УДК 004.056

КОТЕНКО И.В., САЕНКО И.Б., ЮСУПОВ Р.М.

АНАЛИТИЧЕСКИЙ ОБЗОР ДОКЛАДОВ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ «МАТЕМАТИЧЕСКИЕ МОДЕЛИ, МЕТОДЫ И АРХИТЕКТУРЫ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ» (MMM-ACNS-2010)

Котенко И.В., Саенко И.Б., Юсупов Р.М. **Аналитический обзор докладов Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010).**

Аннотация. В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010), проходившей в Санкт-Петербурге 8–10 сентября 2010 г. С докладами выступили такие известные в мире ученые, как Э. Дебар, Д. Гольманн, Г. Моррисетт, Б. Пренель, Р. Сандху и А. Сабельфельд. На секциях конференции были рассмотрены актуальные вопросы, связанные с моделированием безопасности и скрытых каналов, политиками безопасности и формальным анализом свойств безопасности, аутентификацией, авторизацией, управлением доступом и криптографией с открытым ключом, обнаружением вторжений и вредоносных программ, безопасностью многоагентных систем и защитой программного обеспечения, адаптивной защитой информации, живучестью компьютерных сетей и виртуализацией.

Ключевые слова: компьютерные сети, защита информации, математические модели и методы, архитектура системы.

Kotenko I.V., Saenko I.B., Yusupov R.M. **Analytical review of talks on the International Conference «Mathematical Methods, Models and Architectures for Computer Network Security» (MMM-ACNS-2010).**

Abstract. The paper provides an analytical review of talks by leading foreign and domestic experts in the security of computer networks, presented at the International Conference «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-2010), held in St. Petersburg from 8 to 10 September, 2010. World-known scientists, such as E. Debar, D. Golmann, G. Morrisett, B. Prenel, R. Sandhu, and A. Sabelfeld, made invited talks. On sections of the conference there were discussed topical issues related to the modeling of security and covert channels, security policies and formal analysis of security properties, authentication, authorization, access control and public key cryptography, intrusion detection, malicious software, security of multi-agent systems and software protection, adaptive information security, survivability of computer networks and virtualization.

Keywords: computer networks, information security, mathematical models and methods, system architecture.

1. Введение. Пятая международная конференция «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010), проведенная с 8 по 10 сентября 2010 г. в Санкт-

Петербурге, стала одним из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей.

Предыдущие международные конференции MMM-ACNS, проведенные в 2001, 2003, 2005 и 2007 гг., продемонстрировали острый интерес исследовательских организаций и ученых всего мира к тематике использования формальных методов, моделей и разработке перспективных архитектурных решений для обеспечения безопасности информационных ресурсов в компьютерных сетях. Опыт их организации показал, что проведение подобной конференции в Санкт-Петербурге стимулирует разработку новых результатов и плодотворные обмены мнениями между различными школами (зарубежными и российскими) в области защиты информации, облегчает распространение новых идей и продвигает дух сотрудничества между исследователями в международном масштабе. Поэтому решено регулярно проводить эту конференцию.

Конференция была организована СПИИРАН и Университетом Бингхэмтона — государственным университетом штата Нью-Йорк (США). Финансовую поддержку конференции обеспечили Европейское управление воздушно-космических исследований и разработок США, Управление научных исследований ВМС США и Российский фонд фундаментальных исследований. Международный программный комитет, включавший известных специалистов по теме конференции из 18 стран Европы, Австралии и Америки, выступал гарантом высокого научного уровня конференции.

Сопредседателями конференции были чл.-корр. РАН, проф. Р. М. Юсупов (директор СПИИРАН, Россия) и Р. Л. Герклотц (Управление научных исследований ВВС США). Сопредседатели программного комитета — проф. И. В. Котенко (СПИИРАН, Россия) и профессор В. А. Скормин (Бингэмптоновский Университет, США) (рис. 1).

На конференции было зарегистрировано 67 участников (рис. 2, 3). Статистические данные о принадлежности участников к различным областям деятельности таковы: число участников из университетской среды — 29; из научных организаций — 26; из коммерческих организаций — 6; из государственных учреждений — 6.

Рис. 1. Сопредседатели конференции и программного комитета:
Р. Юсупов (Россия), В. Скормин (США),
Р. Герклотц (США) и И. Котенко (Россия).

Рис. 2. Участники конференции.

Рис. 3. Участники конференции: Д. Голлман (Германия),
И. Котенко (Россия) и Б. Пренель (Бельгия).

2. Приглашенные докладчики. Для участия в конференции были персонально приглашены шесть известных в мире специалистов в области защиты информации. В частности, с докладами выступили такие известные ученые, как Э. Дебар (Институт Телеком, Франция), Д. Гольманн (Технический университет Гамбурга, Германия), Г. Моррисетт (Гарвардский университет, США), Б. Пренель (Католический университет, Бельгия), Р. Сандху (Техасский университет Сан-Антонио, США) и А. Сабельфельд (Чалмерский университет, Швеция).

Представим темы докладов приглашенных ученые подробнее.

Э. Дебар *(Франция)* выступил с докладом на тему *«Зависимости сервисов при обеспечении безопасности информационных систем»* (рис. 4). Автор представил модель зависимостей информационных услуг, разработанную с целью обеспечения администраторов безопасности системой поддержки принятия количественных решений для развертывания и управления политиками безопасности. Данная система позволяет определять наиболее критические места в политиках безопасности и сокращает в целом расходы на управление безопасностью информационных систем.

