УДК 004.056

И.В. Котенко, И.Б. Саенко

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, МЕТОДЫ И АРХИТЕКТУРЫ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ: ОБЗОР ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ ИССЛЕДОВАНИЙ ПО РЕЗУЛЬТАТАМ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ MMM–ACNS–2012

Котенко И.В., Саенко И.Б. **Математические модели, методы и архитектуры для защиты компьютерных сетей: обзор перспективных исследований по результатам Международной конференции MMM–ACNS–2012.**

Аннотация. В статье приводится аналитический обзор перспективных направлений исследований по результатам докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на шестой Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM–ACNS–2012), проходившей в Санкт-Петербурге с 17 по 19 октября 2012 года. С приглашенными докладами выступили такие известные в мире ученые, как А. Ставро, Б. Лившиц, Л. Кхан и Ф. Мартинелли. На секциях конференции были рассмотрены актуальные вопросы, связанные с предотвращением, обнаружением и реагированием на вторжения, противодействием вредоносному программному обеспечению, прикладной криптографией и протоколами безопасности, разграничением доступа и защитой информации, управлением событиями и информацией безопасности, моделированием защиты информации и безопасностью облачных вычислений, политиками безопасности.

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

Kotenko I.V., Saenko I.B. **Mathematical Methods, Models and Architectures for Computer Network Security: the review of perspective research directions according to the results of the International Conference MMM–ACNS–2012.**

The summary. The paper provides an analytical review of perspective research directions according to the talks by leading foreign and domestic experts in the security of computer networks, presented at the 6th International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM–ACNS–2012), held in St. Petersburg from 17 to 19 October, 2012. World-known scientists, such as A. Stavrou, B. Livshits, L. Khan, and F. Martinelli, made invited talks. On sections of the conference there were discussed topical issues related to the intrusion prevention, detection, and response, anti-malware techniques, applied cryptography and security protocols, access control and information protection, security event and information management, security modeling and cloud security, and security policies.

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

1. Введение. Шестая международная конференция “Математические модели, методы и архитектуры для защиты компьютерных сетей”» (MMM–ACNS–2012), проведенная с 17 по 19 октября 2012 года

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, 2007 и 2010 годах, продемонстрировали острый интерес исследовательских организаций и ученых всего мира к тематике использования и разработки перспективных формальных методов, моделей и 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 в области защиты информации (как зарубежными, так и российскими), облегчает распространение новых идей и продвигает дух сотрудничества между исследователями в международном масштабе. Поэтому было принято решение о регулярном проведении этой конференции.

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 и Управление научных исследований ВМС США. Международный программный комитет, включавший известных специалистов по теме конференции из 18 стран Европы, Африки и Америки, выступал гарантом высокого научного уровня конференции.

Сопредседателями конференции являлись член-корреспондент РАН, профессор Р. М. Юсупов (директор СПИИРАН, Россия), Р. Л. Герклотц (Управление научных исследований ВВС США) и Ч. Д. Холланд (отделение научных исследований ВМС США в Праге, США). Сопредседатели программного комитета — профессор И. В. Котенко (СПИИРАН, Россия) и профессор В. А. Скормин (Бингэмптоновский Университет, США) (рис. 1).

На конференции было зарегистрировано 80 участников (рис. 2). Статистические данные о принадлежности участников к различным областям деятельности таковы: количество участников из университетской среды — 36; из научных организаций — 28; из коммерческих организаций — 8; из государственных учреждений — 6.

Рис. 1. Сопредседатели конференции и программного комитета: Ч.Д. Холланд (США), В.А. Скормин (США), Р.М. Юсупов (Россия) и И.В. Котенко (Россия).

Рис. 2. Участники конференции в зале заседаний.

Представим темы приглашенных докладов более подробно.

А. Ставро *(США)* выступил с докладом на тему "*Выявление рисков безопасности для коммерческих мобильных устройств*" (рис. 3). Автор показал, что последние достижения в области аппаратных возможностей мобильных портативных устройств способствуют быстрому развитию открытых операционных систем и появлению большого числа приложений для мобильных телефонов и планшетных устройств. Новое поколение интеллектуальных средств, в частности iPhone и Google Android, является достаточно мощным и позволяет выполнять большую часть пользовательских задач, ранее требовавших использования персонального компьютера. Кроме того, мобильные устройства имеют доступ к персональной идентифицирующей информации (Personally Identifiable Information) от различных датчиков, таких как GPS, веб-камера, микрофон и другие.

