитектура управления безопасностью произвольной информационной системы. Автор продемонстрировал возможность реализации данного подхода, в том числе возможность трансляции утверждений политики высокого уровня в настройки конкретных устройств. Б. Тсоумас показал, что такая архитектура может поддерживать действия экспертов по определению требований к безопасности и выбору необходимых мер защиты.

В докладе также представлен структурный подход к формированию архитектуры управления безопасностью и идентификации ее критических частей.

В сообщении *С. С. Йео* (*S. S. Yeo, Чунгангский Университет, Сеул, Корея*) **«Новая схема защиты информации о местоположении в средах мобильной коммуникации»**, подготовленном совместно со *С. С. Ким* (S. S. Kim), *Х. Д. Парк* (H. J. Park) и *С. К. Ким* (S. K. Kim), предложен подход к защите данных о местоположении пользователя от атак внутри мобильной сети, проанализирована его эффективность.

*В. Молисц* (*W. Molisz, Гданьский Университет технологии, Польша*) совместно с *Д. Рак* (J. Rak) представили сообщение **«Схема защиты/восстановления зоны в живучих сетях»**. В этом сообщении предложено понятие защиты/восстановления зоны передачи сообщений, в соответствии с которым для защиты некоторой области активного пути передачи сообщений используется специальный резервный путь. Авторы показали, что использова-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ние предложенных механизмов защиты/восстановления позволяет сохранить на разумном уровне время восстановления и объем используемых сетевых ресурсов.

## 5. Секция «Аутентификация, авторизация и управление доступом»

На секции было представлено два доклада и три сообщения.

Доклад *Т. Косиатракул, С. Олдер* и *Ш.-К. Чин* (*T. Kosiyatrakul, S. Older, S.-K. Chin, Сиракузский Университет, США*) **«Модальная логика для ролевого управления доступом»**, представленный Ш.-К. Чин, ввел логику управления доступом, позволяющую не только специфицировать механизмы ролевого управления доступом, но и рассуждать о них. Актуальность решаемой задачи мотивируется известным фактом, что создание правильных решений по управлению доступом является одним из центральных аспектов обеспечения защиты информации. Это, в свою очередь, требует корректного учета идентификаторов, сертификатов, ролей, полномочий и привилегий пользователей и их агентов. В сетевых системах эти решения являются сложными из-за необходимости поддержки механизмов делегации полномочий и использования различных политик контроля доступа.

Логика управления доступом, предложенная в докладе, обеспечивает методы выполнения строгих рассуждений об управлении доступом. Эта логика, с одной стороны, является достаточно простой для использования проектировщиками с целью обеспечения соответствия проектируемых систем требованиям контроля доступа, а, с другой стороны, — достаточно мощной, чтобы рассуждать о делегировании, сертификатах и доверенных полномочиях.

В докладе описаны такие компоненты ролевого управления доступом, как назначение пользователей, назначение разрешений, наследование ролей, активация ролей и запросы пользователей. Доказана корректность предложенной логики и ее расширений, и осуществлена ее реализация в системе автоматического доказательства теорем HOL (Higher Order Logic, версия 4). Логика также обеспечивает формальную поддержку для ролевого управления доступом, статическое разделение обязательств и динамическое разделение ограничений на обязательства в системе автоматического доказательства теорем HOL. Авторы заявили, что HOL может использоваться для проверки свойств политик ролевого управления доступом, сертификатов, полномочий и делегаций.