Автор подробно рассмотрел положение дел в области моделирования зависимостей услуг, требования, предъявляемые к моделированию зависимостей, и обосновал необходимость разработки представления сервисных зависимостей, которое включает информацию не только об их размере, но и о привилегиях.

Рис. 4. Выступление профессора Э. Дебара (Франция).

Была предложена новая формальная модель зависимостей. Вначале автор рассмотрел простую модель услуг. Затем представил ее расширение с помощью понятия привилегии, а также механизмы разделения привилегий, задаваемые предикатами *Credential* и *Trust*. С использованием языка анализа и проектирования AADL (*Architecture Analysis and Design Language*) были показаны различные варианты представления зависимостей. Автор ввел следующие характеристики зависимостей: тип (*type*), режим (*mode*) и влияние (*impact*). Возможными типами зависимостей являются: «со стороны сервиса» (*service-side*), «со стороны пользователя» (*user-side*) и прокси (*proxy*). Сервис имеет четыре операционных режима: запуск (*start mode*), ожидание запроса (*idle mode*), обработка запроса (*request mode*) и останов (*stop mode*). Влияние зависимостей отображается последовательностями состояний деградации ведущего сервиса, которые изменяют доступ к данным с помощью зависимого сервиса.

В заключение своего выступления докладчик остановился на вопросах реализации предложенной модели зависимостей услуг и ее применения для оценки последствий распространения атак в сети.

В докладе ***Д. Гольманна*** *(Германия)* «*Безопасные приложения без безопасных инфраструктур*» были рассмотрены примеры атак прикладного уровня, против которых нельзя обеспечить защиту на уровне инфраструктуры Интернета (рис. 5). К числу таких атак, в частности, автор относит: атаки «SQL-инъекции», межсайтовый скриптинг

(*Cross-Site Scripting*), межсайтовую подделку запроса (*Cross-Site Request Forgery*), атаки «отравления кэша» (*Cache Poisoning*), атаки «связывания DNS» (*DNS Rebinding*) и атаки «человека в середине» (*Man-in-the-Middle*). Последний вид атаки основывается на применении протокола SSL/TLS, позволяющего установить защищенное туннельное соединение между клиентом и веб-сервером.

Рис. 5. Выступление профессора Д. Голлмана (Германия).

Докладчик показал, что развертывание защищенной инфраструктуры не является достаточным условием для защиты критически важных приложений. Приложения можно защищать, не полагаясь на безопасность сервисов, предоставляемых инфраструктурой. Следовательно, развертывание защищенной инфраструктуры не является необходимым условием для защиты критически важных приложений. В то же время это является единственно необходимым условием обеспечения вычислительной целостности (*execution integrity*) самой инфраструктуры, а также ее доступности. Доступность является первичным свойством, которое требуется от коммуникационной инфраструктуры. Другие сервисы безопасности, такие, как конфиденциальность, целостность и аутентичность, эта инфраструктура может не обеспечивать.

Докладчик сделал вывод, что в последнее время акцент в мониторинге безопасности все больше смещается от защищенных операционных систем (1980-е гг.) и веб-браузеров (1990-е гг.) на прикладные

приложения. В этой связи достаточно актуальна задача создания безопасных приложений «без-безопасных» инфраструктур. Ответственность за обеспечение безопасности в этом случае все в большей степени возлагается на разработчиков данных приложений и конечных пользователей. Однако специалисты указанных категорий редко хорошо подготовлены для решения данной задачи.

Доклад ***Г. Моррисетта*** *(США)* «*Интеграция типов и спецификаций для разработки безопасного программного обеспечения*» был посвящен исследованию взаимосвязи безопасности системного программного обеспечения и ошибками программирования (рис. 6). Многие простейшие виды ошибок, например, переполнение буфера, могут быть предотвращены при использовании типизированных языков вместо традиционных, таких как C и C++. Языки Java, Scheme и ML являются примерами языков, в которых по крайней мере принципиально не может иметь место переполнение буфера. Однако остаются угрозы, связанные с использованием недостатков программирования на более высоком уровне, например, атаки класса «SQL-инъекции». Таким образом, следующее поколение языков программирования должно основываться на системах типизации, которые могут выражать и выполнять политики безопасности конкретных приложений.

Рис. 6. Выступление профессора Г. Моррисетта (США).

Тем не менее существующие типизированные языки обладают рядом недостатков. Например, к ним относится высокая стоимость переписывания программ в новых языках (система Windows включает более чем 60 млн строк кода). Другие недостатки требуют для своего устранения новых фундаментальных исследований в области языков системного программирования.

В основу языков системного программирования следующего поколения автор предлагает положить применение так называемых «утонченных» (*refinement*) типов данных, т.е. типов, имеющих форму

$$«\{x : T \mid P\,(x)\}»,$$

где T — тип, а $P\,(x)$ — предикат над значениями типа T.

Однако основная проблема использования утонченных типов данных заключается в нахождении способов проверки типов.

Автор приводит пример системы Coq, относящейся к классу «помощников доказательств» (*Proof Assistants*), которая обеспечивает мощный унифицированный способ написания следующих алгоритмов:

а) программ;

б) спецификаций и моделей, охватывающих желаемые свойства программ, от простой типизации и свойств безопасности вплоть до полной корректности;

в) формальных машинно-проверяемых доказательств того, что программа соответствует своей спецификации.

