ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ № 4(8), 2011, с. 17–31

УДК 004.042

Ю. Г. Емельянова, В. П. Фраленко

Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления

Аннотация. Проведен обзор деятельности национальных и международных организаций в области стандартизации систем защиты облачных сред. Выполнен анализ наиболее значимых исследований и патентов. Рассмотрены проблемы и уязвимости систем облачных вычислений и представлены предложения по созданию экспериментального образца интеллектуальной системы защиты от атак.

Ключевые слова и фразы: облачные вычисления, сетевая атака, защита, стандартизация, патент.

Введение

«Облачные вычисления» (cloud computing) являются инновационной технологией, предоставляющей динамично масштабируемые вычислительные ресурсы и приложения посредством интернет-сервисов под управлением поставщика услуг с оплатой за реально полученные услуги или ресурсы. «Облачные вычисления» становятся все более популярными, особенно в последнее время, когда ограниченность финансовых ресурсов вынуждает компании оптимизировать затраты: не надо тратить огромные средства на создание собственных центров обработки данных, на оплату лицензионного программного обеспечения, на содержание квалифицированного персонала. Вы просто можете автоматизировать все ИТ-процессы, купив готовые пакеты SaaS, DaaS, IaaS или PaaS. Однако возникают некоторые сомнения в безопасности этих решений, в частности, вопросы по защищенности от сетевых атак. В связи с этим ведущие компании-разработчики программного обеспечения направили свои усилия на создание средств

защиты сред облачных вычислений. Национальные и международные организации, лидирующие в области разработки стандартов, ведут серьезную работу. В настоящей статье проведен анализ проблем уязвимости систем облачных вычислений, национальных и международных стандартов по оригинальным источникам, даны предложения по созданию системы обнаружения и предотвращения сетевых атак на облачные вычисления.

1. Проблемы и уязвимости систем облачных вычислений

Бурное развитие облачных сред повлекло множество новых проблем, среди которых можно выделить следующие:

- Потеря клиентов. По причине значительного притока пользователей сервисов, использующих облачные вычисления (например, Flickr или Amazon), растет вероятность потери клиентов из-за наличия утечек информации с подобных ресурсов. Так, например, в 2009 году сервис для хранения закладок Magnolia потерял все свои данные, в результате чего часть клиентов покинула сервис [1].
- Отсутствие принятого большей частью рынка стандарта обеспечения безопасности облачных вычислений. Несмотря на существование разных сертификационных процедур и тестов, базирующихся на критериях и требованиях безопасности, единого подхода и методики для обеспечения защищенности облачных вычислений пока нет, нет и единой методики проверки адекватности защиты провайдера подобных сервисов.
- Ограничения модели безопасности. Традиционная модель безопасности предприятия основывается на сети брандмауэров и шлюзов. Тем не менее, соглашения об использовании некоторых провайдеров (к примеру, для служб Amazon EC2) напрямую запрещают сканирование на наличие уязвимостей [2].
- По мере того как возрастает число предприятий и организаций, перешедших на веб-службы, попытки внедрения в веб-службы и нарушения их работы становятся все более изощренными. Можно перечислить следующие уязвимости [3]:
  - Уязвимость программного обеспечения элементов облака. Угроза реализуется злоумышленниками при помощи использования уязвимостей в операционных системах, сетевых сервисах и т.д. Например, серверы баз данных могут быть атакованы методом SQL-инъекции. Успешная реализация любой

подобной атаки предоставит злоумышленнику доступ к данным системы или нарушит ее функциональность.

– Уязвимость сетевой инфраструктуры облака. Этот вид уязвимости связан с распределенной архитектурой облака и общим принципом безопасности, в соответствии с которым защищенность системы определяется защищенностью ее самого слабого звена. Успешная DoS-атака на один из компонентов сети может заблокировать доступ ко всей системе несмотря на то, что остальные связи между компонентами системы не будут нарушены.
– Наличие атак на систему виртуализации. Для объединения и координации различных узлов облака используются виртуальные среды, поэтому атаки на систему виртуализации, исходящие от пользовательских задач, выполняющихся в облаке, угрожают всему облаку в целом. Этот тип угроз является специфическим для систем облачных вычислений. Уязвимости в различных средствах виртуализации, таких как Xen, VMware, Microsoft Virtual Server, могут привести к компрометации всей системы.
– Наличие атак на клиентов облака. Клиенты работают с сервисом облачных вычислений с помощью Интернет-браузера, поэтому традиционные атаки на клиентов WEB-приложений, такие как Cross Site Scripting (XSS), перехваты веб-сессий, кража паролей, атаки «человека посредине», являются актуальными для систем облачных вычислений.
– Комплексные угрозы системам облачных вычислений. Обеспечение безопасности в процессе контроля работы всех узлов облака и управления ими также является тонким местом в защите систем облачных вычислений. Нарушитель может поставить своей целью использовать облако для решения своих задач и внести искажения в оценку ресурсов облака, управление виртуальными машинами и конфигурацию системы. Этот тип угроз также специфичен для облачных вычислений и связан с возможностью злоупотреблений, которые могут привести к тому, что вычислительная мощь облака и его ресурсы будут работать в интересах нарушителя.

