УДК 004.056

И.В. Котенко, И.Б. Саенко

НАУЧНЫЙ АНАЛИЗ И ПОДДЕРЖКА ПОЛИТИК БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ: ОБЗОР ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ ИССЛЕДОВАНИЙ ПО РЕЗУЛЬТАТАМ МЕЖДУНАРОДНОГО СЕМИНАРА SA&PS4CS 2012

Котенко И.В., Саенко И.Б. **Научный анализ и поддержка политик безопасности в киберпространстве: обзор перспективных исследований по результатам Международного семинара SA&PS4CS 2012.**

Аннотация. В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на втором Международном семинаре "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2012), проходившем в Санкт-Петербурге 20 октября 2012 года. Среди зарубежных ученых выступили В. Скормин (США), Ф. Мартинелли (Италия), В. Олещук (Норвегия), Р. Рике (Германия), Э. Хатчисон (ЮАР), Л. Кхан (США), П. Ласков (Германия) и С. Мьёлснес (Норвегия). Среди российских участников выступили В. Майоров, А. Свистунов, Р. Юсупов, А. Грушо, П. Зегжда, А. Смирнов, А. Земцов и И. Котенко. Основными темами выступлений семинара являлись обнаружение, распознавание и определение различных видов деятельности злоумышленников, реагирование на атаки и вторжения в киберпространстве, включая информационные операции национального уровня, идентификация новых перспективных технологий, способов, методов и средств обеспечения взаимодействия в области поддержки политик безопасности в киберпространстве.

Ключевые слова: киберпространство, защита информации, политика безопасности, кибертерроризм, киберпреступность.

Kotenko I.V., Saenko I.B. **Scientific analysis and policy support for cyber security: the review of perspective research directions according to the results of the International Workshop SA&PS4CS 2012.**

Absract. The paper provides an analytical review of the invited talks by leading foreign and domestic experts in the security of computer networks, presented at the 2nd International Workshop "Scientific Analysis and Policy Support for Cyber Security" (SA&PS4CS 2012), held in St. Petersburg October 20, 2012. The following foreign scientists had presentations: V. Skormin (USA), F. Martinelli (Italy), V. Oleshchuk (USA), R. Rieke (Germany), A. Hutchison (RSA), L. Khan (USA), P. Laskov (Germany), and S. Mjølsnes (Norvey). The following Russian specialists were invited: V. Mayorov, A. Svistunov, R. Yusupov, A. Grusho, P. Zegzhda, A. Smirnov, A. Zemtsov, and I. Kotenko. The main topics of the workshop's presentations were detection, recognition and identification of various types of malicious activity, responding to attacks and intrusions in cyberspace, including information operations at the national level, the identification of new promising technologies, techniques, methods and means of cooperation ensuring in the field of security policies support in cyberspace.

Keywords: cyberspace, information security, security policy, cyber terrorism, cyber crime.

1. Введение. Второй международный семинар “Научный анализ и поддержка политик безопасности в киберпространстве” (SA&PS4CS 2012) был проведен 20 октября 2012 года в Санкт-Петербурге совместно с шестой Международной конференцией “Математические методы, модели и архитектуры для защиты компьютерных сетей” (MMM-ACNS-2012).

Семинар был нацелен на объединение усилий специалистов, вовлеченных в различные области деятельности, относящиеся к научному анализу и поддержке политик безопасности в киберпространстве, для обмена идеями и изучения последних исследований и разработок в этой важной сфере.

Семинар был организован СПИИРАН и Университетом Бингхэмтона — государственным университетом штата Нью-Йорк (США). Финансовую поддержку обеспечили Европейское управление воздушно-космических исследований и разработок США и Управление научных исследований ВМС США.

Сопредседателями семинара 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).

2. Приглашенные доклады. Для участия в семинаре были персонально приглашены известные специалисты в области защиты информации из различных стран. Всего было представлено 16 приглашенных докладов, которые сделали представители шести стран: Россия — 8, США — 2, Норвегия — 2, Италия — 1, Германия — 2 и ЮАР — 1.