В докладе *П. Шартнера* и *М. Шаффера* (*P.Schartner, M.Schaffer, Университет Клагенфурта, Австрия*) **«Уникальные цифровые псевдонимы, генерируемые пользователем»** рассмотрена методика формирования цифровых псевдонимов, которая не использует централизованных запрашивающих сторон (issuers) или любых онлайн-коммуникаций между ними. В соответствии с предложенной методикой, каждый пользователь может сформировать собственный псевдоним локально в некоторой среде защиты, например, в своей смарт-карте или с использованием личного электронного секретаря. Данный подход не требует какого-либо информационного обмена между задействованными сторонами или наличия глобальных данных (особенно ключей), кроме уникальных идентификаторов каждого пользователя и каждого устройства системы. Кроме того, держатель псевдонима может доказать, что он сгенерировал определенный псевдоним, не показывая его идентификатор, и он может показать его идентификатор посредством раскрытия псевдонима. Следует учиты-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

вать, что верификатор раскрытого псевдонима может убедиться, что предъявитель псевдонима является его держателем (то есть, пользователем, который первоначально сгенерировал этот псевдоним). Идентификатор пользователя и идентификатор устройства пользователя используются для генерации уникальных псевдонимов, причем оба компонента сохраняются в псевдониме в зашифрованной форме.

В сообщении *Э. Йедеса*, З. *Хорнака* и *К. Кормоцы* (*Erno Jedes, Zoltan Hornak, Ksaba Kormoczi, SEARCH Lab, Венгрия*) **«Кодирование секретного ключа с использованием отпечатка пальца»**, сделанном З. Хорнаком, предложен метод хранения секретного ключа, закодированного на основе отпечатка пальца (fingerprint). В соответствии с этим методом ключ может быть извлечен только с использованием отпечатка пальца владельца. Предложенный подход совместим с существующими инфраструктурами публичных ключей (Public Key Infrastructures, PKI), и может быть использован в широко применяемых в настоящее время приложениях, в которых для проверки цифровых сертификатов реализуется асимметричное шифрование.

*М. Шаффер* и *П. Шартнер* (*P. Schartner, M. Schaffer, Университет Клагенфурта, Австрия*) представили второе сообщение этой секции, имеющее название **«Депонирование ключей, использующее структуру доступа на основе деревьев»**. В этом сообщении предложена система, в которой множество людей может вести конфиденциальный обмен сообщениями на базе общего сеансового ключа. Предполагается, что из-за обеспечения требования наблюдаемости со стороны государственных структур, этот ключ будет депонирован на основе использования многосторонней версии криптосистемы Эльгамаля.

*С. Янг* (*S. Yang, Университет Сувона, Корея*) сделала третье сообщение **«Модель эффективного управления доступом, использующая атрибутное структурирование сертификатов»**. Основная идея предлагаемого подхода состоит в группировании и структурировании ролей в дерево отношений. Для обеспечения распределения сертификатов спецификации ролей, автор предлагает использовать мультивещание (мультикастинг). Улучшение производительности структурирования сертификатов спецификации ролей оценивается в количестве потерь пакетов. Показано, что предложенные процессы обновления и распределения ролей являются защищенными и эффективными.

## 6. Секция «Анализ информационных потоков, скрытые каналы и управление в доверенных системах»

На данной секции было представлено три доклада и одно сообщение.

В докладе **«Вероятностный, ориентированный на свойства подход к информационным потокам»**, подготовленном *Д. Беаукуйером*, *М. Дюфло* (*D. Beauquier, M. Duflot, Университет Парижа 12, Франция*) и *Мариусом Минеа* (*Marius Minea, Instmtym e-Austria, Румыния*), исследуются вероятностные информационные потоки с точки зрения ориентации на свойства. Для представляющего интерес свойства, специфицированного в виде множества трасс, определяется, влекут ли разные наблюдения нижнего уровня различные вероятности возникновения свойства. Учитывая все свойства заданного класса (например, трассы высокого уровня, или последовательности высокого уровня, отделенные событиями нижнего уровня), авторы получают различные определения информационного потока. Они анализируют системы, которые являются



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

безопасными согласно этим определениям. Авторы рассматривают свойства, которые выражены с использованием трассы в целом, и свойства, которые различаются между прошлым и будущим событиями по отношению к некоторой контрольной точке. В этой архитектуре выразимы как некоторые классические определения вероятностной безопасности, так и более детальные количественные меры информационного потока.