В докладе были рассмотрены угрозы безопасности, которые вытекают из новых возможностей смарт-устройств и онлайновых рынков приложений для мобильных устройств. Эти угрозы включают вредоносные программы, эксфильтрацию данных, использование USB и отслеживание действий пользователя и данных.

Рис. 3. Выступление А. Ставро (США).

Предлагаемые в докладе подходы к обеспечению безопасности устройств на платформе Android включают анализ исходного кода и двоичных файлов мобильных приложений с использованием “сети уровня ядра” и шифрования данных, а также управление коммуникационными механизмами для синхронизации контента пользователей с компьютерами и другими телефонами, включая обновления операционной системы или приложений через USB.

Докладчик детально рассмотрел принципы, положенные в основу проектирования механизма аутентификации для USB соединения, получившего название USBsec. Они направлены на минимальное использование оборудования и модификацию минимального набора протоколов USB с целью достижения приемлемого уровня безопасности, включая идентификацию личности и авторизацию соединения. Основными принципами являются: независимость идентификации от драйверов USB–устройства; отсутствие модификации USB–оборудования; обратная совместимость; проведение идентификации на целое устройство (в случае составного USB–устройства).

В качестве основы для реализации защищенной файловой системы была выбрана EncFS (Encrypted File System), реализованная в операционной системе Android. Предлагаемый в докладе подход для ее реализации обладает следующими возможностями: прямая и обратная совместимость EncFS с различными версиями Android; использование возможностей стандартной криптографической библиотеки OpenSSL; прозрачная поддержка других файловых систем, включая yaffs2, ext4 и vfat.

Для анализа приложений разработан ряд средств, которые запускаются на компьютере и в ходе исполнения конкретного Android-приложения осуществляют абстрактное выделение (abstraction) в нем определенных особенностей, что позволяет осуществлять автоматический анализ программы без необходимости ввода пользователем каких-либо дополнительных данных.

Разработанный механизм, способный дисассемблировать пакетные файлы Android–приложений, на выходе дает байт–код Далвика (Dalvik bytecode). Для исполнения этого байт–кода разработана Java–реализация для каждой его инструкции. Дизассемблированное приложение будет пропускать код, предназначенный для интерфейса Android API, так как он является резидентным для всех мобильных устройств.

Докладчик остановился также на проблемах, возникающих при решении поднятых вопросов обеспечения безопасности мобильных

устройств, направленных на развертывание защищенных смартфонов в военных сценариях.

В докладе ***Б. Лившица*** "*Обнаружение вредоносного программного обеспечения в веб-приложениях*" были рассмотрены имеющиеся у компании Майкрософт результаты поиска вредоносных программ в Интернете (рис. 4). Докладчик подчеркнул, что в последние годы вредоносные программы, основанные на JavaScript, стали одним из самых популярных способов реализации осуществляемых с помощью атак drive-by-download через браузеры. Это явилось причиной разработки ряда методов, которые направлены на обнаружение и предотвращение последствий вредоносного программного обеспечения.

Рис. 4. Выступление Б.Лившица (США).

В докладе освещались результаты трех исследовательских проектов в этой области: Nozzle, Zozzle и Rozzle.

Первые два проекта были направлены на разработку детекторов вредоносных программ: Nozzle — детектор во время выполнения программ, Zozzle — статический детектор. Rozzle является методом, обрабатывающим результаты, полученные первыми двумя детекторами.

Детектор Nozzle сосредоточен на поиске атак "распыления кучи" (heap spraying). Он использует методы "легковесной" эмуляции (light-

weight emulation) для обнаружения объектов, содержащих исполняемый код. Для снижения ошибок, было предложено и разработано понятие “здоровья кучи” (heap health). Nozzle сканирует “кучу” (heap) связанных данных объекта для идентификации правильных последовательностей кода x86, дизассемблирует этот код и создает граф управляющих потоков (control flow graph). Предложенные метрики “здоровья кучи” позволяют эффективно разделять доброкачественное поведение кода от вредоносных атак.

Детектор Zozzle является статическим детектором, способным обнаруживать вредоносные программы, реализованные на JavaScript, относящиеся к атакам “распыления кучи” и другим типам атак. Для идентификации синтаксических элементов, которые имеют вредоносный код, детектор использует байесовскую классификацию иерархических особенностей абстрактных синтаксических деревьев JavaScript-программ.

Rozzle является многозадачной виртуальной машиной. За счет проверки множества возможных путей исполнения кода, он позволяет выявлять специфичные для среды исполнения вредоносные программы.