Выступления были разделены на три секции. Основными темами выступлений семинара являлись обнаружение, распознавание и определение различных видов деятельности злоумышленников, реагирование на атаки и вторжения в киберпространстве, включая информационные операции национального уровня, идентификация новых перспективных технологий, способов, методов и средств обеспечения взаимодействия в области поддержки политик безопасности в киберпространстве.

Была опубликована брошюра семинара, включающая общие сведения о семинаре, его программу, аннотации всех докладов и краткие библиографические данные о докладчиках.

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

На семинаре было зарегистрировано 46 участников (рис. 2). Представим темы отдельных докладов более подробно.

Рис. 2. Участники семинара.

Владимир Майоров *(Отдел информационной безопасности, противодействия техническим разведкам и развития систем защиты информации, Комитет по информатизации и связи Санкт-*

Петербурга, Российская Федерация) выступил с приветствием от имени Комитета по информатизации и связи Санкт-Петербурга (рис. 3). В приветствии было подчеркнуто, что в условиях глобализации мировой экономики вопросами обеспечения безопасности в киберпространстве обеспокоено все мировое сообщество. В этой связи объединение усилий представителей разных стран по обеспечению кибербезопасности посредством эффективного внедрения передовых технологий становится актуальным. Правительство города в лице Комитета по информатизации и связи ведет активную работу по развитию инфраструктуры электронного правительства и расширению перечня государственных и муниципальных услуг, оказываемых в электронном виде.

Рис. 3. Выступление Владимира Майорова (Российская Федерация).

Такое виртуальное взаимодействие предполагает наличие максимально эффективных и безопасных инструментов обеспечения информационного обмена.

В заключение докладчик выразил уверенность, что семинар позволит еще в большей степени скоординировать усилия при решении задач обеспечения кибербезопасности и придаст новый импульс развитию информационного сообщества.

Доклад ***Андрея Свистунова*** *(Казенное учреждение "Оператор «электронного правительства»", Российская Федерация)* назывался

“Противодействие кибер–злоумышленникам на примере реализации единого Центра управления системами защиты информации информационных систем органов исполнительной власти Ленинградской области” (рис. 4).

Рис. 4. Выступление Андрея Свистунова (Российская Федерация).

В докладе были рассмотрены вопросы централизации механизмов управления и мониторинга средствами и системами защиты государственных информационных ресурсов органов исполнительной власти (ОИВ) Ленинградской области на примере реализации единого Центра управления системами защиты информации информационных систем ОИВ Ленинградской области. При этом были обозначены основные проблемы управления средствами и системами защиты информации, возникающие при оперативном реагировании на кибератаки в крупных территориально-распределенных государственных и отраслевых информационных системах. В заключение были показаны практические пути решения данных проблем на примере организации единого подхода к обеспечению информационной безопасности в ОИВ Ленинградской области и централизации функций управления, мониторинга и оперативного реагирования на кибератаки в едином центре управления.

В докладе ***Рафаэля Юсупова*** (*СПИИРАН, Российская Федерация*) “*Информатизация общества и национальная безопасность*” были

рассмотрены особенности проблемы национальной безопасности в условиях информатизации общества, обусловленные широким внедрением информационных и коммуникационных технологий (ИКТ) во все сферы человеческой деятельности, включая систему обеспечения национальной безопасности (рис. 5).

Рис. 5. Выступление Рафаэля Юсупова (Российская Федерация).

Докладчик показал, что проблема приобретает ряд специфичных свойств, связанных с повышением в обществе роли информации, информационных ресурсов и ИКТ. Влияние ИКТ на обеспечение национальной безопасности является двойственным. ИКТ расширяют возможности как опасностей и угроз национальной безопасности (например, международного терроризма), так и системы обеспечения национальной безопасности. Было отмечено, что информационная безопасность в условиях информатизации является важнейшим компонентом национальной безопасности, пронизывающим все остальные ее составляющие.

Фабио Мартинелли *(Институт информатики и телематики, Национальный исследовательский совет, Италия)* в своем докладе на тему *"Кибербезопасность и мобильные устройства"* рассмотрел проблемы информационной безопасности, касающиеся использования мобильных устройств (рис. 6). Докладчик подробно остановился на рассмотрении возможных видов атак на мобильные устройства, а также способов использования мобильных устройств в качестве источников атак на инфраструктуры.

