УДК 004.056

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

АНАЛИТИЧЕСКИЙ ОБЗОР ДОКЛАДОВ МЕЖДУНАРОДНОГО СЕМИНАРА «НАУЧНЫЙ АНАЛИЗ И ПОДДЕРЖКА ПОЛИТИК БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ» (SA&PS4CS 2010)

Котенко И.В., Саенко И.Б., Юсупов Р.М. **Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010).**

Аннотация. В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на Международном семинаре «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010), проходившем в Санкт-Петербурге 11 сентября 2010 г. Среди зарубежных ученых выступили В. Скормин (США), П. Лосиевич (США), Ш.-К. Чин (США), Р. Сандху (США), А. Мана (Испания), А. Кириченко (Финляндия) и Р. Шори (Индия). Среди российских ученых выступили А. Азарсков, Р. Юсупов, П. Зегжда, С. Бажин, И. Трифаленков, М. Вус, А. Писемский 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., Yusupov R.M. **Analytical review of the reports of the International Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA&PS4CS 2010).**

The summary. The paper provides an analytical review of invited talks by leading foreign and domestic experts in the security of computer networks, presented at the International Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA&PS4CS 2010), held in St. Petersburg September 11, 2010. The following foreign scientists had presentations: V. Skormin (USA), P. Losievich (USA), Sh.-K. Chin (USA), R. Sandhu (USA), A. Manna (Spain), A. Kirichenko (Finland) and R. Shorey (India). The following Russian specialists were invited: A. Azarskov, R. Yusupov, P. Zegzhda, S. Bazhin, I. Trifalenkov, M. Vus, A. Pisemskiy 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. Первый международный семинар «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) был проведен 11 сентября 2010 г. в Санкт-Петербурге совместно с пятой Международной конференцией «Математические методы, модели и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2010).

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, Управление научных исследований ВМС США, Российский фонд фундаментальных исследований и компания «Группа информационной безопасности» (Group-IB), Россия.

Сопредседателями семинара являлись 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).

2. Приглашенные докладчики. Для участия в семинаре были персонально приглашены известные специалисты в области защиты информации из различных стран. Всего было представлено 15 сообщений приглашенных докладчиков, представителяющих пять стран: Россию (8 докладов), США (4 доклада), Финляндию (1 доклад), Индию (1 доклад), Испанию (1 доклад). Выступления были разделены на три секции. Была опубликована брошюра, включающая общие сведения о семинаре, его программу, аннотации всех докладов и краткие библиографические данные о докладчиках. На семинаре был зарегистрирован 51 участник (рис. 2).

Основными темами выступлений семинара являлись обнаружение, распознавание и определение различных видов деятельности злоумышленников, реагирование на атаки и вторжения в киберпростран-

стве, включая информационные операции национального уровня, идентификация новых перспективных технологий, способов, методов и средств обеспечения взаимодействия в области поддержки политик безопасности в киберпространстве.

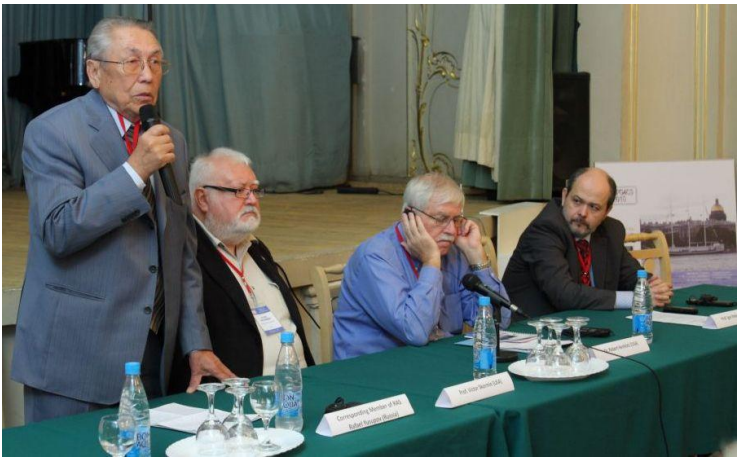

Рис. 1. Сопредседатели семинара и программного комитета:
Р.Юсупов (Россия), В.Скормин (США),
Р.Герклотц (США) и И.Котенко (Россия).

Рис. 2. Участники семинара.

Представим темы отдельных докладов более подробно.