Рассмотрены теоремы, характеризующие структуру систем, для которых гарантируется отсутствие информационных потоков согласно этим понятиям: например, для свойств, которые могут отличать последовательности событий высокого уровня, отделенные событиями нижнего уровня необходим некоторый изоморфизм между вероятностными деревьями. Также показано, как некоторые классические понятия вероятностного информационного потока, такие как невыводимость (noninference), невмешательство (noninterference) и сепарабельность, могут быть выражены с использованием качественных версий предложенных определений.

В докладе **«Обобщенное абстрактное невмешательство: абстрактный анализ безопасных информационных потоков для автоматов»** *Р. Гиакобацци* и *И. Мастроени* (*R. Giacobazzi, I. Mastroeni, Университет Вероны, Италия*) было рассмотрено свойство абстрактного невмешательства (noninterference), введенное как ослабляющее невмешательство, моделирующее нарушителей в форме абстрактных интерпретаций семантики языка программирования (то есть статических анализаторов).

Авторы обобщили понятие абстрактного невмешательства, чтобы иметь дело с древовидными моделями вычислений. Это позволило расширить границы абстрактного невмешательства для моделирования свойств безопасности, используя автоматы как модели систем реального времени и конкурентных систем. Показано, что известные определения невмешательства в этих моделях вычислений могут рассматриваться как примеры предложенного обобщения. Данный результат доказывает, что абстрактное невмешательство может разумно трактоваться как общая структура для исследования и сравнения свойств безопасности на различных уровнях абстракции.

В докладе *А. Грушо* и *Е. Тимониной (Российский Государственный Гуманитарный Университет, Россия*) **«Обнаружение несанкционированного информационного потока»** утверждается, что компетентный наблюдатель может обнаружить несколько типов статистических скрытых каналов, которые нарушают политику безопасности информационной системы, обеспечивая передачу информации между враждебными агентами.

Авторы вводят базовую методику обнаружения скрытых каналов и анализируют условия, при которых наблюдатель с ограниченными ресурсами может успешно выполнить свою задачу. В частности, полученные результаты показывают, что для посылки скрытых сообщений может быть выявлено манипулирование распределением вероятностей сообщений в каналах связи. Наблюдатель должен достаточно хорошо знать нормальные свойства каналов связи и их вероятностные характеристики. Тогда возможно создать непротиворечивый тест для обнаружения скрытого сообщения. Именно поэтому основной задачей является формирование статистически скрытого канала, невидимого для наблюдателя. Даже если ресурсы наблюдателя ограничены, скрытое сообщение может быть обнаружено достаточно надежно.

Сообщение *А. Галатенко*, *А. Грушо*, *А. Князева* и *Е. Тимониной* (*Российский Государственный Гуманитарный Университет, Россия*) **«Статистиче-**



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

**ские скрытые каналы через прокси-сервер»** было также представлено А. Грушо. Сообщение посвящено созданию скрытого канала, формируемого на основе перестановки данных в буфере сервера путем использования последовательности пакетов, которые исходят из маршрутизатора, связанного с прокси-сервером. Результирующий поток данных позволяет создавать статистически скрытый канал, который передает информацию, манипулируя математическим ожиданием и дисперсией количества пар в последовательности сетевых адресов.

## 7. Секция «Политики безопасности и защита операционных систем»

На секции было представлено два доклада и два сообщения.

Доклад *Ф. Ж. Г. Клементе*, *И. Д. Х. Ре*, *Г. М. Переса* и *А. Ф. Г. Скармета* (*F. J. G. Clemente, J. D. J. Re, G. M. Perez, A. F. G. Skarmeta, Университет Мурсии, Испания*) **«Регулируемое политикой управление маршрутизацией на основе CIM»** был представлен первым автором. В докладе рассмотрен подход к управлению сетью на основе политик. Подход позволяет реализовать перспективную технологию развертывания и развития сетевых сервисов и приложений, обеспечивающую их (и всей сети в целом) единое системное представление. Предложенный подход подразумевает комбинированное управление различными сетевыми сервисами (безопасности, качества обслуживания (QoS) и маршрутизации).