Рис. 6. Выступление Фабио Мартинелли (Италия).

Доклад ***Виктора Скормина*** (*Бингемтоновский Университет, США*) "*Проект науки о кибербезопасности, как ее видит Фред Шнайдер"* был посвящен рассмотрению вопросов, связанных с формированием кибербезопасности как научной дисциплины (рис. 7).

Необходимость формирования науки о кибербезопасности, которая бы создала фундаментальную базу для разработки систем безопасности и определила бы законы, позволяющие разработчикам оценивать последствия выбора того или иного архитектурного решения и его реализации, настоятельно назрела.

Рис. 7. Выступление Виктора Скормина (США).

Эти законы должны оперировать новыми абстракциями и моделями, не привязанными к какой-либо конкретной технологии или атаке. Благодаря этому они приобретут педагогическую ценность, позволят создавать новые механизмы защиты от информационных угроз, выявлять неявные зависимости между атаками, механизмами защиты и политиками, формируя тем самым лучшее понимание окружающей реальности. Поэтому, разрабатывая науку о кибербезопасности, нельзя ограничиваться только изучением уязвимостей в проектируемых системах и созданием контрмер против конкретных атак. Следует понимать, что применение данной науки не тожественно созданию абсолютно безопасной системы или даже установлению того факта, что безопасность системы требует изменения проекта и реализации. Скорее цель науки о кибербезопасности — это предоставить рабочий набор методик, независимых от конкретных систем, включая допущения и ограничения, которые необходимы для их реализации, и способы, позволяющие преобразовать один набор допущений в другой. Наука о кибербезопасности должна структурировать набор абстракций, принципов и альтернатив для разработки безопасных систем согласно реальным угрозам и требованиям к информационной безопасности.

В докладе ***Александра Грушо*** *(Институт проблем информатики РАН, Российская Федерация) "Математика и кибербезопасность"* были рассмотрены некоторые проблемы компьютерной и сетевой безопасности, которые касаются следующих областей: выявления стеганографии и скрытых каналов в сетевом трафике; поиска уязвимостей в кодах программного обеспечения; анализа безопасности протоколов; выявления бот-сетей и центров управления ими (рис. 8).

Рис. 8. Выступление Александра Грушо (Российская Федерация).

Был приведен пример построения статистических критериев в задаче поиска скрытых каналов и аномалий, основанных на запретах. В данном примере было рассмотрено, как задачи компьютерной и сетевой безопасности породили новое направление исследований в математической статистике и как полученные результаты позволяют оценить возможности выявления скрытых каналов и аномалий.

Владимир Олещук *(Университет Агдера, Норвегия)* в докладе *"Кибербезопасность и приватность"* рассмотрел цели кибербезопасности и приватности, а также имеющиеся в этой области проблемы и конфликты интересов (на индивидуальном, организационном и национальном уровнях) (рис. 9).

Рис. 9. Выступление Владимира Олещука (Норвегия).

Он обратил внимание на то, что кибербезопасность важна для защиты критических инфраструктур и обеспечения стабильности, устойчивости, безопасности и надежности Интернета и сопутствующих служб, в то время как приватность является частью индивидуальной свободы в цифровом веке, правом индивидуумов выбирать как, когда и кому они могут предоставить персональную информацию. Некоторые цели кибербезопасности и приватности могут восприниматься как конфликтующие. Таким образом, необходим тонкий баланс между

требованиями кибербезопасности и приватности. В заключение были представлены некоторые подходы, базирующиеся на применении технологий, которые могут использоваться для разрешения, по крайней мере, некоторых из этих конфликтов.

В докладе ***Петра Зегжды*** *(Санкт-Петербургский государственный политехнический университет, Российская Федерация) "Анализ и контроль безопасности виртуализированных вычислительных систем"* были систематизированы угрозы на средства виртуализации и системы управления виртуализированными вычислительными системами (рис. 10).

Рис. 10. Выступление Петра Зегжды (Российская Федерация).