В заключение был представлен пример разработанного языка Ynot, являющегося расширением Coq, который базируется на теории типов Хоара (*Hoare Type Theory — HTT*), и приведены результаты построения на его основе верифицированной программной системы.

Докладчик завершил свое выступление утверждением, что язык программирования, встроенный в Coq, является высокоуровневым, подобно языку ML. Для многих приложений это является идеальным случаем. Однако в то же время для многих задач системного программирования, например программирования гипервизоров или драйверов устройств, он является языком слишком высокого уровня. Таким образом, необходима разработка низкоуровневой среды программирования, которая может эффективно заменить язык C.

В докладе ***Б. Пренеля*** *(Бельгия) «Криптография для безопасности сетей: неудачи, успехи и проблемы»* были рассмотрены современ-

ные криптографические алгоритмы, используемые для обеспечения безопасности вычислительных сетей (рис. 7). В докладе обсуждалось современное состояние широкого круга криптографических алгоритмов, применяемых в сетевых приложениях, и был сделан вывод, что очень часто проблемы безопасности сетей идентифицируются с данными алгоритмами и их реализациями.

Рис. 7. Выступление профессора Б. Пренеля (Бельгия).

Относительно алгоритмов симметричного шифрования автор рассмотрел опыт разработки и применения следующих программных продуктов:

— блочных шифров (DES, AES);

— потоковых шифров (LFSR, RC4, MIGI, SNOW, HC-128, Rabbit, Salsa20/12, Sosemanuk, Grain, Mickeyv2, Trivium);

— алгоритмов кодов аутентификации сообщений (CBC-MAC, CMAC, HMAC-MD4, HMAC-MD5, HMAC-SHA-1, UMAC);

— хэш-функций (MD4, MD5, SHA, RIPEMID-160);

— режимов проверки подлинности шифрования (IAPM, XCBC, XECB, OCB, GCM).

Среди алгоритмов асимметричного шифрования был рассмотрен алгоритм RSA и различные способы его применения (GNFS,

PRCS#1v.1.5, OAEP, RSA-KEM, RSA-PSS), а также алгоритмы шифрования, основанные на эллиптических кривых (ECC).

Рассмотренные алгоритмы были проанализированы на их устойчивость относительно программных атак. Результаты проведенного анализа позволили автору сформулировать следующие выводы. Алгоритм AES стал *де-факто* в последнее десятилетие стандартом для шифрования данных в компьютерных сетях. HMAC-MD5 и HMAC-SHA-1 являются наиболее общими алгоритмами, используемыми для проверки подлинности сообщений. Однако эти режимы требуют перепроектирования протоколов. По этой причине HMAC усиленно замещается CBC-MAC, основанным на AES или полиномиальной хэш-функции. Последняя работает быстрее, но менее надежна. Беспроводные сети пока используют блочные или потоковые шифры. Сети 3G предпочитают аутентификацию данных, основанную на MAC-алгоритмах.

Для алгоритмов публичных ключей эволюция идет медленнее. Протоколы, основанные на RSA и алгоритме Дифи–Хэлмана (*Diffie–Hellman*) требуют больших вычислительных затрат по сравнению с ECC, в частности, для компьютеров с низким энергопотреблением. Определяющим фактором в этом развитии является относительно меньший размер ключа в алгоритмах класса ECC.

Важнейшей областью исследований становятся атаки по скрытым каналам (*side channel attacks*), которые в настоящее время оказывают сильное воздействие на аппаратную и программную реализацию алгоритмов. Следует ожидать, что в будущем некоторые алгоритмы будут перепроектированы с целью значительного облегчения их реализации в защищенном виде.

В дополнение к новым видам атак разработаны новые доказательства и модели безопасности, которые усиливают понимание в таких областях, как режимы конфиденциальности и аутентификация шифрования, а также использование алгоритмов RSA и ECC. Это вызывает необходимость появления эффективных и безопасных процедур для обновления и исправления криптографических алгоритмов. Тем не менее, замещение криптоалгоритмов пока требует многих лет.

Доклад ***Р. Сандху*** *(США)* «*Основанные на группах модели для безопасного и гибкого совместного использования информации*» был посвящен изложению нового метода разграничения доступа, который

назван автором «основанным на группах» (*group-centric*) (рис. 8). Данный способ разграничения доступа предназначен для гибкого и учитывающего специальные шаблоны разделения информации.

Поиск эффективных решений для классической проблемы безопасности, связанной с разделением информации и сохранением контроля (принцип «разделяй, но защищай») продолжается. Там, где шаблоны разделения являются хорошо определенными и изменяются медленно, целесообразно применять традиционные модели контроля доступа на основе решеток, на основе ролей и атрибутов, а также дискреционную авторизацию для дальнейшего точного управления по мере необходимости. Использование стандартизованных языков разметки прав (*rights markup languages*), например XACML, обеспечивает значительную гибкость контроля конкретных информационных объектов с учетом уже определенных атрибутов пользователей, субъектов и объектов. Однако при этом порождаются проблемы, схожие с теми, которые появляются при возврате от ролевого контроля доступа к дискреционному.

Рис. 8. Выступление профессора Р. Сандху (США).