В докладе представлены полученные авторами результаты по моделированию и развертыванию политик маршрутизации на основе использования стандарта и средств «Common Information Model» (CIM). Также представлена выполненная реализация предложенной системы управления маршрутизацией, которая была успешно протестирована и использовалась для конфигурирования нескольких сетей IPv6, развернутых в рамках европейского проекта Euro6IX.

В докладе *Д. П. Зегжды* и *А. М. Вовк* (*Санкт-Петербургский Политехнический Университет, Россия*) **«Безопасная гибридная Операционная система Linux over Fenix»** рассмотрен подход к созданию безопасных систем обработки данных, основанных на использовании гибридной операционной системы Linux over Fenix. Подход основан на одновременном использовании на одном и том же компьютере нескольких различных операционных систем и обеспечении взаимодействия между ними.

Авторы предлагают использовать безопасную операционную систему Fenix, разработанную в Санкт-Петербургском Государственном Политехническом Университете, в качестве ведущей операционной системы, а популярную операционную систему Linux — в качестве гостевой операционной системы, обеспечивая совместимость с традиционными приложениями. Предлагаемый гибридный подход позволяет обеспечить следующие свойства: (1) полный контроль над всеми информационными взаимодействиями и потоками со стороны доверенных безопасных компонент операционной системы Fenix, за счет чего обеспечивается высокий уровень безопасности; (2) отсутствие возможности обхода или отмены механизмов защиты, так как средства защиты Fenix непосредственно взаимодействуют с аппаратной платформой, в то время как средства Linux, напротив, не имеют доступа к ним; (3) набор доступных приложений может быть расширен, учитывая приложения Linux, что позволяет использовать



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Linux over Fenix фактически везде, где используется Linux; (4) минимизация расхода ресурсов на защиту — в дополнение к коду, обычно используемому в Linux, применяется только код, реализующий необходимые механизмы защиты Fenix.

В сообщении *Ф. Ж. Г. Клементе*, *Г. М. Переса* и *А. Ф. Г. Скармета* (*F. J. G. Clemente, G. M. Perez, A. F. G. Skarmeta, Университет Мурсии, Испания*) **«Архитектура управления, базирующаяся на XML-реализации интегрированной политики»** была описана методика сквозной интеграции XML-технологий в архитектуру управления на основе политик. Авторы предложили архитектуру управления, основанную на XML технологиях, определение информационной базы политик на XML и новый общий открытый сервис политик (Common Open Policy Service), реализованный на языке программирования Java. Разработанный сервис поддерживает два вида кодирования данных политики, которыми обмениваются так называемые PDP-серверы (Policy Decision Point — серверы точек принятия решений по политикам) и PEP-клиенты (Policy Enforcement Point — клиенты точек выполнения политик): XML-кодирование и кодирование, основанное на бинарной кодификации информации.

В сообщении также проанализированы основные методики, используемые для обеспечения сервисов безопасности при управлении политиками.

*А. Тишков* (*Санкт-Петербургский институт информатики и автоматизации РАН, Россия*) представил второе сообщение **«Архитектура верификатора защиты для управления безопасностью на основе политик»**, подготовленное совместно с *И. Котенко* и *Е. Сидельниковой*. В сообщении рассмотрена архитектура модуля верификации, предназначенного для обнаружения и разрешения конфликтов в политике безопасности. Модуль верификации рассматривается как многомодульное приложение. Менеджер верификации запускает зарегистрированные в системе модули верификации, которые осуществляют поиск противоречий в наборе правил на основе собственных математических методов. Модули, способные разрешить конфликт (изменяя набор правил), запускаются последовательно. Модули, предназначенные только для обнаружения конфликтов, могут быть запущены параллельно с другими. Все модули имеют фиксированную структуру, полученную на основе наследования от одного абстрактного класса, что делает систему открытой для добавления новых модулей.

Продемонстрированы механизмы обнаружения конфликтов, основанные на исчислении событий.