Виртуализированные вычислительные системы (системы облачных вычислений, грид-системы, виртуальные центры обработки данных) представляют собой не столько технологию обработки информации, сколько бизнес-модель предоставления пользователю распределенных вычислительных и информационных ресурсов в виде единого удаленного сервиса.

Такие системы повышают эффективность использования ресурсов для большого числа пользователей, однако при этом не обеспечивается всесторонний контроль над безопасностью информации. Докладчик

рассмотрел существующие методы защиты таких систем, привел оценку их эффективности. Им были проанализированы возможность и принципы построения доверенной виртуализированной среды, основанной на управлении безопасностью и мониторинге выполнения условий безопасной виртуализации. Результаты анализа позволили предложить метод динамической верификации безопасности на примере грид-систем. В заключение были показаны возможности сокращения угроз безопасности в случае создания доверенных средств виртуализации и выдвинуты требования к практическим решениям.

В докладе ***Роланда Рике*** *(Институт безопасных информационных технологий Фраунгофера, Германия) "Повышение ситуационной осведомленности, безопасности и надежности процессов в системах систем"* был рассмотрен подход к построению систем управления информацией и событиями безопасности (Security Information and Event Management, SIEM) следующего поколения, который обеспечивает эффективную поддержку управления и идентификации ситуаций по безопасности (рис. 11).

Рис. 11. Выступление Роланда Рике (Германия).

Докладчик подчеркнул, что Интернет уже представляет собой новую среду, которая существенно повышает наши возможности по созданию новейших приложений и процессов. Эта среда делает использование множества сервисов прозрачным и гибким, автоматически

адаптируемым к поведению пользователя, и во многих случаях развивающимся за пределы предварительно планируемых областей и целей.

Географически распределенные реальные и виртуальные инфраструктуры, сервисы и ресурсы являются компонентами таких процессов внутри масштабных, сильно взаимосвязанных систем. Тем не менее, эта развивающаяся среда также способствует развитию новых угроз и увеличивает риски как финансового, так и физического ущерба.

Во многих случаях, информация сама по себе будет значимым продуктом, который заслуживает того, чтобы быть защищенным. В Интернете вещей (Internet-of-things) заслуживают нашего внимания реальные и виртуальные киберфизические ресурсы. Кибербезопасность при таких условиях является областью глобального внимания, которой пока сложно управлять и которую, возможно, даже сложнее измерить. Несмотря на тот факт, что разработаны безопасные технические решения, существует огромное множество примеров компрометируемых систем, процессов и транзакций.

Далее в докладе были рассмотрены компоненты и принципы построения надежной, адаптируемой, масштабируемой, гибкой и защищенной SIEM-системы. Предложенный подход поддерживает сбор и управление событиями безопасности вовлеченных систем, процессов и приложений с учетом различных уровней представления системы. Особое внимание было уделено в докладе анализу событий на основе реализации интеллектуальных автоматизированных процессов и предсказанию возможных нарушений безопасности. Результаты такого анализа поведения системы в реальном времени могут быть интегрированы с процессами анализа графов атак. Кроме того, докладчик обратил внимание на процессы идентификации предполагаемого воздействия и стратегии противодействия, которые позволят выполнить адаптацию к текущей ситуации и осуществить принятие решений и реализацию проактивного и динамического противодействия.

Эндрю Хатчисон *(T–Systems International, Южно-Африканская Республика)* в докладе *“Поддержка политик для обмена событиями безопасности и их обработки SIEM–системами в контексте развития требований Евросоюза к защите данных”* предложил подход к анализу директив и норм Евросоюза, регулирующих приватность данных (рис. 12).

При этом был сделан особый акцент на особенностях их применения в SIEM–системах, которые могут быть важными механизмами при обнаружении и реагировании на вторжения и атаки.

Для операторов SIEM–систем важным аспектом является нахождение баланса между получением доступа ко всей информации, позволяющей отслеживать возможные и текущие вторжения, и соблюдением прав пользователей (а также регулирующих норм законодательства Евросоюза, в частности).

В докладе также рассматривались проблемы межнационального обмена информацией в контексте требований к защите данных. Как предполагается, поддержка политик безопасности обуславливает рассмотрение и установку параметров и подходов для обмена и интерпретации событий.

Рис. 12. Выступление Эндрю Хатчисона (ЮАР).