Недавно авторами была разработана модель ориентированного на группы разделения информации (*g-SIS*). Она основывается на использовании гибких и удобных специальных шаблонов и, как предполага-

ется, должна стать четвертым широко распространенным способом контроля доступа после дискреционного (DAC), мандатного (MAC или LBAC) и ролевого (RBAC). В данной модели пользователи и информация вместе входят в группу для содействия ее разделению. Пользователи получают доступ в силу своего членства в группе. Образование группы как единицы для безопасного разделения информации имеет те же преимущества, какие есть у использования ролей по сравнению с распределением полномочий по отдельным пользователям. Группы могут быть, с одной стороны, изолированными (*isolated*) или связанными (*coupled*), а с другой — дифференцированными (*differentiated*) или недифференцированными (*undifferentiated*). В изолированной группе членство не оказывает никакого влияния на то, что пользователь может делать в другой группе, в то время как в связанных группах такое влияние может иметь место. В недифференцированной группе пользовательские авторизации не зависят от атрибутов, а только от членства в группе. Комбинирование этими двумя характеристиками групп дает четыре возможных класса g-SIS-моделей. На низшем уровне находится класс изолированных и недифференцированных групп, на верхнем уровне — связанных и дифференцированных. Остальные два находятся на среднем уровне и не пересекаются друг с другом.

Автор остановился в докладе на подробном рассмотрении модели связанных и недифференцированных групп и сравнил ее с такими классическими моделями доступа, как LBAC, доменного и типового усиления (*Domain and Type Enforcement*) и RBAC. Он показал, что предложенная модель может отображать такие же политики, и в то же время позволять удобно управлять динамическими сценариями разделения информации. Докладчик кратко охарактеризовал модель изолированных групп, обсудил возможные межгрупповые связи в модели связанных групп и продемонстрировал гибкость модели связанных групп по сравнению с моделями LBAC и RBAC.

Доклад ***А. Сабельфельда*** *(Швеция)* «*Безопасность Веб-приложений: от фундаментальных проблем к практическим решениям*» был посвящен подходу к защите веб-приложений, основанному на отслеживании информационных потоков (рис. 9).

В настоящее время вопросы безопасности веб-приложений охватывают не только настольные приложения, осуществляющие распро-

странение конфиденциальной информации между веб-сервером и веб-клиентом и требующие защиты сервера, клиента и связи между ними, но также социальные сети. Анализ первой десятки наиболее популярных атак в 2010 г. показывает, что практически все они основаны на реализации нежелательных информационных потоков. Так, атака «инъекции кода» (первое место в списке) осуществляет нежелательный поток данных на сервер-интерпретатор, а атака XSS (второе место) — поток в скрипте клиента. Это выдвигает на первое место ряд фундаментальных задач:

— в области политик безопасности — внутреннюю децентрализацию Web и потребность в политиках внутреннего недоверия,

— в области реализации — разработку языков динамического веб-программирования.

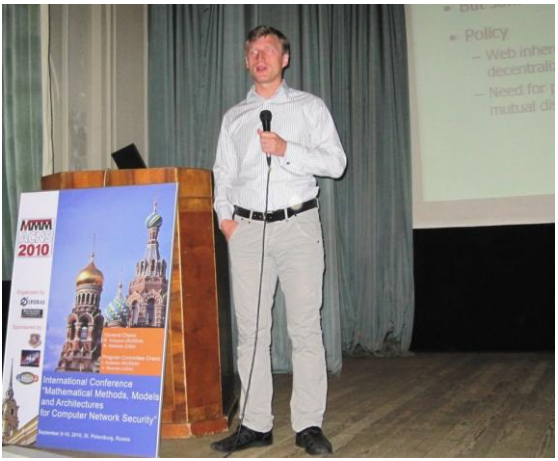

Рис. 9. Выступление профессора А. Сабельфельда (Швеция).

Корнем решения данных задач, по мнению автора, является контроль информационных потоков. Управление информационными потоками в 1970–1980-е гг. изучалось в военных системах, в 1990-е гг. возродилось в мобильных кодах, а в 2000-х гг. стало базовой темой для основанной на языках (*language-based*) безопасности в веб-приложениях. На примере модели LBAC автор рассмотрел различные

сценарии контроля информационных потоков, сущность внутреннего недоверия и проблемы медленного закрытого потока. В завершение доклада автор остановился на реализационных аспектах контроля информационных потоков в интересах обеспечения безопасности веб-приложений.

3. Секционные доклады. В ходе подготовки к конференции получено 54 доклада из 19 стран. Наибольшее число статей поступило из России, США, Франции и Испании. Каждая из статей была тщательно проанализирована тремя-четырьмя рецензентами. В результате международным программным комитетом было отобрано 22 лучших секционных доклада, представляющих 10 стран: Россию, США, Австрию, Польшу, Канаду, Францию, Германию, Норвегию, Испанию и Турцию. Из них было выбрано 16 докладов для полных презентаций и 6 — для коротких.

Программа конференции включала работу шести секций:

1) «Моделирование безопасности и скрытые каналы»;

2) «Политики безопасности и формальный анализ свойств безопасности»;

3) «Аутентификация, авторизация, управление доступом и криптография с открытым ключом»;

4) «Обнаружение вторжений и вредоносных программ»;

5) «Безопасность многоагентных систем и защита программного обеспечения»;

6) «Адаптивная защита информации, живучесть компьютерных сетей и виртуализация».