Алексей Азарсков (*Комитет по информатизации и связи Санкт-Петербурга, Российская Федерация*) выступил с докладом на тему «*Обеспечение информационной безопасности жизнедеятельности*

населения Санкт-Петербурга» (рис. 3). Автор рассмотрел вопросы создания пилотной зоны комплексной системы обеспечения безопасности (КСОБ) жизнедеятельности Санкт-Петербурга, являющейся результатом совместной работы МЧС, ГУВД, ФСБ и Правительства Санкт-Петербурга, которая велась в течение последних 5 лет. За этот период времени созданы и внедрены в практическое использование основные элементы КСОБ жизнедеятельности Санкт-Петербурга: мониторинговый центр; система видеонаблюдения в четырех районах города; служба обработки экстренных вызовов; система информирования и оповещения населения; система обеспечения безопасности объектов городского хозяйства; единая система видеоконференцсвязи.

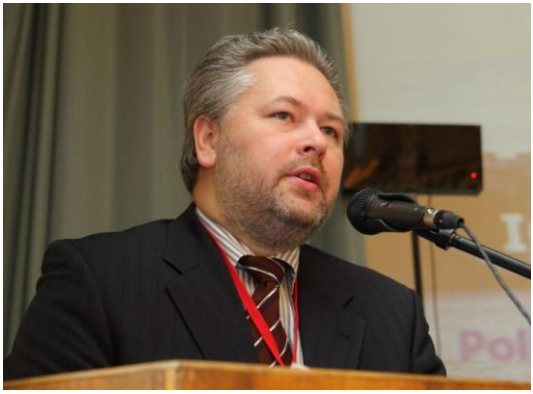

Рис. 3. Выступление Алексея Азарскова (Российская Федерация).

Опыт работы силовых ведомств и городских служб во время проведения в Санкт-Петербурге крупных международных и массовых мероприятий доказывает состоятельность выбранного пути по использованию новых информационных технологий в процессе обеспечения безопасности жизнедеятельности города. Следующей задачей по развитию КСОБ является создание единой системы информирования и оповещения населения при возникновении чрезвычайных ситуаций. Она должна интегрировать в себя все способы доведения информации до населения, в том числе звуковые сообщения через специализированные системы на улицах и внутри городских объектов, видео- и текстовую информацию на электронных табло, массовую рассылку тре-

вожных сообщений на мобильные устройства (*Cell Broadcast*). Отработанные в Санкт-Петербурге на практике организационные, технологические и информационные решения по комплексному обеспечению безопасности жителей города в дальнейшем могут быть тиражированы в других субъектах Российской Федерации.

В докладе ***Рафаэля Юсупова*** (*СПИИРАН, Российская Федерация*) «*Информатизация общества и национальная безопасность*» (рис. 4) рассмотрены особенности проблемы национальной безопасности в условиях информатизации общества, т.е. при широкомасштабном внедрении информационных и коммуникационных технологий (ИКТ) во все сферы человеческой деятельности, в том числе и в систему обеспечения национальной безопасности. При этом основная сущность и содержание национальной безопасности сохраняются. В тоже время проблема приобретает ряд специфичный свойств, связанных с повышением в обществе роли информации, информационных ресурсов и ИКТ. Информационная «окраска» проникает во все основные составляющие проблемы национальной безопасности: геополитику, национальные интересы, угрозы безопасности, ее силы и средства, направления (виды) безопасности. В докладе отмечался двойственный характер влияния ИКТ на обеспечение национальной безопасности: ИКТ одновременно расширяют возможности как опасностей и угроз национальной безопасности (например, международного терроризма), так и системы обеспечения национальной безопасности. Особое внимание было уделено вопросам информационной безопасности, под которой автор понимает следующую триаду: защиту информации, защиту от информации и добывание информации о намерениях и возможностях противоборствующей стороны в информационной сфере. Было отмечено, что информационная безопасность в условиях информатизации является важнейшим компонентом национальной безопасности, пронизывающим все остальные ее составляющие (экономическую, социальную, оборонную, политическую безопасность и т.д.). В заключение был затронут вопрос об отношении США и России к проблеме повышения роли ИКТ в решении задач обеспечения национальной безопасности.