## 8. Секция «Моделирование угроз безопасности, оценка уязвимостей и расследование инцидентов в сетях»

На секции было представлено три доклада и одно сообщение.

Доклад *Ф. Баярди*, *К. Тельмона* (*F. Baiardi, C. Telmon, Университет Пизы, Италия*) **«Теоретическая модель для усредненного воздействия атак на билинговые инфраструктуры»** был представлен Ф. Баярди. Автор рассмотрел математическую модель, названную моделью «нулевой задержки», предназначенную для оценки воздействия атак на инфраструктуру, служащую для составления счетов множеству пользователей некоторого сервиса. Данная модель представляет поиск и использование уязвимостей в виде соревнования между множеством атакующих и защищающихся, заинтересованных, соответственно, в реализации атак на данную инфраструктуру и внесении исправлений



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

в нее для защиты. Как следует из названия этой модели, она основывается на том, что и нападение, и внесение исправлений происходят сразу после обнаружения уязвимости. Предполагается, что мощность воздействия увеличивается с ростом размера окна уязвимости, т.е. времени, прошедшего с момента обнаружения уязвимости некоторым атакующим и защищающимся. В модели этот размер связан с количеством атакующих и защищающихся.

В докладе также рассмотрены примеры использования предложенной модели.

В докладе *И. Котенко* и *М. Степашкина* (*Санкт-Петербургский институт информатики и автоматизации РАН, Россия*) **«Анализ уязвимостей и измерение уровня защищенности на этапах проектирования и эксплуатации жизненного цикла компьютерных сетей»** (рис. 3) предложен подход к активному анализу уязвимостей и оценке уровня защищенности компьютерных сетей, который может быть реализован на различных стадиях их жизненного цикла. Предлагаемый подход к анализу уязвимостей и оценки уровня защищенности базируется на механизмах автоматической генерации и выполнения распределенных сценариев атак с учетом разнообразия целей и уровня знаний злоумышленников.