Более того, еще на этапе разработки самой политики безопасности необходимо учитывать возможность информационного обмена, определив методы и подходы к его организации.

Анатолий Смирнов *(Национальный институт исследований глобальной безопасности, Российская Федерация)* в докладе *"Мягкая сила 2.0 и актуальные вопросы международной информационной безопасности"* привел результаты исследования одной из самых острых проблем XXI века — использования новейших ИКТ в современной матрице глобальной безопасности (рис. 13).

Результаты исследования данной проблемы Национальным ин-

ститутом исследований глобальной безопасности были подробно изложены в книге “Глобальная безопасность и “мягкая сила 2.0”: вызовы и возможности для России”, изданной в 2012 году. В этой книге феномен сегодняшнего этапа информационной революции — охвата глобальными социальными сетями миллиардов участников — исследуется как принципиально новое геополитическое явление.

Докладчик позиционировал новейшие теоретические и практические наработки на стыке ИКТ и международных отношений к новым вызовам и угрозам, а также к возможностям цивилизации и России обеспечить глобальную безопасность.

Рис. 13. Выступление Анатолия Смирнова (Российская Федерация).

Доклад ***Анатолия Земцова*** *(Group-IB, Российская Федерация) “Безопасность и борьба с преступностью в киберпространстве. Правовые аспекты”* был посвящен обзору актуальных проблем законодательной и правоприменительной практики в Российской Федерации в области обеспечения безопасности и борьбы с преступностью в киберпространстве (рис. 14).

Наряду с кратким анализом общепринятых “компьютерных” статей УК РФ, претерпевших за прошедший год серьезные изменения, поднимался вопрос об иных, требующих криминализации, деяниях —

DDoS–атаках, создании и управлении бот–сетями и других. Здесь особое внимание уделялось проблеме наиболее актуальных преступлений, непосредственным образом связанных с применением информационных технологий, — мошенничестве в системах дистанционного банковского обслуживания. Отдельно освещалась проблематика распространения контрафакта в сети Интернет, а также вопросы недобросовестной и преступной эксплуатации бренда.

Существенная часть доклада была посвящена прикладным юридическим практикам, применяемым в целях минимизации возможных правовых рисков компаний в вопросах предотвращения инцидентов информационной безопасности.

Рис. 14. Выступление Анатолия Земцова (Российская Федерация).

В том числе была дана правовая оценка различным аспектам обеспечения информационной безопасности (например, применению систем DLP в организации) и расследования инцидентов информационной безопасности в компании.

В докладе ***Латифура Кхана*** *(Университет Техаса, Даллас, США) "Интеллектуальный анализ потоков данных и его применения для информационной безопасности"* обсуждался структурированный подход к применению различных методов интеллектуального анализа информационных потоков, в частности, было показано применение классификации для анализа эволюционирующих потоков (рис. 15).

Потоки данных представляют собой непрерывные последовательности данных. Примеры таких потоков — сетевой трафик, данные сенсоров, записи call–центров и т.д. Большие объемы и скорости поступления данных значительно затрудняют процессы их интеллектуального анализа. Потоки данных обладают рядом уникальных свойств, таких как смещение и эволюция концепта (понятия). Смещение концепта в потоках данных возникает при изменении рассматриваемого концепта данных во времени. Эволюция концепта возникает при появлении новых классов концептов в потоках данных. Каждое из этих свойств вносит новые трудности в процесс интеллектуального анализа потоков данных.

Рис. 15. Выступление Латифура Кхана (США).

В докладе были рассмотрены такие примеры приложений интеллектуального анализа потоков данных, как адаптивное обнаружение вредоносного кода, оперативное детектирование вредоносных URL и выявление угроз инсайдеров. Данное исследование было выполнено при финансовой поддержке НАСА и Управления научных исследований ВМС США (AFOSR).

Павел Ласков *(Университет Тюбингена, Германия)* в докладе *“Долговременный структурный мониторинг PDF–документов на ресурсе VirusTotal”* подчеркнул, что портал VirusTotal является популярным ресурсом, на котором собрана коллекция вредоносного про-

граммного обеспечения, и целью которого является анализ данных и сбор информации обо всех существующих антивирусных решениях (рис. 16).