Секция «Моделирование безопасности и скрытые каналы» была посвящена рассмотрению общих моделей безопасности и скрытых каналов.

В докладе ***Л. Питр-Камбаседеса*** *(Франция)* были представлены теоретические основы динамического моделирования атак и защиты от них на основе булевой логики скрытых Марковских процессов. Данный формализм, успешно применяющийся в проектировании высоконадежных систем, в последнее время успешно адаптируется для использования в области моделирования безопасности. Он образует привлекательный компромисс между читабельностью, мощностью моделирования, масштабируемостью и возможностями количественной оценки. Автор развил и довел до завершения теоретические основы

такой адаптации и представил результаты их распространения на аспекты безопасности. В частности, в данных теоретических положениях полностью интегрированы модели обнаружения и отражения атак. Релевантность данного подхода проиллюстрирована примерами применения и количественной оценки.

В. Санкаранарайанан *(США)* представил теоретико-игровую модель для обнаружения кооперации пользователей в компьютерных системах и регулирования качества услуг. Автор предлагает изменить методологию проектирования компьютерных систем за счет обеспечения кооперации пользователей с механизмами обеспечения безопасности на основе применения подходящей обратной связи. Пользователям предлагаются стимулы в форме увеличения качества услуг (QoS), выраженного в терминах производительности прикладного и системного уровней. Мотивы пользователей и их действия моделируются на основе теории игр, используя класс обобщенных дифференциальных игр преследования-убегания.

В докладе ***Л. Домнитсера*** *(США)* рассмотрена прогнозирующая модель для побочных кэш-каналов в многослойных и многопоточных микропроцессорах, на которой исследовались типовые сценарии возможных атак. Недавние исследования показали возможность использования разделенного кэша как побочного канала для извлечения закрытого ключа из вычислительно безопасного криптографического приложения. Побочный кэш-канал несовершенен в том смысле, что способность атакующего по обнаружению утечки критических данных ограничена временными рамками. Более того, некоторые обнаруженные утечки оказываются связанными с некритическими данными. Таким образом, представляется достаточно затруднительным оценить степень уязвимости, задаваемую несовершенной природой побочного канала. Для этих целей предлагается математическая модель для оценки ожидаемой утечки в кэше как функции параметров кэша и поведения атакуемого приложения. Чтобы проверить достоверность модели, было осуществлено имитационное моделирование и количественное оценивание этих параметров для типовых сценариев атак. Авторами было показано, что предложенная модель достаточно точно оценивает утечки побочных каналов для случаев шифрования и дешифрования на основе алгоритмов AES и Blowfish на множестве различных кэш-конфигураций.

Доклад ***А. Грушо*** *(Россия)* был посвящен обсуждению проблем моделирования при анализе скрытых каналов и возможности их решения на основе вероятностных моделей. Автор показал, каким образом проблема обнаружения скрытого канала зависит от корректности выбора вероятностной модели. Была найдена зависимость суждений о невидимости скрытого канала от ограничений вероятностной модели основного канала.

На *секции «Политики безопасности и формальный анализ свойств безопасности»* были представлены доклады ***Р. Хоури*** *(Канада),* ***Ш.-К. Чина*** *(США)* и ***Д. Унала*** *(Турция)*.

В докладе ***Р. Хоури*** *(Канада)* рассмотрена методика использования отношений эквивалентности для корректирующего применения политик безопасности. Автор представил основы оперативного (в реальном времени) исполнения политик безопасности и показал, при каких условиях можно использовать отношения эквивалентности, чтобы обеспечивать успешное выполнение политики безопасности. На конкретных примерах отношений эквивалентности, применяемых к значимым свойствам безопасности, был исследован вопрос, как априорные знания о поведении целевой программы увеличивают эффективность мониторинга безопасности.

В докладе ***Ш.-К. Чина*** *(США)* предложены формальные средства логики управления доступом (*Access-Control Logic*), основанной на многоагентной пропозициональной модальной логике. Доказана корректность предложенной логики и ее расширений и осуществлена ее реализация в системе автоматической идентификации и уничтожения воздушных целей. Докладчик показал, что для реализации критических военных операций используемые интеллектуальные автономные системы должны функционировать, обеспечивая поддержку намерений командира и гарантируя целостность самой операции. Автор показал, что политика, выраженная с помощью логики управления доступом, может играть роль связующего моста между командиром и исполнителем его решений. Используя логику управления доступом на основе многоагентной пропозициональной модальной логики, можно эффективно описать политику и проверить принимаемые решения по доступу, и автор продемонстрировал это на примерах.

В докладе ***Д. Унала*** *(Турция)* представлен подход к проверке на модели (*model checking*) спецификаций политики безопасности, бази-

рующейся на местоположении и мобильности в исчислении событий во внешнем окружении. Верификация безопасности для мобильных сетей требует спецификации и верификации политик безопасности в многодоменной среде. Одной из проблем для такой среды является спецификация и верификация политик безопасности для мобильных пользователей. Формальные методы создания систем, как известно, гарантируют, что построение системы основывается на точном воспроизведении ее спецификации. Формальные методы для спецификации и верификации политик безопасности гарантируют исполнение политики безопасности элементами сети в заданной конфигурации. Автор представил метод и инструментарий проверки на модели, предназначенные для формальной спецификации и верификации местоположения и мобильности политик безопасности для мобильных сетей. Формальными языками, используемыми для спецификации, являются логика предикатов и исчисление событий (*Ambient Calculus*). Представленное инструментальное средство способно осуществлять проверку пространственных спецификаций для правил политики безопасности, а для проверки темпоральных моделей используется верификатор NuSMV.