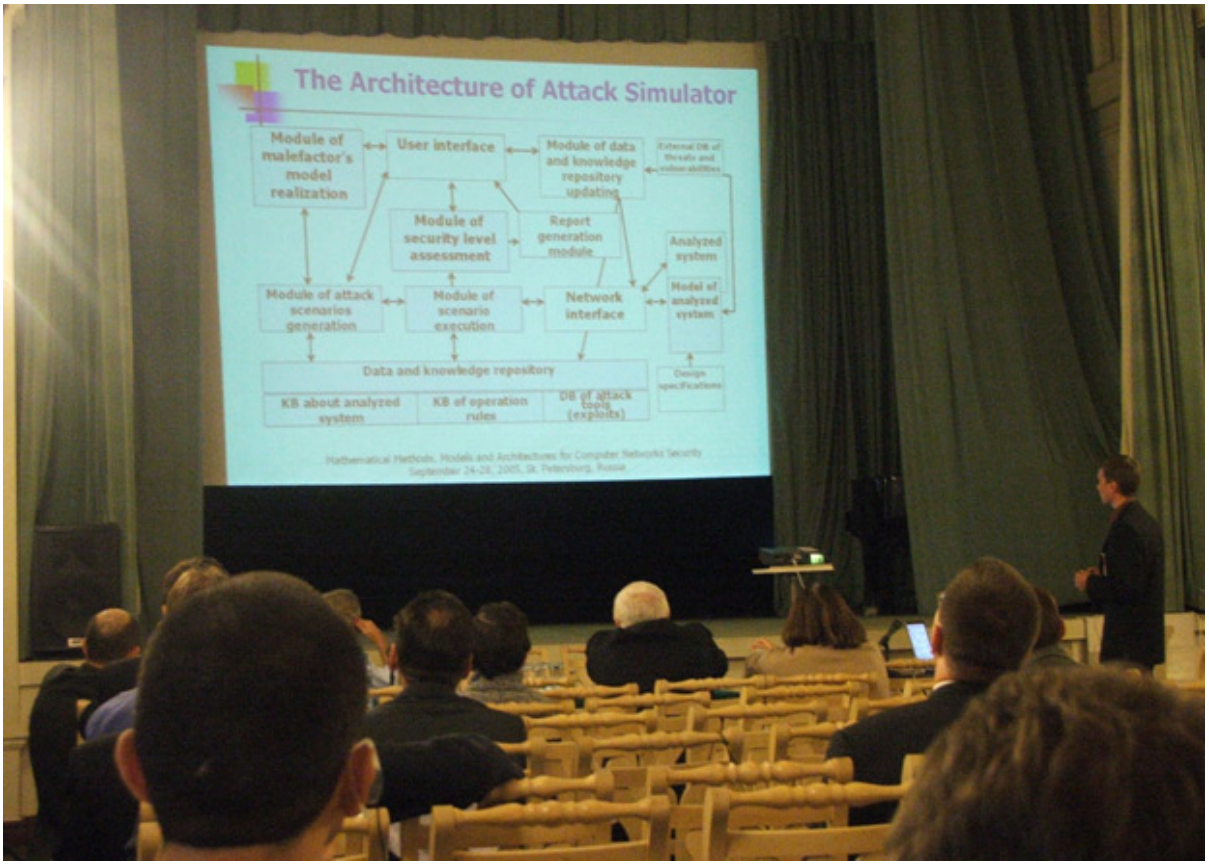


Рис. 3. В ходе доклада И. Котенко и М. Степашкина (СПИИРАН) «Анализ уязвимостей и измерение уровня защищенности на этапах проектирования и эксплуатации жизненного цикла компьютерных сетей».

В докладе представлены обобщенная модель атак, модели анализируемой системы и оценки уровня защищенности. На этапе проектирования используется модель анализируемой компьютерной сети, которая базируется на за-



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

данной спецификации компьютерной сети и реализуемой политике безопасности. На этапе эксплуатации исследуется реальная компьютерная сеть.

Результаты генерируемых атак позволяют определить уязвимости, построить трассы (графы) возможных атак, выявить «узкие места» в компьютерной сети, и вычислить различные метрики безопасности, которые могут быть использованы для оценки общего уровня защищенности компьютерной сети (системы), а также уровня защищенности ее компонентов. Полученные результаты обеспечивают также выработку обоснованных рекомендаций по устранению выявленных узких мест и усилению защищенности системы.

В докладе было приведено описание архитектуры и особенностей реализации разработанного программного прототипа и проведенных экспериментов.

*М. О. Калинин* (*Санкт-петербуржский Политехнический Университет, Россия*) представил доклад **«Обнаружение уязвимостей в конфигурациях операционной системы MS Windows»**, подготовленный совместно с *П. Д. Зегждой* и *Д. П. Зегждой*. В докладе рассмотрена методика обнаружения уязвимостей, применимая для проверки свойств безопасности конфигураций операционной системы MS Windows. Для обнаружения уязвимостей использовано представление механизмов управления доступом в виде автоматной модели. В докладе рассмотрено автоматизированное средство обнаружения уязвимостей в среде MS Windows, определяющее уязвимые параметры настройки, и продемонстрировано, как предложенная методика может быть применена для верификации механизмов защиты.

Сообщение *Д. В. Буттса*, *Р. Ф. Милза* и *Р. О. Болдуина* (*J.W.Butts, R.F.Mills, R.O.Baldwin, Технологический институт Военно-воздушных сил, США*) **«Разработка модели угроз со стороны внутреннего нарушителя, основанной на функциональной декомпозиции»** было посвящено разработке таксономии угроз со стороны внутренних пользователей и возможностям ее использования для обнаружения внутренних злоумышленников.

## 9. Секция «Обнаружение вторжений»

На секции было представлено четыре доклада и одно сообщение.