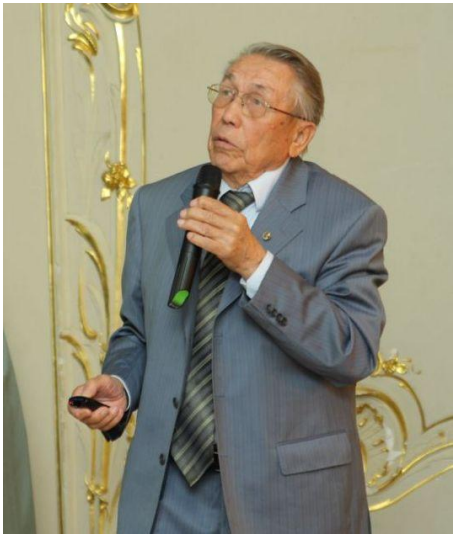

Рис. 4. Выступление Рафаэля Юсупова (Российская Федерация).

Доклад ***Виктора Скормина*** (*Бингемтоновский Университет, США*) «*Безопасность киберпространства как новая область совместных международных исследований*» (рис. 5) был посвящен анализу кибератак и возможным направлениям сотрудничества для их обнаружения и реагирования. Эти атаки скрытны по своей сути, по ним трудно идентифицировать атакующих, а киберпространство не соответствует географическим и геополитическим реалиям. Поэтому в ответ на вызванные кибератаками экономические потери и дестабилизацию обстановки в глобальном масштабе правительства, различные организации и профессиональные сообщества должны активизировать совместные усилия по противодействию этому явлению. Это является единственным путем для успешного обнаружения источников этих атак, определения нарушителей и смягчения последствий атак. Сутью международных усилий должно стать установление взаимного доверия между специалистами, которое, в конечном итоге, приведет к развитию взаимного доверия между государствами. При этом во многих случаях совместные международные усилия в области кибербезопасности должны соответствовать образцам сотрудничества, проявляющимся, например, в случаях предсказывания ураганов и распростране-

ния инфекционных заболеваний. Такое сотрудничество будет способствовать решению многих вопросов борьбы с киберпреступностью и кибертерроризмом.

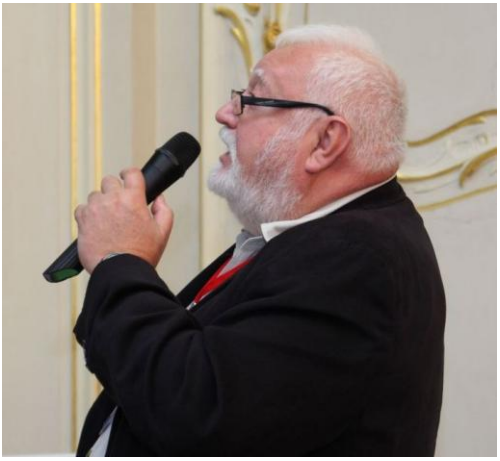

Рис. 5. Выступление Виктора Скормина (США).

В докладе ***Пола Лосиевича*** (*Управление научных исследований ВМС США*) «*Интересы Министерства обороны в области исследований по поддержке национальной безопасности и международной стабильности*» (рис. 6) были рассмотрены вопросы соответствия кибероперациий известным законам войны (например, Закону о сухопутной войне, Army FM-100) и определения технологических подходов и методов, которые могут и должны быть использованы, чтобы отличить, если это возможно, легитимное использование средств национальной безопасности от способов уголовной или террористической деятельности. Обсуждались такие различия и сходные элементы между кибер- и обычными, ядерными, биологическими и химическими действиями, как асимметрия, дискриминация, живучесть и пропорциональность. Как результат проведенного анализа, автором был предложен ряд мер, которые могут принять государства, чтобы повысить стабильность в мире и не стать жертвой текущих асимметричных угроз в киберпространстве.

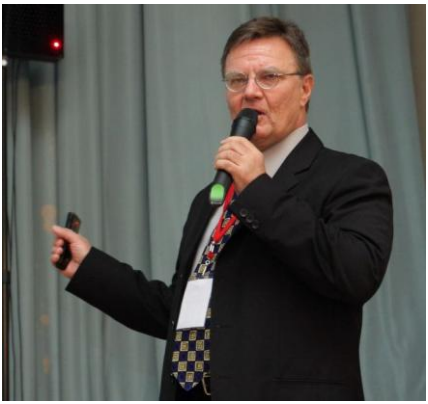

Рис. 6. Выступление Пола Лосиевича (США).

В докладе ***Петра Зегжды*** (*Санкт-Петербургский государственный политехнический университет, Российская Федерация*) «*Безопасность киберпространства — современное состояние и тенденции*» (рис. 7) была приведена статистика наиболее распространенных и опасных угроз в киберпространстве, источники их возникновения и распространения, тенденции развития.