Доклады, заслушанные на секции *«Аутентификация, авторизация, управление доступом и криптография с открытым ключом»*, посвящены перспективным аспектам управления доступом и криптографии.

Г. Бенсон *(США)* рассмотрел формальный подход к управлению сертификатами для значимых транзакций на основе предложенного исчисления управления доступом.

К. Саша *(Польша)* представил основанный на ролях язык управления доверием RTT как средство спецификации политик безопасности и использования цепочек сертификатов для защиты конфиденциальных ресурсов от несанкционированного доступа. Автор привел формальное описание синтаксиса и семантики языка и определил мандатные графы RTT и мандатные цепи как средства получения защищенных ответов на запросы. Для построения мандатных цепей был предложены алгоритмы прямого и обратного поиска.

Доклад ***Н. Молдовяна*** *(Россия)* был посвящен решению новой вычислительно сложной задачи по некоммутативным конечным группам, связанной с построением протокола соглашения открытого ключа

и алгоритмов для открытого и коммутативного шифрования. Для реализации этих протоколов и алгоритмов созданы и исследованы как примитивы конечные некоммутативные группы четырехмерных векторов на основном поле, базирующиеся на предложенной сложной задаче.

И. Саенко (*Россия*) рассмотрел метод генетической оптимизации схем разграничения доступом в виртуальных локальных сетях, основанный на полихромосомном представлении промежуточных точек. Автор представил формальную постановку задачи разграничения доступа к ресурсам, размещенным в виртуальной локальной вычислительной сети, в которой определил исходные данные, переменные, ограничения и целевую функцию, определяющую меру отклонения реальной схемы разграничения доступа от требуемой. Целесообразность использования генетических алгоритмов для оптимизации схемы разграничения доступа обусловлена нелинейностью, дискретностью и высокой размерностью целевой функции и ограничений. Полихромосомное представление промежуточных точек позволило значительно повысить сходимость метода. Однако этот фактор потребовал поиска и реализации отдельных оригинальных решений в генетическом алгоритме.

На *секции «Обнаружение вторжений и вредоносного программного обеспечения»* были заслушаны доклады ***Х. Моралеса*** (*США*), ***П. Теуфла*** (*Австрия*), ***Я. Маркова*** (*Россия*) *и* ***С. Петровича*** (*Норвегия*).

В докладе ***Х. Моралеса*** (*США*) была рассмотрена технология обнаружения бот-процессов, основанная на использовании определенных пользователем множеств симптомов, свойственных известным примерам ботов. Предложенный метод обнаружения бот-процессов основывается на следующих симптомах:

— попытках установления TCP-соединения,
— деятельности сервера DNS,
— цифровых подписях,
— неавторизованной подделке,
— сокрытии процесса.

Симптомы разделяются на множества и поступают на вход классификатора, генерирующего частные модели обнаружения. Эти модели позже интегрируются для доказательства точности обнаружения.

В докладе ***П. Теуфла*** (*Австрия*) для анализа вредоносного программного обеспечения предложено использовать методы обработки ограниченного естественного языка. Обработка естественного языка в комбинации с машинным обучением играет важную роль в области автоматического анализа текста. В то же время все вредоносные программы основываются на некотором виде машинного языка — от ассемблерного кода, вызывающего переполнение буфера, до высокоуровневых языков, таких, как JavaScript, используемый в веб-атаках. Следовательно, к областям анализа вредоносных программ могут быть применены хорошо известные процессы анализа естественного языка. Автор представил архитектуру системы анализа вредоносных программ, выделил отдельные методы обработки естественного языка и адаптировал их для процесса данного анализа.

Я. Марков *(Россия)* представил архитектуру системы интеллектуального обнаружения вторжений, основанную на применении методов выравнивания последовательностей. Алгоритмы выравнивания последовательностей используются в биоинформатике для обнаружения сходства в различных последовательностях генов. Автор рассмотрел два метода их использования:

— первый предназначен для обнаружения мутации атаки,

— второй применим для обнаружения аномалий.

Автор показал, какие алгоритмы выравнивания последовательностей могут быть использованы в этих методах, и продемонстрировал эффективность этих методов на практике.

С. Петрович (*Норвегия*) сравнил различные методы выделения признаков для задачи обнаружения вторжений. Выделение признаков — важная предварительная фаза в обнаружении атак. Достижение редукции числа релевантных признаков трафика без негативных последствий для точности классификации — та цель, которая сильно влияет на общую эффективность системы обнаружения вторжений. Основная задача здесь — выбор соответствующих методов выделения признаков, которые могут точно определять релевантность признаков и их избыточность. Автор предложил две новые меры выделения признаков, применимые в задачах обнаружения вторжений:

1) меру корреляции выделения признаков,

2) меру минимальной избыточности с максимальной релевантностью.

Эти меры были проверены на различных ранее известных автоматических алгоритмах выделения признаков, в частности, на деревьях классификации и регрессии. Как показали экспериментальные результаты, предложенный метод общего выделения признаков для обнаружения вторжений превосходит по производительности все существующие подходы, так как обеспечивает удаление более чем 30 % выделенных признаков из оригинального набора данных, сохраняя или даже улучшая точность классификации.