В докладе *А. Алхарби* и *Х. Имэй* (*A. Alharby, H. Imai, Институт индустриальных наук, Университет Токио, Япония*) **«Гибридная модель обнаружения вторжений, основанная на упорядоченных последовательностях»** рассмотрен подход к созданию гибридной системы обнаружения вторжения, основанный на анализе поведения, и предложен алгоритм, который может использоваться для генерации сигнатур атак и обнаружения аномального поведения. Алгоритм обеспечивает выявление порядка действий при реализации атаки, и свободен от ограничений алгоритмов, основанных на определении несоответствий или частот событий, которые реализуют статистический анализ данных об атаках на основе правил ассоциации или алгоритмов выделения частых эпизодов. Для исследования свойств алгоритма использовались записи сетевых сессий, извлеченные из широко применяемого для целей исследований набора DARPA-данных. Показано, что сложность разработанного алгоритма меньше, чем сложность известных подобных алгоритмов. Используя предложенный алгоритм для обработки транзакций известных атак, авторы определили, что он описывает атаки более точно, и может обнаружить эти атаки за ограниченное количество транзакций.



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Доклад *В. Городетского*, *О. Карсаева*, *В. Самойлова* и *А. Уланова* (*Санкт-Петербургский институт информатики и автоматизации РАН, Россия*) **«Корреляция асинхронных предупреждений в многоагентных системах обнаружения вторжений»**, который представил В. Самойлов, был посвящен рассмотрению задачи обнаружения вторжений на основе гетерогенных асинхронных данных. В докладе было подчеркнуто, что, хотя обнаружение вторжений является областью интенсивных исследований в течение, по крайней мере, последнего десятилетия, множество важных проблем и особенностей этой задачи не были глубоко исследованы.

Один из основных недостатков существующих подходов заключается в упрощенном представлении входных данных, используемых системой обнаружения вторжений. Действительно, наряду с разнообразием и разнородностью источников данных, которые должны приниматься во внимание, критическими являются и другие специфические особенности входных данных. Среди этих особенностей следует выделить темпоральный и асинхронный характер, высокую динамику. Эти факторы приводят к необходимости учитывать такой важный аспект как старение информации, вызванное тем, что потоки входных данных поступают на вход системы обнаружения вторжения с различными частотами и асинхронно.

Входная модель данных, рассмотренная в докладе, принимает во внимание вышеупомянутые факторы. Для такой модели входных данных системы обнаружения вторжений авторы предложили подход, названный гетерогенной корреляцией предупреждений. Главная идея подхода состоит в организации системы обнаружения вторжений в виде структурированного множества взаимодействующих классификаторов, обрабатывающих данные, полученные от различных источников. Первый уровень этой структуры составлен из классификаторов, работающих с отдельными специфическими источниками данных. Каждый из них обучается для обнаружения атак установленного класса (в разработанном программном прототипе рассматриваются классы атак DoS (отказа в обслуживании), Probe (разведывательные действия) и U2R (получение пользователем прав администратора)). Каждый из таких специализированных классификаторов генерирует решения двух типов: «Предупреждение» (в отношении специфического класса атак) или «Норма». Особенность операций классификаторов состоит в том, что они производят решения в различные моменты времени. Эти решения асинхронно достигают классификаторов второго уровня, ответственных за корреляцию предупреждений для атак конкретного класса и обученных для обнаружения атак того же самого класса. В свою очередь, результаты корреляции предупреждений, произведенных специализированными классификаторами второго уровня, асинхронно отправляются на верхний уровень. Классификатор верхнего уровня решает задачу обнаружения вторжений: он комбинирует гетерогенные предупреждения специализированных классификаторов корреляции и комбинирует их, генерируя решение в терминах специфического класса атак. Для осуществления описанного подхода должны быть решены две теоретических проблемы: разработка модели старения данных и развитие частных методов обучения классификаторов для принятия решений, основанных на асинхронном потоке входных данных.

Решения, предложенные авторами, были реализованы в разработанном прототипе системы обнаружения вторжений. В докладе представлена архитектура прототипа и результаты некоторых экспериментов.