Он используется как обычными Интернет–пользователями, так и производителями антивирусных продуктов для анализа подозрительных данных и оценки точности антивирусных сигнатур. Информация, собранная на портале VirusTotal, отражает последние тенденции в развитии вредоносного программного обеспечения.

В докладе в качестве примера использования данного ресурса в научных целях были представлены результаты длительного непрерывного мониторинга за набором данных, содержащего все PDF–документы, загруженные в базу данных портала.

Рис. 16. Выступление Павла Ласкова (Германия).

Представленная в докладе методика основана на структурном анализе PDF–файлов и их сравнении. Она позволяет получить точную классификацию зараженных и безобидных PDF–документов, идентифицировать структурно идентичные наборы файлов и дифференцировать их по содержанию в рамках заданного синтаксического контекста.

Дальнейшее направление исследования, рассмотренное в докладе, связано с применением описанной методики для обнаружения ранее неизвестного вредоносного программного обеспечения, предназначенного для заражения PDF–файлов.

Доклад ***Стига Мьёлснеса*** *(Норвежский университет науки и технологий, Норвегия) "Атаки отказа в обслуживании на протоколы беспроводного доступа"* был посвящен проблеме семантических атак на протоколы, т.е. атак, которые используют уязвимости в сообщениях и поведении протокола (рис. 17).

Беспроводной мобильный доступ к системам связи — это на настоящий момент повсеместная практика, является ли это мобильной телефонией, доступом к веб–серверам или доступом к Интернету в целом. Немедленная и постоянная доступность систем связи важна для выполнения операций в чрезвычайных ситуациях, реализации различных форм мониторинга и систем аварийного предупреждения, критичных приложений безопасности (медицинских, транспортной безопасности и др.), для которых любой сбой может привести к различным видам ущерба. К сожалению, большинство широко используемых на сегодняшний день протоколов беспроводного доступа уязвимы к атакам на отказ в обслуживании.

Рис. 17. Выступление Стига Мьёлснеса (Норвегия).

Игорь Котенко (*СПИИРАН, Российская Федерация*) в докладе "*Кибервойны интеллектуальных агентов в сети Интернет*" предложил общий подход и его практическое применение для исследования и реализации различных видов адаптивных и кооперативных способов функционирования команд программных интеллектуальных агентов для реализации распределенных компьютерных атак и механизмов

защиты в сети Интернет (рис. 18).

Для осуществления своих целей, как системы нападения, так и системы защиты в Интернет должны быть кооперативными, адаптивными и динамически эволюционировать и изменять реализуемые механизмы поведения при изменении условий функционирования. Для реализации этих возможностей в перспективных системах защиты компьютерных сетей необходимо обеспечить динамическое адаптивное поведение, автономность и адаптацию отдельных компонентов, использовать методы, основанные на переговорах и кооперации, которые лежат в основе многоагентных систем и/или автономных вычислений.

Рис. 18. Выступление Игоря Котенко (Российская Федерация).

3. Панельная дискуссия. На семинаре была проведена панельная дискуссия, посвященная обсуждению форм международного взаимодействия по предупреждению, обнаружению и реагированию на кибер-вторжения и атаки (рис. 19). В панельной дискуссии приняли участие: В. Скормин (США) — ведущий дискуссии, П. Зегжда (Россия), А. Грушо (Россия), А. Земцов (Россия), Л. Кхан (США), П. Ласков (Германия) и С. Мьёлснес (Норвегия).

Рис. 19. Участники панельной дискуссии.

4. Заключение. Важной особенностью международного семинара явилось акцентирование внимания как на теоретических аспектах кибербезопасности, так и на практических решениях, которые могут найти широкое применение, с одной стороны, для обнаружения и реагирования на атаки и вторжения в киберпространстве, а с другой, — в развитии международного сотрудничества по противодействию киберпреступности и кибертерроризму.

В целом, семинар получился достаточно интересным, и его научно-практический уровень соответствовал мировым стандартам. По результатам дискуссии среди участников семинара, было решено продолжить его проведение в будущем.