Докладчик привел оценки эффективности рассматриваемых детекторов и показал, что все они являются достаточно точными. У детектора Nozzle вероятность появления ошибки первого рода составляет величину менее чем один раз в миллиард. У детектора Zozzle это значение равно примерно один на миллион. Ruzzle повышает эффективность мониторного детектора в три раза, а статического — почти в семь раз.

В заключительной части доклада автор сосредоточился на рассмотрении взаимосвязей между предложенными способами статического и мониторного анализа и описал возможные способы переноса полученных результатов исследований в реальные изделия.

Доклад ***Л. Кхана*** *(США)* “*Проектирование и разработка системы гарантированного обмена информацией, основанной на облачных технологиях*” был посвящен рассмотрению системы гарантированного обмена информацией, основанной на облачных технологиях (рис. 5).

Докладчик подчеркнул, что появление облачных вычислений и продолжающееся движение в сторону парадигмы “программное обеспечение как услуга” (Software as a Service) создают растущую потребность в гарантированном обмене информацией как облачной службы.

В докладе рассматривалась система, получившая название Cloud-centric Assured Information Sharing System (CAISS).

В архитектуре этой системы выделяются три слоя. Верхним является слой пользовательского интерфейса.

Рис. 5. Выступление Л. Кхана (США).

Промежуточный слой содержит политики безопасности и управляет ими. Низшим является слой хранения данных, который объединяет различные источники данных, находящиеся в облаке.

Предлагаемый в CAISS механизм управления политиками основан на использовании конфигурационных документов формата RDF (Resource Description Framework), которые кодируют логику пользовательского интерфейса, настраиваемые параметры, правила политик безопасности и отображения URI на хранимые данные, учитывая допустимые соединения с данными. Управление RDF–данными осуществляется с помощью механизма SPARQL–запросов. SPARQL (SPARQL Protocol and RDF Query Language) является языком, широко используемым в сообществе Semantic Web для выполнения запросов к данным в формате RDF, и считается более выразительным, чем другие XML–ориентированные языки представления политик безопасности.

На интерфейсном уровне выполняется регистрация пользователей и “агентств” (agency). Регистрация пользователей осуществляется с помощью регистрационной формы, содержащей имя пользователя, пароль и другие пользовательские метаданные. Метаданные могут быть “агентством”, частью которого является пользователь, или данными, отображающими пользовательские учетные данные в роли, которые пользователи должны исполнять. При регистрации “агентств” вначале создаются RDF–документы, содержащие имя агентства, его адрес, отрасль, принадлежность и т.д. Затем с помощью URI описываются ресурсы. После этого определяются политики для ресурсов, примерами которых являются управление доступом, редакция, обмен информацией и т.д. Затем описываются правила политик. Наконец, при завершении регистрации определяются SPARQL–запросы.

Промежуточный слой использует в качестве исходных данных пользовательские учетные данные и URI. Затем оценивается логика, лежащая в политике, и на интерфейсный слой возвращается RDF–граф. URI указывает на конфигурационный документ, который содержит другие идентификаторы URI, указывающие на политики применительно к агентским ресурсам, и на агентские ресурсы слоя хранения данных.

Слой хранения данных является механизмом соединений (connection factory), создающим объекты соединений (connection objects). Эти объекты выражают некоторые функциональные свойства, необходимые для разработчика политик. Для этих целей делается запрос на уровень RDF–политик. Обратно возвращается RDF–модель объекта, которая учитывает память соединения. В качестве памяти соединения могут выступать локальное соединение, соединение с реляционной базой данных и соединение с облаком. Механизм соединений позволяет агентствам хранить свои ресурсы в любой облачной инфраструктуре (в личном облаке, в корпоративном облаке или в общедоступном облаке), которые отличаются уровнем контроля доступа.

При рассмотрении отдельных аспектов реализации модуля политик докладчик рассмотрел такие вопросы, как взаимность политик, разработка и масштабирование политик, обоснование ресурсов, а также спецификация и усиление политик.

В докладе ***Ф. Мартинелли*** *(Италия) “От качественного к количественному выполнению политик безопасности”* были представлены качественные и количественные аспекты проблемы реализации политики безопасности (Security Policy Enforcement) (рис. 6).

По мнению докладчика, проблема выполнения политики безопас-

ности достаточно хорошо изучена за последнее десятилетие после появления новаторской работы Ф. Шнейдера (F.B. Schneider) по безопасным автоматам (security automata).

Рис. 6. Выступление профессора Ф. Мартинелли (Италия).