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

*В. Сердюк* (*Российский Государственный Технологический Университет, Россия*) представил доклад **«Модель обнаружения и предотвращения вторжений в компьютерных сетях на основе поведения»**. В докладе описана модель обнаружения и предотвращения вторжений, основанная на использовании машин состояний и формальных грамматик для обнаружения и предотвращения аномального сетевого трафика, связанного с информационными атаками. Предложенная модель позволяет обнаруживать компьютерные атаки посредством моделирования нормального сетевого трафика. Параметры такого нормального сетевого трафика представляются в терминах формальной грамматики. Каждый пакет данных, который нарушает эти параметры, рассматривается как часть вторжения и блокируется сетевыми фильтрами.

Описанный подход был проиллюстрирован на основе примера обнаружения атак на Web-серверы. Разработанная модель была реализована в системе обнаружения и предотвращения вторжения «Форпост».

В докладе *О. Тараканова*, *С. Квачева* и *А. Сухорукова* (*Санкт-Петербургский институт информатики и автоматизации РАН, Россия*) **«Формальная иммунная сеть и ее реализация для обнаружения вторжений в реальном времени»** была предложена модель иммунной сети, которая названа «формальной иммунной сетью». В работе использовано разложение сингулярных значений набора данных обучения и введен ряд понятий, например, входной вектор назван антигеном или формальным протеином, а один из сингулярных векторов (например, правый) — антителом. Остальная часть доклада касалась использования идей разложения сингулярных значений для формирования подхода к обучению и Евклидова расстояния как основы для распознавания образов. Авторы протестировали предложенный подход на широко используемом тестовом наборе данных KDD Cup. Результаты продемонстрировали высокое качество распознавания на основе разложения сингулярных значений. Также была рассмотрена аппаратная реализация предложенного подхода, которая названа иммуночипом.

*У. Пейер* совместно с *П. Теуфлом*, *Ш. Краксбергером* и *М. Ламбергером* (*U. Payer, P. Teufl, S. Kraxberger, M. Lamberger, Институт информатики и коммуникаций, Австрия*) представил сообщение **«Методы обработки массивных данных для обнаружения полиморфного кода»**. Авторы исследовали несколько различных статистических методов с целью обнаружения полиморфного кода («вирусов», «червей»). Основная цель работы заключалась в выборе среди различных методов получения данных (data mining), таких как нейронные сети, самоорганизующиеся карты (Self Organizing Maps), Марковские модели и генетические алгоритмы, наиболее перспективных кандидатов для автоматического обучения обнаружению полиморфного кода. Проведенные исследование показали, что использование нейронных сетей дает наиболее приемлемые результаты в обнаружении неизвестного полиморфного кода. С другой стороны, применение Марковских моделей имеет преимущество, связанное с возможностью хранения информации о последовательности данных.

## 10. Заключение

В целом, в соответствии с единодушным мнением участников семинара (рис. 4), он получился достаточно интересным и его научный уровень соответствовал мировым стандартам. По единодушному мнению участников семинара было решено продолжить его проведение в будущем.



Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Важной особенностью международного семинара, проведенного в 2005 году, является, с одной стороны, акцентирование внимания на математических аспектах информационной безопасности, а с другой, внимание уделялось и практическим решениям, которые могут найти широкое применение для защиты современных компьютерных сетей. В числе рассматриваемых вопросов — математические модели, архитектуры и протоколы для защиты информационных ресурсов в компьютерных сетях; механизмы аутентификации, авторизации и разграничения доступа; анализ информационных потоков и скрытых каналов; модели и механизмы управления политиками безопасности; анализ уязвимостей и обнаружение вторжений в компьютерных сетях и другие.

Рис. 4. Участники семинара.

Информацию по данному семинару можно найти на Web-странице <http://space.iias.spb.su/mmm-acns05/>.

## Литература


1. Computer Network Security. Lecture Notes in Computer Science / Gorodetski V., Kotenko I., Skormin V. (eds.). New York: Springer-Verlag, 2005. Vol. 3685. 480 p.