В качестве основных тенденций развития компьютерных сетей, оказывающих влияние на распространение вредоносных программ, были выделены: возрастание популярности использования социальных сетей; использование злоумышленниками социальной инженерии; сохранение множества уязвимостей; увеличение числа атак на веб-сайтах и случаев их использования в преступных целях; возрастание скорости создания новых угроз; способность бот-сетей к DoS-атакам, взлому паролей и другим вредоносным действиям; достижение количеством пользователей *Mac* критического уровня, за которым киберпреступники становятся заинтересованными в этой платформе; увеличение числа вредоносных программ для мобильных устройств; прогнозирование увеличения числа вредоносных программ для Windows 7.

Основным мотивациями киберпреступников в настоящее время являются получение доступа к информации и манипуляция данными путем наиболее популярных видов преступных действий — обхода средств защиты и DoS-атак.

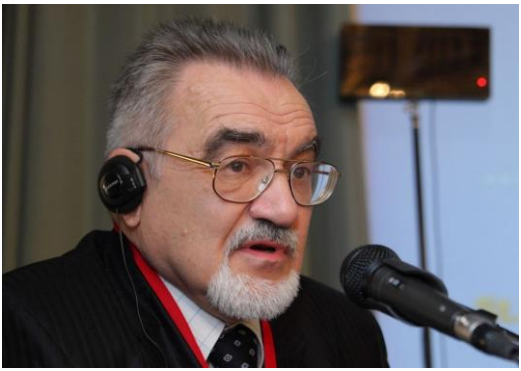

Рис. 7. Выступление Петра Зегжды (Российская Федерация).

В качестве основных направлений дальнейшего развития средств защиты автором были предложены: совершенствование программных средств разработки (Visual Studio 2010) и языков программирования (Java, C#) с целью предотвратить появление уязвимостей на этапе разработки; совершенствование аппаратных средств (в том числе на уровне процессора) защиты уязвимостей; развитие средств и методов поиска уязвимостей в классическом программном обеспечении и в веб-приложениях; разработка новых подходов к архитектуре защиты вне зависимости от операционной системы и устройства; разработка средств безопасности, основанных на принципах виртуализации.

В заключение автор высказался о необходимости разработки концепции безопасности как баланса между конфиденциальностью, целостностью и доступностью.

В докладе ***Шиу-Кай Чина*** (*Сиракьюсский университет, Исследовательская лаборатория BBC, США*) «*Навстречу полноценной интеграции системного проектирования и искусства ведения операций в кибер-пространстве*» (рис. 8) рассмотрены текущие исследования, направленные на обнаружение или разработку общих принципов и концепций, которые могут быть строго применены к операциям в киберпространстве.

Будущие операции в киберпространстве потребуют объединения искусства военной стратегии с наукой системного проектирования. С одной стороны, суть оперативного искусства заключается в возможности осуществлять правильную координацию во времени и простран-

стве централизованных действий, чтобы нейтрализовать, ослабить или уничтожить противника для достижения конечной военной цели. С другой стороны, системное проектирование заключается в разработке следующего:

1) сочетания элементов (включая все аппаратное и программное обеспечение, оборудование, оснащение, персонал, процессы и процедуры), функционирующих вместе для удовлетворения некоторых требований и реализации заданной цели;

2) конечного продукта операций (выполняющего оперативные функции) и вспомогательных продуктов (предоставляющих услуги поддержки жизненного цикла конечных продуктов), которые вместе образуют систему.

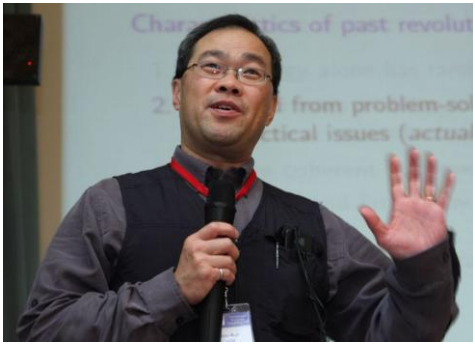

Рис. 8. Выступление Шиу-Кай Чина (США).

Военные операции в киберпространстве являются реализацией кибер-возможностей, где главной целью является достижение военных целей и результатов в киберпространстве или на основе использования киберпространства.