На *секции «Безопасность многоагентных систем и защита программного обеспечения»* особого внимания заслуживают доклады, сделанные ***А. Манна*** (*Испания*), ***Ш. Краксбергером*** *(Австрия)* и ***В. Десницким*** *(Россия).*

В докладе ***А. Манна*** (*Испания)* предложен подход к решению проблемы обнаружения вредоносных хостов, основанный на использовании «доверенных вычислительных модулей» (*Trusted Computing Module*). Результатом выполненной автором работы является библиотека, встроенная в платформу JADE (*Java Agent DEvelopment framework*), которая обеспечивает выполнение безопасной миграции агентов и называется SecMiLiA (*Secure Migration Library for Agents*). Эта библиотека обеспечивает дружественное использование технологии доверенных вычислений для агентов, созданных разработчиками системы.

В докладе ***Ш. Краксбергера*** *(Австрия)* рассмотрена архитектура защищенной многоагентной системы, основанной на использовании многоскачковых пиринговых сетей. Динамическое поведение многоагентных систем и распределенной гетерогенной среды, в которой они используются, являются причинами появления множества сетевых проблем и проблем безопасности. Предлагаемое автором для многоскачковых сред решение способствует безопасному сотрудничеству и функционированию агентов, а также их мобильности. Это достигается за счет использования защищенной неструктурированной P2P-платформы как коммуникационной среды и ее интеграции с хорошо известными многоагентными системами.

В докладе ***В. Десницкого*** *(Россия)* рассмотрена методика обеспечения защищенности и масштабируемости защиты программного обеспечения на основе механизма удаленного доверия. Предложенный автором метод позволяет выбирать для применения наиболее эффективную комбинацию различных механизмов защиты. Метод направлен

на поиск компромисса между производительностью механизма защиты и его способностью обеспечить безопасность, что позволяет достигнуть необходимого уровня безопасности, а также приемлемой масштабируемости. Метод основывается на количественном оценивании производительности и уровня безопасности частных механизмов защиты, принадлежащих к единому механизму.

На *секции «Адаптивная защита информации, живучесть компьютерных сетей и виртуализация»* было сделано несколько интересных докладов.

Я. Рак *(Польша)* рассмотрел новый подход к обеспечению дифференцированных уровней стойкости услуг в сетях IP-MPLS/WDM, основанный на использовании генетических алгоритмов. Предложенный подход разделяет комплексную задачу обеспечения устойчивой маршрутизации в IP-MPLS/WDM сетях на две подзадачи, по одной для каждого сетевого уровня, которые способны находить решение в относительно короткие сроки. Применение генетического подхода позволяет путем итеративного решения задачи значительно повысить качество результата. Результаты моделирования показали, что проведение разумного числа итераций позволяет получить достаточно хорошее решение (на 22.55 % лучше первоначального), дальнейшее совершенствование которого практически невозможно.

Доклад ***М. Калинина*** *(Россия)* был посвящен решению задачи контроля целостности в доверенной информационной среде. Главная идея предложенного подхода состоит в нахождении безопасных состояний для изменяемых программных компонентов, которые формируют безопасную среду. Предложенный автором подход основан на итеративном поиске взаимно совместимых и согласованных друг с другом безопасных состояний. Полученная в результате архитектура системы управления безопасностью и целостностью воплощает основные принципы построения автоматизированных систем управления и управления безопасностью.

Е. Рудина *(Россия)* предложила подход к моделированию безопасности виртуальной среды, который позволяет расширить функциональные возможности защищенных операционных систем. Целью проведенного исследования является определение условий, при которых механизм виртуализации способен гарантировать соответствие

заданной политике безопасности. Автором формально доказано, что если виртуальное окружение не является доверенным, то механизм виртуализации обязательно должен быть запущен в доверенной операционной системе.

В докладе ***Р. Рике*** *(Германия)* был рассмотрен подход к прогнозирующему анализу безопасности для событийно-управляемых процессов, основанный на операционных формальных моделях. Для того чтобы динамически выделять события из различных процессов и архитектурных уровней и оценивать их с учетом требований безопасности, используется анализ процессов и угроз и методы имитационного моделирования. Автором предложена архитектура системы поддержки принятия решений, основанная на выполнении динамического моделирования и анализа безопасности процессов с учетом изменяющихся в реальном времени событий. Данная система позволяет осуществлять идентификацию будущих состояний, вызывающих угрозы безопасности, и выдавать на выходе прогностическое предупреждение соответствующего нарушения.

4. Панельная дискуссия. На конференции была проведена *панельная дискуссия*, посвященная обсуждению современных проблем и тенденций в области безопасности компьютерных сетей (рис. 10).

Рис. 10. Участники панельной дискуссии (слева направо): Р. Сандху (США), Б. Пренель (Бельгия), А. Грушо (Россия), А. Мана (Испания), Г. Моррисетт (США), Х. Дебар (Франция) и Д. Голлман (Германия).

В панельной дискуссии приняли участие: Ш.-К. Чин (Сиракьюсский университет, США) — ведущий дискуссии, Х. Дебар (Институт Телеком, Франция), Д. Голлман (Технический университета Гамбурга, Германия), А. Грушо (Российский государственный гуманитарный университет, Россия), А. Мана (Университет Малаги, Испания), Г. Моррисетт (Гарвардский университет, США), Б. Пренель (Бельгия) и Р. Сандху (Техасский университет Сан-Антонио, США).