В докладе эта проблема вначале рассматривается в качественном аспекте, а затем — в количественном, причем констатируется, что в последнем случае задача является намного более сложной.

Качественный аспект направлен на то, чтобы определить, является ли используемый для реализации политики безопасности оперативный монитор “хорошим”, и описать его. Для этой цели предлагается перейти от безопасных автоматов к операторам контроллера алгебры процессов (process algebra controller operators). В качестве таковых рассматриваются следующие операторы: сокращения (truncation), подавления (suppression), вставки (insertion) и редактирования (edit). Каждый из этих операторов имитирует один из безопасных автоматов. При определенных условиях операторы контроллера могут синтезироваться автоматически, используя метод частичной “проверки на модели” (partial model checking).

Количественный аспект направлен на определение, какой контроллер является наилучшим либо наихудшим, и почему принимается

такая оценка.

Существует ряд направлений исследований, связанных с количественной реализацией политики безопасности. Докладчик остановился на рассмотрении следующих направлений: неточная реализация (inexact enforcement) политики безопасности, вероятностное будущее (probabilistic future), стоимость реализации (cost of enforcement) и отслеживание реализации.

В заключение доклада были кратко рассмотрены направления дальнейших исследований по поставленной проблеме. К их числу, в первую очередь, относится синтез контроллера в количественном аспекте, гарантирующий, что синтезируемый контролер будет удовлетворять ряду количественных свойств. Предпочтительным способом решения этой задачи видится адаптация метода частичной "проверки на модели" для вероятностной алгебры процессов и темпоральных логик. Другим интересным направлением является пересмотр традиционных взглядов на определение того, какой вид политик может быть реализован в заданном контексте, используя введенные понятия стоимости, точности и т.д. Это позволит отличить политики, которые могут быть реализованы только с неограниченной стоимостью, от тех, которые имеют конечную стоимость. В результате становится возможным выявление таких политик, стоимость которых превышает выигрыш, получаемый от их реализации.

3. Секционные доклады. В ходе подготовки к конференции было получено 44 доклада из 12 стран. Наибольшее количество статей поступило из России, США и Франции. Каждая из статей была тщательно проанализирована тремя–четырьмя рецензентами. В результате международным программным комитетом было отобрано двадцать два лучших секционных доклада, представляющих 10 стран: Россию, США, Канаду, Мексику, Италия, Францию, Германию, Норвегию, Испанию и ЮАР. Из этих докладов 14 было выбрано для полных презентаций и 8 — для коротких.

Программа конференции включала работу *семи секций*:

- "Предотвращение, обнаружение и реагирование на вторжения",
- "Противодействие вредоносному программному обеспечению",
- "Прикладная криптография и протоколы безопасности",
- "Разграничение доступа и защита информации",
- "Управление событиями и информацией безопасности",
- "Моделирование защиты информации и безопасность облач-

ных вычислений” и

- “Политики безопасности”.

Секция *“Предотвращение, обнаружение и реагирование на вторжения”* была посвящена рассмотрению различных моделей, методов и средств, предназначенных для борьбы с вторжениями в компьютерные сети.

Доклад ***В. Скормина*** *(США)* был посвящен вопросам использования поведенческого моделирования и настраиваемых профилей нормальности для защиты компьютерных сетей от целевых кибер–атак.

Докладчик показал, что наилучшие результаты в области обнаружения аномалий могут быть получены, если выполнять поведенческий анализ на самом высоком семантическом уровне. При этом большинство критических компьютерных систем выполняют специфические функции и, как ожидается, исполняют ограниченный набор программ.

Докладчик остановился на рассмотрении результатов моделирования такого поведения путем создания пользовательских профилей нормальности этих систем. Также были представлены результаты оценки того, насколько хорошо происходит обнаружение аномалий в этих случаях.

Й.Б. Мустафа *(Франция)* рассмотрела аспекты реализации баз данных обманных систем и сетей, позволяющие повысить эффективность корреляции сигналов тревоги в системах управления информацией и событиями безопасности (Security Information and Event Management, SIEM). В докладе была представлена стратегия повышения эффективности предупреждений, целью которой является улучшение локальных знаний о событиях за счет учета глобальной информации об угрозах. Наиболее значимыми источниками информации о глобальных угрозах являются большие обманные системы и сети, которые позволяют собрать значительную часть скрытой информации, касающейся образа действий нарушителей, наблюдая за динамикой распространения угроз. Докладчик представил результаты исследования четырех баз данных обманных систем, которые собирают данные о распространении вредоносных программ и информацию безопасности о профиле веб–сервера. Предлагаемый докладчиком подход основан на проведении межуровневой корреляции предупреждений. Эксперименты показали, что на информацию, хранящуюся в текущей обманной базе данных, воздействуют следующие ограничения: взаимодействия обманных систем; сбора необработанных данных; стандартизации в области представления информации; документации, описывающей доступную информацию.