Поиск или разработка общих принципов и концепций, которые охватывают военную стратегию, политику, вычислительную технику и компьютерную безопасность, является более сложным процессом, чем формулировка определений. Автор рассмотрел результаты выполняющихся исследований, целью которых является обнаружение или разработка этих общих принципов и концепций, которые могут быть строго применены к операциям в киберпространстве.

Сергей Бажин (*Северо-Западный филиал ЗАО «Комстар-Регионы», Российская Федерация*) в докладе «*Сравнительный анализ законодательства Российской Федерации и США в сфере борьбы к компьютерной преступностью*» (рис. 9) привел результаты сравнительного анализа действующего законодательства России и США в сфере борьбы с компьютерной преступностью и выделил различия в подходах, а также возможные слабые стороны действующих правовых норм в законодательном пространстве двух стран. На основе практического опыта были рассмотрены особенности и различия в проведении расследований компьютерных преступлений, степень взаимосвязи их с другими (налоговыми, экономическими и пр.) преступлениями.

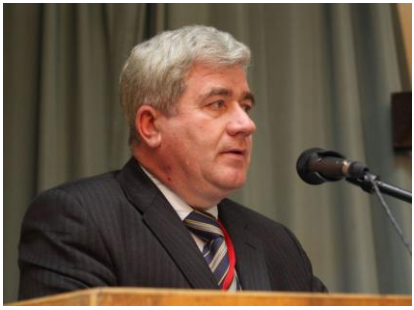

Рис. 9. Выступление Сергея Бажина (Российская Федерация).

Была подчеркнута необходимость дополнительной оценки квалифицированного состава, ужесточения санкций и выработки механизма признания преступными средств компьютерной техники, используемой злоумышленниками. Автор предложил использовать единый подход к разработке законодательных основ в сфере борьбы с компьютерной преступностью не только между Россией и США, но и с участием других стран на международном уровне.

В докладе ***Рави Сандху*** (*Институт кибербезопасности, США*) «*Законы кибербезопасности*» (рис. 10) обсужден характер предложенных им законов безопасности киберпространства. По аналогии с микро- и макроэкономикой проведено различие между микро- и макрокибербезопасностью. Утверждалось, что определение микро-кибербезопасности более понятно, и предлагались конкретные законы, применяющиеся в этой области.

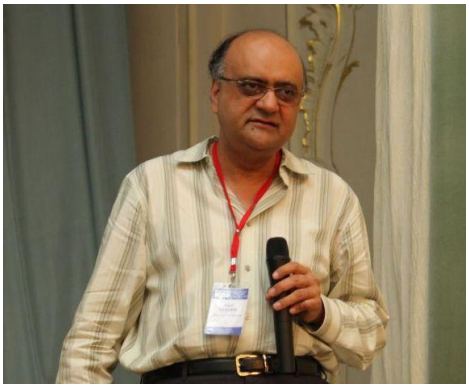

Рис. 10. Выступление Рави Сандху (США).

К числу таких законов автор относит следующие:

1) «злоумышленники существуют» (следствием этого закона является утверждение, что любой пользователь может быть атакован);

2) «злоумышленники резко подняли свою стимуляцию» (теперь все чаще целями атак становятся деньги, терроризм, войны, шпионаж, саботаж и т.д.);

3) «злоумышленники ленивы» (они следуют по пути меньшего сопротивления, в результате чего атаки будут обостряться, но не быстрее, чем это необходимо);

4) «злоумышленники являются новаторами (скрытыми)» (все возможные атаки, в конце концов, проявятся);

5) «злоумышленники являются подражателями» (число известных атак будет возрастать);

6) «злоумышленники обладают асимметричным преимуществом» (им нужна всего одна точка отказа).

Также автор выделил следующие операционные принципы:

1) готовиться к завтрашним атакам, а не только ко вчерашним;

2) готовиться к завтрашним атакам прежде, чем к тем, что появится в следующем году;

3) планировать защиту от будущих атак и вносить в эти планы своевременные коррективы;

4) выдерживать компромисс между безопасностью, удобством и стоимостью.

Для макрокибербезопасности, по мнению автора, обсуждение данных вопросов является более спекулятивным и предварительным.

Илья Трифаленков (*РНТ, Российская Федерация*) в докладе «*Большие системы: от защиты информации к управлению безопасностью*» (рис. 11) рассмотрел проблему минимизации рисков, вызванных сращиванием процессов деятельности больших систем с информационными технологиями (ИТ).