Информацию по данному семинару можно найти на Web-странице http://www.comsec.spb.ru/saps4cs12/.

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 30.12.2012.

РЕФЕРАТ

Котенко И.В., Саенко И.Б. **Научный анализ и поддержка политик безопасности в киберпространстве: обзор перспективных исследований по результатам Международного семинара SA&PS4CS 2012.**

В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на втором Международном семинаре “Научный анализ и поддержка политик безопасности в киберпространстве” (SA&PS4CS 2012), проходившем в Санкт-Петербурге 20 октября 2012 года.

Семинар был нацелен на объединение усилий специалистов, вовлеченных в различные области деятельности, относящиеся к научному анализу и поддержке политик безопасности в киберпространстве, для обмена идеями и изучения последних исследований и разработок в этой важной сфере.

Среди зарубежных ученых выступили В. Скормин (США), Ф. Мартинелли (Италия), В. Олещук (Норвегия), Р. Рике (Германия), Э. Хатчисон (ЮАР), Л. Кхан (США), П. Ласков (Германия) и С. Мьёлснес (Норвегия). Среди российских участников выступили В.Майоров, А. Свистунов, Р. Юсупов, А. Грушо, П. Зегжда, А. Смирнов, А. Земцов и И. Котенко. Основными темами выступлений семинара являлись обнаружение, распознавание и определение различных видов деятельности злоумышленников, реагирование на атаки и вторжения в киберпространстве, включая информационные операции национального уровня, идентификация новых перспективных технологий, способов, методов и средств обеспечения взаимодействия в области поддержки политик безопасности в киберпространстве.

На панельной дискуссии было проведено обсуждение международного взаимодействия по предупреждению, обнаружению и реагированию на кибервторжения и атаки.

Важной особенностью международного семинара явилось акцентирование внимания как на теоретических аспектах кибербезопасности, так и на практических решениях, которые могут найти широкое применение, с одной стороны, в области обнаружения и реагирования на атаки и вторжения в киберпространстве, а с другой, — в развитии международного сотрудничества по противодействию киберпреступности и кибертерроризму.

В целом, в соответствии с единодушным мнением участников семинара, семинар получился достаточно интересным, и его научно-практический уровень соответствовал мировым стандартам. По результатам дискуссии среди участников семинара, было решено продолжить его проведение в будущем.

SUMMARY

Kotenko I.V., Saenko I.B. **Scientific analysis and policy support for cyber security: the review of perspective research directions according to the results of the International Workshop SA&PS4CS 2012.**

This paper provides an analytical review of talks by leading foreign and domestic experts in the security of computer networks, presented at the 2nd International Workshop "Scientific Analysis and Policy Support for Cyber Security" (SA & PS4CS 2012), held in St. Petersburg on 20 October, 2012.

The Workshop aimed to bring together specialists involved in various areas related to scientific analysis and support of security policies in cyberspace to share ideas and explore the latest research and developments in this important area.

The following foreign scientists had presentations: V. Skormin (USA), F. Martinelli (Italy), V. Oleshchuk (USA), R. Rieke (Germany), A. Hutchison (RSA), L. Khan (USA), P. Laskov (Germany), and S. Mjølsnes (Norvey). The following Russian specialists were invited: V. Mayorov, A. Svistunov, R. Yusupov, A. Grusho, P. Zegzhda, A. Smirnov, A. Zemtsov, and I. Kotenko.

The main topics of the workshop's presentations were detection, recognition and identification of various types of malicious activity, responding to attacks and intrusions in cyberspace, including information operations at the national level, the identification of new promising technologies, techniques, methods and means of cooperation ensuring in the field of security policies support in cyberspace.

The panel discussion was followed by a discussion of forms of international cooperation to prevent, detect and respond to cyber intrusions and attacks.

An important feature of the international workshop was to focus both on the theoretical aspects of cybersecurity and on practical solutions that can be widely used, on the one hand, to detect and respond to attacks and intrusions into cyberspace and, on the other hand, are to promote international cooperation against cyber crime and cyber terrorism.

In general, in accordance with the unanimous opinion of the participants, the workshop turned out interesting enough and its scientific and practical level consistent with international standards. According to participants, it was decided to continue its conduct in the future.