В докладе ***Т.В. Степановой*** *(Россия)* была рассмотрена разработанная стохастическая модель взаимодействия между бот–сетями и распределенными вычислительными системами. Предлагаемая модель позволяет предсказать результат взаимодействия между бот–сетью и системой защиты и может быть использована как основа для построения эффективной распределенной системы защиты от атак бот–сетей.

На секции *"Противодействие вредоносному программному обеспечению"* были представлены доклады Ч. Явари (США), А. Сарацино (Италия) и Д. Комашинского (Россия).

В докладе ***Ч. Явари*** (*США*) была предложена классификация вредоносного программного обеспечения, основанная на рассмотрении поведенческих компонентов. Для этой цели использовался подход так называемой "мягкой кластеризации". Докладчик остановился на экспериментальных результатах, показывающих, что существующий подход к классификации вредоносных программ, основанный на доминантной функциональности и фиксирующий классификационное дерево, не показывает связи между вредоносными программами с учетом их поведения. Согласно предлагаемому подходу, итеративно строятся диапазоны характеристик, которые формируют мягкие кластеры, отображающие разделяемые черты компонентов. Оценка показала высокую масштабируемость и производительность предлагаемой схемы компонентного анализа на реальном множестве из 1727 образцов вредоносных программ.

Доклад ***А. Сарацино*** *(Италия)* посвящен рассмотрению разработанного многоуровневого детектора аномалий вредоносного программного обеспечения на платформе Android, получившего название MADAM (Multi-level Anomaly Detector for Android Malware). Детектор MADAM постоянно контролирует систему Android как на уровне ядра, так и на пользовательском уровне. Он выявляет заражение, используя методы машинного обучения, позволяющие отличить стандартное поведение от вредоносного. Первый же прототип детектора MADAM оказался способным обнаруживать некоторые реальные вредоносные программы, впервые найденные для Android. Детектор не оказывает существенного влияния на производительность мобильного устройства, так как реализованный в нем метод после прохождения стадии обучения дает малое количество ошибок обнаружения.

В докладе ***Д. Комашинского*** *(Россия)* предложен подход к обнаружению вредоносного программного обеспечения, связанный с использованием низкоуровневых динамических атрибутов на основе интеллектуального анализа данных. Идея этого подхода заключается в

рассмотрении любого приложения, требующего анализа, в виде последовательности исполняемых инструкций, которая рассматривается как основной источник признаков, необходимых для представления анализируемого приложения в векторной форме для использования методов интеллектуального анализа данных.

Доклады, заслушанные на секции *"Прикладная криптография и протоколы безопасности"*, посвящены перспективным аспектам криптографии и разработки протоколов безопасности.

В. Коржик *(Россия)* для модели активного злоумышленника в каналах с шумом предложил новые протоколы распределения ключей, основанные на использовании экстракторов, и подход к их оптимизации. Полученные результаты оценки предлагаемых протоколов по основным показателям показали их высокую эффективность.

С.Ф. Мьёлнес *(Норвегия)* рассмотрел результаты исследования уязвимостей в протоколах аутентификации и согласования ключей UMTS и LTE. Предложены решения по корректировке этих протоколов. Исследована возможность использования средства CriptoVerif для верификации процесса идентификации и ключевых свойств секретности для скорректированных протоколов.

В докладе ***Н. Молдовяна*** *(Россия)* рассматривались предложения по созданию схемы слепой цифровой подписи с длиной 384 бит. Данная схема получается путем использования конечной субгруппы мультипликативной группы конечного кольца остатков по модулю, являющемуся произведением двух достаточно больших простых чисел.

На секции *"Разграничение доступа и защита информации"* были заслушаны доклады К. Джин (США), В. Олещука (Норвегия) и А. Грушо (Россия).