5. Заключение. Важной особенностью данной международной конференции, является, с одной стороны, акцентирование внимания на математических аспектах информационной безопасности, а с другой, — внимание 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.

В целом конференция получилась достаточно интересной, ее научный уровень соответствовал мировым стандартам. Было решено продолжить ее проведение в будущем.

Труды конференции опубликованы в сборнике «Lecture Notes in Computer Science» издательства «Шпрингер», Германия, под редакцией И. В. Котенко (Россия) и В. А. Скормина (США)[1].

Более детальную информацию о данной конференции можно найти на веб-странице *http://comsec.spb.ru/mmm-acns10/*.

Котенко Игорь Витальевич — д-р техн. наук, проф., заведующий лабораторией проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление полити-

[1] *Kotenko I., Scormin V.* (Eds.) Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-2010). September 8–10, 2010, St. Petersburg, Russia. 346 p.

ками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибертерроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Kotenko Igor Vitalievich — Ph.D., Professor, Head of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Саенко Игорь Борисович — д-р техн.наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций **—** 220. ibsaen@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 220. ibsaen@comsec.spb.ru; SPIIRAS, 14th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Юсупов Рафаэль Мидхатович — чл.-корр. РАН, д-р техн. наук, проф., директор Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН, Заслуженный деятель науки и техники РФ. Область научных интересов: теория управления, информатика, теоретические основы информатизации и информационного общества, информационная безопасность. Число научных публикаций — 350. СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; тел.(812)328-33-11, (812)328-34-11, факс(812)328-44-50, E-mail: yusupov@iias.spb.su

Yusupov, Rafael Midkhatovich — Corresponding Member of the Russian Academy of Sciences (RAS), Doctor of Sciences (Tech.), Professor, Director of Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS) Honored Scientists of the Russian Federation. Research interests: control theory, informatics, theoretic basics of informatization and information society, information security. Number of research publications:

350. SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-3411; fax: +7(812)328-4450, e-mail: yusupov@iias.spb.su; www.spiiras.nw.ru.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией, д-р техн.наук, проф. И.В. Котенко.
Статья поступила в редакцию 22.11.2010.

РЕФЕРАТ

Котенко И.В., Саенко И.Б., Юсупов Р.М. **Аналитический обзор докладов Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010).**

В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010), проходившей в Санкт-Петербурге с 8 по 10 сентября 2010 г.

Конференция стала одним из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей и продемонстрировала острый интерес исследовательских организаций и ученых всего мира к тематике использования формальных методов, моделей и построению перспективных архитектурных решений для обеспечения безопасности информационных ресурсов в компьютерных сетях.

С приглашенными докладами выступили такие известные в мире ученые, как Э. Дебар (Франция), Д. Гольманн (Германия), Г. Моррисетт (США), Б. Пренель (Бельгия), Р. Сандху (США) и А. Сабельфельд (Швеция). На 6 секциях конференции были рассмотрены 22 доклада, авторы которых представляли 10 стран: Россию, США, Австрию, Польшу, Канаду, Францию, Германию, Норвегию, Испанию и Турцию. Каждый из докладов был тщательно проанализирован тремя-четырьмя рецензентами международного программного комитета. Доклады были посвящены рассмотрению актуальных вопросов, связанных с моделированием безопасности и скрытых каналов, политиками безопасности и формальным анализом свойств безопасности, аутентификацией, авторизацией, управлением доступом и криптографией с открытым ключом, обнаружением вторжений и вредоносных программ, безопасностью многоагентных систем и защитой программного обеспечения, адаптивной защитой информации, живучестью компьютерных сетей и виртуализацией.

Важной особенностью данной международной конференции, является, с одной стороны, акцентирование внимания на математических аспектах информационной безопасности, а с другой, — внимание практическим решениям, которые могут найти широкое применение для защиты современных компьютерных сетей.

SUMMARY

Kotenko I.V., Saenko I.B., Yusupov R.M. **Analytical review of the International Conference «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-2010).**

This paper provides an analytical review of talks by leading foreign and domestic experts in the security of computer networks, presented at the International Conference «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-2010), held in St. Petersburg from 8 to September 10, 2010.

The Conference has become one of the leading international forums for the study of fundamental and applied problems of computer network security and has demonstrated a keen interest in research organizations and scientists around the world to the subject of formal methods, models and construction of advanced architectural solutions for the security of information resources in computer networks.

World-known scientists, such as E. Debar (France), D. Golmann (Germany), G. Morrisett (USA), B. Prenel (Belgium), R. Sandhu (USA) and A. Sabelfeld (Sweden), made invited talks. Twenty-two talks were discussed on six sections of the conference. The speakers represent 10 countries: Russia, USA, Austria, Poland, Canada, France, Germany, Norway, Spain, and Turkey. Each of the talks was carefully reviewed by three - four reviewers of the International Program Committee. Reports were devoted to consideration of topical issues related to security modeling and covert channels, security policies and formal analysis of security properties, authentication, authorization, access control and public key cryptography, intrusion detection and malware, secure multi-agent systems and software protection, adaptive information security, survivability of computer networks and virtualization.

An important feature of this international conference, on the one hand, is the focus on the mathematical aspects of information security, and on the other - on practical solutions that can be widely used for the protection of modern computer networks.