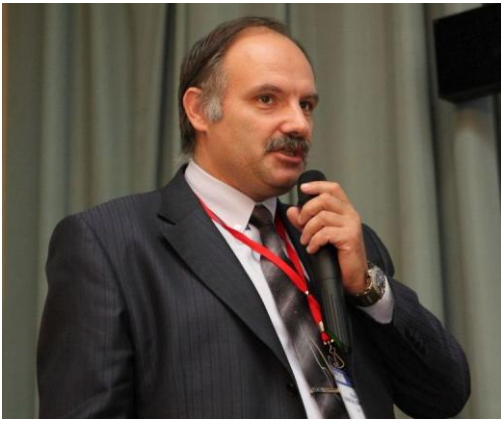

Рис. 11. Выступление Ильи Трифаленкова (Российская Федерация).

Сегодня зависимость деятельности любой организации от информационных технологий (ИТ) достаточно велика, причем чем больше организация, тем теснее ее основные процессы деятельности сращиваются с ИТ. При этом, с одной стороны, ИТ-риски становятся критичными, с другой стороны, их минимизация представляет собой сложную задачу. Проблема усугубляется еще и тем, что по сути дела большие информационные системы, как правило, собраны из нескольких систем, каждая из которых исторически создавалась в разных условиях и по различным требованиям. Кроме того, часть систем может иметь иного собственника и проводить собственную политику. Чтобы в таких условиях обеспечить требуемый доказательный уровень рисков или уровень защищенности, практически единственным способом является привязка рисков и мер противодействия им не к системам и ресурсам, а к процессам деятельности. Сегодня такой подход с

точки зрения реализации базируется, с одной стороны, на наборе международных стандартов семейства ISO27000, с другой стороны, на сквозных механизмах обеспечения безопасности, таких, как управление инцидентами, управление идентификацией, управление непрерывностью функционирования.

Доклад ***Антонио Мана*** (*Университет Малаги, Испания*) «*Поддерживающая расширение инфраструктура для раннего обнаружения и реагирования на проблемы безопасности*» (рис. 12) был посвящен рассмотрению инфраструктуры *EvolutionIST*, предназначенной для мониторинга распределенной информации с соблюдением конфиденциальности информации каждой системы, входящей в эту инфраструктуру.

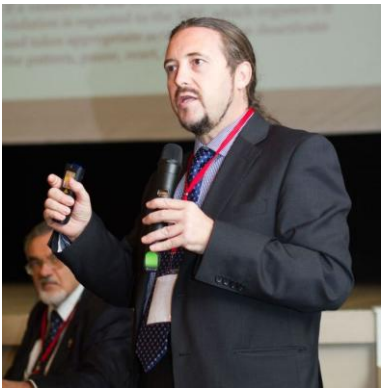

Рис. 12. Выступление Антонио Мана (Испания).

Такая инфраструктура может быть использована на глобальном уровне в целях повышения безопасности, позволяя системам реагировать на атаки, ошибки и т.д. до возникновения серьезных последствий. Предложенная инфраструктура позволяет осуществлять мониторинг информации, подвергающейся распределенной обработке, с соблюдением конфиденциальности каждой входящей в инфраструктуру системы, допуская при этом новые действия по мониторингу в интересах как разработчиков, так и конечных пользователей. Одним из главных преимуществ этой инфраструктуры является то, что атаки на одну из платформ и выполняемые на ней программные элементы генерируют

полезную информацию для расширения этих систем, а также помогают защитить другие системы.

Михаил Вус (*СПИИРАН, Российская Федерация*) в докладе «*О сотрудничестве государств-участников СНГ в вопросах обеспечения информационной безопасности*» (рис. 13) рассмотрел итоги 6-го Евразийского форума «Международные проблемы информационного взаимодействия и информационной безопасности», основными темами которого стали вопросы противодействия международному терроризму и социальной ответственности за Интернет.

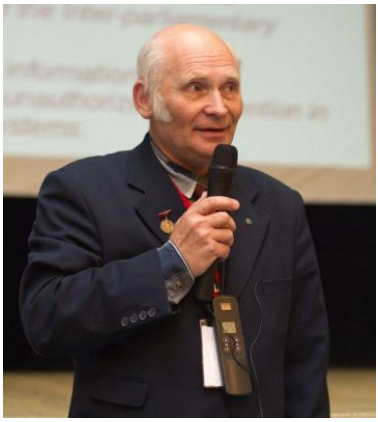

Рис. 13. Выступление Михаила Вуса (Российская Федерация).