В докладе ***К. Джин*** (*США*) была рассмотрена формальная модель ролевого управления доступом, основанного на атрибутах, получившая название RABAC (Role-Centric Attribute-Based Access Control). Она является расширением стандартизированной ролевой модели RBAC в направлении ограничения полномочий ролей через атрибуты. Докладчик сделал общий обзор модели, представил ее формальные основы и обсудил ее функциональную спецификацию. Было показано, что, по сравнению со стандартной моделью RBAC, потребовали своего переопределения две функции: функция FilteredSessionPerm, возвращающая допустимые полномочия для каждой сессии, и функция CheckAccess, осуществляющая проверку выполнения действий над объектами.

В докладе ***В. Олещука*** (*Норвегия*) предложено расширение роле-

вой модели RBAC, в котором перед установлением доступа учитывается доверительность пользователей. Эта модель получила название TA-RBAC (Trust-Aware RBAC). В этой модели каждая роль связана с выражением, которое описывает доверительность субъектов, требующих доступа, и позволяет активизировать роль, а каждый пользователь (субъект) имеет некоторый уровень доверия. Этим обеспечивается более высокая гибкость модели при делегировании ролей и при управлении чтением/обновлением объектов за счет отклонения тех действий, в которых нарушаются требования, предъявляемые к доверительности субъектов.

Доклад ***А. Грушо*** *(Россия)* был посвящен рассмотрению, по терминологии докладчика, альтернативных механизмов защиты конфиденциальности, целостности и доступности информации, к которым были отнесены предложенные математические модели недостоверной информации. Кроме того, был предложен метод введения недостоверности в информацию.

На секции *"Управление событиями и информацией безопасности"* были сделаны доклады Г.Г. Гранадильо (Франция), Э. Хатчисоном (ЮАР) и Дж. Шутте (Германия).

В докладе ***Г.Г. Гранадильо*** (*Франция)* предложен качественный подход к выбору оптимальных контрмер по обеспечению безопасности, который основан на учете показателя возврата инвестиций. Предлагаемый подход предполагает два этапа действий. На первом этапе для каждой возможной контрмеры вычисляется усовершенствованный показатель возврата инвестиций, который учитывает не только стоимость контрмеры и связанное с нею смягчение риска, но также ожидаемые потери, которые могут иметь место как следствие вторжения или атаки. На втором этапе осуществляется ранжирование отдельных контрмер и выбор оптимальной среди них. В качестве сценария для проверки разработанных моделей расчета данного показателя была выбрана предметная область службы перевода мобильных денег (Mobile Money Transfer Service), показавшая высокую применимость предлагаемого подхода.

В докладе ***Э. Хатчисона*** *(ЮАР)* рассмотрены требования по безопасности и достоверности, предъявляемые к перспективной системе управления информацией и событиями безопасности (Security Information and Event Management, SEIM). Предлагаемый подход выделяет четыре сценария применения таких систем: инфраструктура проведения крупных спортивных соревнований, система мобильных платежей, провайдер услуг и критическая инфраструктура. Основываясь на базо-

вых элементах и атрибутах каждого сценария, докладчик показал требования к SIEM–системам нового поколения по безопасности, обработке событий, надежности и методике компиляции.

В докладе ***Дж. Шутте*** *(Германия)* рассмотрен основанный на моделях подход к обнаружению инцидентов безопасности, вызванных событиями, и управлению ими. Эта модель поддерживает мониторинг безопасности с помощью корреляции событий на различных уровнях. Сложные события безопасности собираются от компонентов компьютерной инфраструктуры, от компонентов, предоставляющих информацию об атаках и уязвимостях, а также от прогностических анализаторов безопасности. Реализация этого подхода позволяет объединить воедино все преимущества, присущие в настоящее время различным системам управления инцидентами безопасности: обнаружения, отчетности, управления и объяснения.

На секции *"Моделирование защиты информации и безопасность облачных вычислений"* было сделано несколько интересных докладов.

В. Десницкий *(Россия)* рассмотрел подход к обеспечению безопасности встроенных систем на основе их конфигурирования. Докладчик представил основные положения, касающиеся разработанной конфигурационной модели встроенных систем, и показал, что она дает возможность создавать более безопасные и энергетически эффективные встроенные системы. Модель позволяет находить наиболее эффективные комбинации защищенных конструкционных блоков на основе решения оптимизационной задачи. В качестве критерия для оптимизации конфигурации было выбрано минимальное потребление ресурсов, связанных с функциями защиты. Ограничения оптимизационной задачи в конфигурационной модели налагаются на возможность реализации функциональных свойств, на числовые значения нефункциональных свойств, а также на свойства платформенной совместимости.

Доклад ***Б. Керригана*** *(США)* был посвящен важному аспекту исследования источников энтропии в "облачных компьютерах", которым является генерация случайных чисел на хостах "облачных вычислений". Так как "облачные вычисления" опираются на виртуализацию, доступ к аппаратному генератору случайных чисел ограничен, и виртуализация может иметь непредвиденные последствия для функционирования систем, основанных на генераторах случайных чисел. Для защиты от возможных атак на источники энтропии в "облачных компьютерах", в частности от потенциальной атаки "планового отравления пула" (Scheduled Pool Poisoning Attack), в докладе предлагается

использовать разработанную авторами систему управления “облачной” энтропией (Cloud Entropy Management System), позволяющую выявлять слабости такой генерации.

Доклад ***А.С. Коноплева*** *(Россия)* был посвящен моделированию безопасности грид–систем с использованием сетей Петри. Докладчик рассмотрел проблему безопасности вычислений и информационных ресурсов в грид–системах. Он описал характеристики относительной безопасности грид–архитектуры и предложил общую модель угроз в грид–системе. Затем докладчик проанализировал методы, применяющиеся для обеспечения безопасности грид–систем, и обсудил их недостатки. Как результат такого анализа, была предложена основанная на сетях Петри модель разграничения доступа для грид–систем. Новизна предложенной модели заключается в описании времени и изменения состояния грид–системы как двух дискретных переменных и в учете предопределенных отношений доступа.

Доклад ***А.В. Никольского*** *(Россия)* был посвящен использованию теории графов для моделирования безопасности “облачной” системы. Вначале докладчик обозначил проблемы безопасности в “облачных” системах. Затем он представил модель “облачной” системы, которая позволяет формально описать различные задачи безопасности. Предложенная модель основана на теории графов и описывает основные характеристики виртуальных машин в “облачных” системах. После этого были представлены формальные основы преобразования операций доступа к данным, которые имеют место в программном обеспечении гипервизора благодаря технологии виртуализации. Это позволило затем формально определить несколько проблем безопасности “облачных” систем для программного обеспечения гипервизора. В завершение докладчик рассмотрел проблемы безопасности, связанные с разделенным использованием виртуальных машин в “облаке”.

На секции *“Политики безопасности”* были рассмотрены доклады Н. Тоби (Канада), Т. Аванесова (Франция) и А. Чечулина (Россия).

Н. Тоби *(Канада)* представила подход к обеспечению политик информационных потоков, основанный на применении трехзначного типизированного (type-based) анализа. Основная идея предложенного подхода заключается в том, что если программа является хорошо типизированной в соответствии со своими правилами типизации, то она является безопасной в соответствии с заданными свойствами безопасности. Суть подхода заключается в управлении безопасной типизацией на основе трехзначной логики. Каждая программа рассматривается как хорошо типизированная, плохо типизированная или неопределенная.

Оценка безопасности в двух первых случаях является традиционной. В последнем случае необходимо использовать инструментарий, имеющийся в предлагаемой системе безопасных типов, чтобы гарантировать удовлетворение невмешательства (non-interference).

В докладе ***Т. Аванесова*** *(Франция)* представлены результаты работы в области синтеза безопасных сервисов с помощью медиатора (mediator). Эта проблема ранее была сведена к проблеме разрешения ограничений выводимости, подобной тем, которые решаются при анализе криптографических протоколов. Автор рассматривает расширение процедуры синтеза медиатора, используемого для создания безопасных сервисов, основанное на построении выражений, в которых некоторые данные не доступны для медиатора. Затем предлагается решающая процедура для верификации того, что медиатор, удовлетворяющий данной незакрытой политике, может быть успешно синтезирован. Для реализации этой процедуры разработано средство анализа протоколов CL-AtSe.

А. Чечулин *(Россия)* предложил комбинированный подход к анализу сетевых информационных потоков во встроенных системах. Данный подход развивает теоретические аспекты анализа информационных потоков и базируется на совместном использовании двух основных подходов в этой области — топологического и основанного на политиках. Принципы обоих существующих подходов были подробно рассмотрены в докладе. В качестве сценария для апробации предложенного подхода была выбрана сеть интеллектуальных измерительных приборов (Smart Metering Devices Network), которая является усовершенствованной измерительной инфраструктурой, состоящей из нескольких доверенных измерителей, серверов баз данных, клиентских приложений и коммуникационной инфраструктуры. Были продемонстрированы структуры основных данных и спецификации информационных потоков разработанного программного прототипа, позволяющего провести экспериментальную оценку информационных потоков для этого сценария.