Кроме того, были рассмотрены документы и решения 11-го заседания Комиссии по информационной безопасности при Координационном совете государств-участников СНГ по информационной безопасности при Региональном содружестве в области связи. Принятые решения направлены на создание в рамках государств-участников СНГ Центра по обеспечению безопасности в киберпространстве, интернационализации управления глобальной сетью Интернет и о юридической защите межграничного обмена информацией. Приоритетными задачами Центра являются создание объединенного банка инцидентных данных как международной автоматизированной информационной системы коллективного доступа и развитие проектов, представляющих общие стандарты, процедуры и правила реакции на инциденты в киберпространстве. Также была обсуждена

Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности.

Алексей Кириченко (*F-Secure, Финляндия*) в докладе «*Инициативы и деятельность в сфере информационной безопасности: перспективы в Финляндии*» (рис. 14) обсудил последние актуальные события в области информационной безопасности в Финляндии на национальном уровне и роль правительства, промышленности и научных кругов. Среди других вопросов рассматривалось место информационной безопасности в рамках национальных программ научных исследований и связанные с ними определенные проблемы.

Рис. 14. Выступление Алексея Кириченко (Финляндия).

Доклад ***Александра Писемского*** (*Group-IB, Российская Федерация*) «*Киберпреступность в сети Интернет. Практический опыт борьбы и расследований*» (рис. 15) был посвящен развитию киберпреступности в России и существующей практике расследования схем компьютерных преступлений. Обосновывалось утверждение, что специалистам в области безопасности необходимо знать данные схемы, чтобы уже сейчас иметь возможность строить системы информационной безопасности с учетом новых реалий. Описывались новые методы совершения преступлений и монетизации средств, полученных преступным путем. Рассматривались следующие типы преступлений: мошенничество в системах Интернет-банкинга, атаки DoS и бот-сети, фишинговые атаки. Приводились примеры, собранные компанией Group-IB в реальных расследованиях.

Рис. 15. Выступление Александра Писемского (Российская Федерация).

В докладе ***Раджива Шори*** (*Университет «Национальный институт информационных технологий», Индия*) «*Кибербезопасность: ключевые проблемы и совместные решения*» (рис. 16) обсуждались совместные усилия по обеспечению кибербезопасности как с точки зрения глобальной перспективы, так и с позиции состояния кибербезопасности в Индии, на примере которой было показано, что в последние годы потребность в обеспечении кибербезопасности резко возросла. Сегодня поставщики услуг, частные учреждения и государственные организации сталкиваются с множеством проблем по сохранению работоспособности своих сетей. Несколько организаций стали мишенями сложных и разрушительных атак, а также целями для не являющегося вредоносным, но нежелательного трафика, такого, как спам. С появлением новых услуг и приложений неотъемлемой частью повседневной деятельности по поддержке функционирования сетей стали новые типы атак и новые модели поведения.

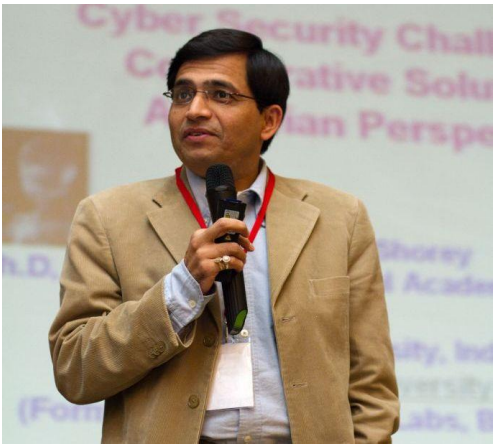

Рис. 16. Выступление Раджива Шори (Индия).

В докладе было показано, что сетевой мониторинг и решения по сетевой защите должны быть простыми, динамичными, гибкими и экономически эффективными. Во множестве случаев вновь предложенные решения рискуют устареть еще до развертывания. С учетом множества подобных аспектов организациям сегодня необходимы эффективные инструменты и политики, которые делают возможным управление и защиту гетерогенных сетей.

Игорь Котенко (*СПИИРАН, Российская Федерация*) в докладе «*Исследовательский анализ атак бот–армий и защиты от них*» (рис. 17) предложил подход к исследованию различных видов бот-сетей и механизмов защиты от них на основе кооперации различных механизмов защиты (используемых различными поставщиками услуг Интернета и организациями) с возможностями к адаптации и самообучению. Подход базируется на использовании иерархии макро- и микроуровневых моделей бот-сетей и механизмов защиты от них (аналитических, основанных на имитации сетевых пакетов, базирующихся на эмуляции), а также реальных сетей (имитационных стендов) небольшого размера. Предполагается, что в контексте ведения киберконфликтов предлагаемый подход и разрабатываемый инструментарий моделирования и эмуляции могут использоваться для анализа текущих и будущих сетевых атак и механизмов защиты, «проигрывания» сце-

нариев кибератак и киберзащиты, а также применяться для расследований инцидентов, связанных с использованием бот-сетей и сетевых атак.

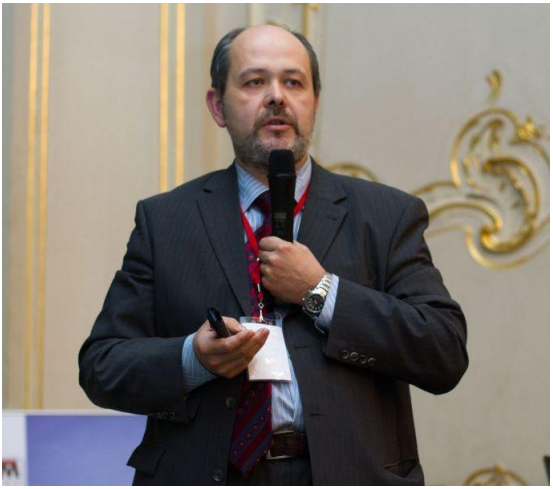

Рис. 17. Выступление Игоря Котенко (Российская Федерация).

3. Панельная дискуссия. На семинаре была проведена панельная дискуссия, посвященная обсуждению форм международного взаимодействия по предупреждению, обнаружению и реагированию на кибервторжения и атаки. В панельной дискуссии приняли участие: В. Скормин (США) — ведущий дискуссии, С. Бажин (Россия), М. Вус (Россия), П. Зегжда (Россия), П. Лосиевич (США), А. Мана (Испания), А. Писемский (Россия), Р. Сандху (США), И. Трифаленков (Россия), Ш.-К. Чин (США) и Р. Шори (Индия).

4. Заключение. Важной особенностью международного семинара стало акцентирование внимания на следующем:

— теоретических аспектах кибербезопасности;

— практических решениях, которые могут найти широкое применение для обнаружения и реагирования на атаки и вторжения в киберпространстве;

— международном сотрудничестве по противодействию киберпреступности и кибертерроризму.

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

Информацию по данному семинару можно найти на веб-странице *http://www.comsec.spb.ru/saps4cs10/.*

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 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, 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, 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 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, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Юсупов Рафаэль Мидхатович — член-корреспондент РАН, д-р техн. наук, профессор, 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, 14-th 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 Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010).**

В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на Международном семинаре «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010), проходившем в Санкт-Петербурге 11 сентября 2010 г.

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 ведущих зарубежных ученых выступили В. Скормин (США), П. Лосиевич (США), Ш.-К. Чин (США), Р. Сандху (США), А. Мана (Испания), А. Кириченко (Финляндия) и Р. Шори (Индия). Среди российских ученых выступили А. Азарсков, Р. Юсупов, П. Зегжда, С. Бажин, И. Трифаленков, М. Вус, А. Писемский 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 форм международного взаимодействия по предупреждению, обнаружению и реагированию на кибер-вторжения и атаки.

Важной особенностью международного семинара явилось, с одной стороны, акцентирование внимания на теоретических аспектах кибербезопасности, а с другой, — на практических решениях, которые могут найти широкое применение для обнаружения и реагирования на атаки и вторжения в киберпространстве, и 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 мнению участников семинара, было решено продолжить его проведение в будущем.

SUMMARY

Kotenko I.V., Saenko I.B., Yusupov R.M. **Analytical review of the reports of the International Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA&PS4CS 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 Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA & PS4CS 2010), held in St. Petersburg on Sept. 11, 2010.

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), P. Losievich (USA), Sh.-K. Chin (USA), R. Sandhu (USA), A. Manna (Spain), A. Kirichenko (Finland) and R. Shorey (India). The following Russian specialists were invited: A. Azarskov, R. Yusupov, P. Zegzhda, S. Bazhin, I. Trifalenkov, M. Vus, A. Pisemskiy 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, on the one hand, the focus on theoretical aspects of cyber security, and the other — on practical solutions that can be widely used to detect and respond to attacks and intrusions in cyberspace, and 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.