4. Панельная дискуссия. На конференции была проведена *панельная дискуссия*, посвященная обсуждению современных проблем и тенденций в области безопасности компьютерных сетей (рис. 7). В панельной дискуссии приняли участие: В. Скормин (США) - ведущий дискуссии, А. Грушо (Россия), Э. Хатчисон (ЮАР), Л. Кхан (США), В. Коржик (Россия), П. Ласков (Германия), Р. Рике (Германия), Ф. Мартинелли (Италия), С. Мьёлнес (Норвегия), В. Олещук (Новегия) и И. Котенко (Россия).

5. Заключение. Важной особенностью данной международной конференции являлось сбалансированное сочетание результатов, которые, с одной стороны, были посвящены вопросам математического обеспечения информационной безопасности, с другой стороны являются конкретными результатами, имеющими высокую практическую значимость для защиты современных компьютерных сетей.

Рис. 7. Участники панельной дискуссии.

В числе рассматриваемых вопросов — предотвращение, обнаружение и реагирование на вторжения, противодействие вредоносному программному обеспечению, прикладная криптография и протоколы безопасности, разграничение доступа и защита информации, управление событиями и информацией безопасности, моделирование защиты информации и безопасность облачных вычислений, политики безопас-

ности 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», издательство «Шпрингер», Германия, том 7531, под редакцией И.В. Котенко (Россия) и В.А. Скормина (США) [1].

Более детальную информацию о данной конференции можно найти на Web–странице http://comsec.spb.ru/mmm-acns12/.

Литература

1. *Kotenko I., Scormin V.* (Eds.) Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. 6th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security, MMM-ACNS 2010. St. Petersburg, Russia, October 2012, Proceedings. 312 p. ISSN 0302-9743.

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками 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 кибер-терроризму. 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, 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, 14-th 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 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 — 250. 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, 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 — 250. ibsaen@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн.наук, проф.
Статья поступила в редакцию 29.12.2012.

РЕФЕРАТ

Котенко И.В., Саенко И.Б. **Математические модели, методы и архитектуры для защиты компьютерных сетей: обзор перспективных исследований по результатам Международной конференции MMM–ACNS–2012.**

В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на шестой Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010), проходившей в Санкт-Петербурге с 17 по 19 октября 2012 года.

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 А. Ставро (США), Б. Лившиц (США), Л. Кхан (США) и Ф. Мартинелли (Италия).

На семи секциях конференции были рассмотрены двадцать два доклада, авторы которых представляли 10 стран: Россию, США, Канаду, Мексику, Италия, Францию, Германию, Норвегию, Испанию и ЮАР. Каждый из докладов был тщательно проанализирован тремя – четырьмя рецензентами международного программного комитета. Доклады были посвящены рассмотрению актуальных вопросов, связанных с предотвращением, обнаружением и реагированием на вторжения, противодействием вредоносному программному обеспечению, прикладной криптографией и протоколами безопасности, разграничением доступа и защитой информации, управлением событиями и информацией безопасности, моделированием защиты информации и безопасностью облачных вычислений, политиками безопасности.

Важной особенностью данной международной конференции являлось сбалансированное сочетание результатов, которые посвящены вопросам математического обеспечения информационной безопасности, и являются конкретными результатами, имеющими высокую практическую значимость для защиты современных компьютерных сетей.

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

SUMMARY

Kotenko I.V., Saenko I.B. **Mathematical Methods, Models and Architectures for Computer Network Security: the review of perspective research directions according to the results of the International Conference MMM–ACNS–2012.**

This paper provides an analytical review of talks made by leading foreign and domestic experts in the security of computer networks, presented at the 6th International Conference “Mathematical Methods, Models and Architectures for Computer Networks Security” (MMM-ACNS-2010), held in St. Petersburg from 17 to 19 October, 2012.

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 A. Stavrou, B. Livshits, L. Khan, and F. Martinelli, made invited talks.

Twenty-two talks were discussed on seven sections of the conference. The speakers represent 10 countries: Russia, USA, Canada, Mexico, Italy, France, Germany, Norway, Spain, and RSA. 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 intrusion prevention, detection, and response, anti-malware techniques, applied cryptography and security protocols, access control and information protection, security event and information management, security modeling and cloud security, and security policies.

An important feature of this international conference is a balanced mix of the results, which, on the one hand, devote districts of mathematical supplement of information security and, on the other, are the concrete results of high feasibility of relevance for the protection of modern computer networks.

Overall, the conference was interesting fairly, its scientific level corresponds to the world standards. It was decided to continue the conference in the future.