2. Деятельность национальных и международных организаций в области стандартизации систем защиты облачных сред

Cloud Standards Summit [4] официально существует с 13 июля 2009 года. Инициатором объединения усилий по стандартизации облачных вычислений и хранения данных выступила рабочая группа Object Management Group (OMG), занимающаяся разработкой и продвижением объектно-ориентированных технологий и стандартов. Целью является развитие информационных технологий и согласование стандартов по проблемам удаленных государственных облачных сред (Coordinating Standardization Activities to Remove Government Cloud Computing Roadblocks) [5]. Созданы следующие рабочие группы:

- Cloud Security Alliance (CSA),
- Distributed Management Task Force (DMTF),
- Storage Networking Industry Association (SNIA),
- Open Grid Forum (OGF),
- Open Cloud Consortium (OCC),
- Organization for the Advancement of Structured Information Standards (OASIS),
- TM Forum,
- Internet Engineering Task Force (IETF),
- International Telecommunications Union (ITU),
- European Telecommunications Standards Institute (ETSI),
- Object Management Group (OMG).

Наиболее известны достижения CSA [6] и OASIS [7], а так же организации Open Data Center Alliance [8] и Национального института стандартов и технологий (NIST) [9]. **CSA** — некоммерческая организация, созданная с целью продвижения передового опыта в области обеспечения безопасности облачных вычислений, а также для повышения уровня осведомленности по данной тематике всех заинтересованных сторон. CSA выделяет для себя целый ряд задач для облачных сред, среди которых:

- поддержка взаимоотношений потребителей и поставщиков услуг в части требований безопасности и контроля качества,
- независимые исследования в части защиты,
- разработка и проведение программ повышения осведомленности и обеспечению безопасности,

- разработка руководств и методических рекомендаций по обеспечению безопасности.

Руководство по безопасности критических областей в фокусе «облачных вычислений» (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1) покрывает основные аспекты и дает рекомендации потребителям сред облачных вычислений в 13 стратегически важных областях:

(1) архитектурные решения сред облачных вычислений;
(2) государственное и корпоративное управление рисками;
(3) легальное и электронное открытие;
(4) соответствие техническим условиям и отчетность;
(5) управление жизненным циклом информации;
(6) портативность и совместимость;
(7) традиционная безопасность, непрерывность деятельности и восстановление в аварийных ситуациях;
(8) работа центра обработки данных;
(9) реакция на риски, уведомление и коррекционное обучение;
(10) прикладная безопасность;
(11) криптография и управление ключами;
(12) идентификация и управление доступом;
(13) виртуализация.

OASIS стимулирует развитие, сведение и принятие открытых стандартов для глобального информационного общества. Являясь источником многих современных основополагающих стандартов, организация видит облачные вычисления как естественное расширение сервисноориентированной архитектуры и моделей управления сетью. Технические агенты OASIS — это набор участников, многие из которых активно участвуют в построении моделей облаков, профилей и расширений на существующие стандарты. Примерами стандартов, разработанных в области политик безопасности, доступа и идентификации, являются OASIS SAML, XACML, SPML, WS-SecurityPolicy, WS-Trust, WS-Federation, KMIP и ORMS. Организация **Open Data**

Center Alliance объявила о публикации двух «моделей использования» (usage models), призванных снять наиболее значимые препятствия на пути внедрения облачных вычислений. Первая модель использования называется «Обеспечение безопасности на стороне провайдера» (The Provider Security Assurance). В ней описаны требования к гранулированному описанию элементов обеспечения безопасности, которые должны предоставить поставщики услуг. Модель использования «Мониторинг соответствия требованиям безопасности» (The Security Monitoring) описывает требования к элементам, которые обеспечивают возможность мониторинга безопасности облачных сервисов в реальном времени [10]. В совокупности две модели использования формируют набор требований, который может стать основой для создания стандартной модели обеспечения безопасности облачных сервисов и осуществления мониторинга этих сервисов в реальном времени. **National Institute of Standards and Technology (NIST)** — Национальный Институт стандартов и технологий вместе с Американским национальным институтом стандартов (ANSI) участвует в разработке стандартов и спецификаций к программным решениям, используемым как в государственном секторе США, так и имеющим коммерческое применение. Сотрудники NIST разрабатывают руководства, направленные на описание архитектуры облака, безопасность и стратегии использования, в числе которых руководство по системам обнаружения и предотвращения вторжений, руководство по безопасности и защите персональных данных при использовании публичных систем облачных вычислений. В руководстве по системам обнаружения и предотвращения вторжений (NIST Guide to Intrusion Detection and Prevention Systems (IDPS)) даются характеристики технологий IDPS и рекомендации по их проектированию, внедрению, настройке, обслуживанию, мониторингу и поддержке. Виды технологий IDPS различаются в основном по типам событий, за которыми проводится наблюдение, и по способам их применения. Рассмотрены следующие четыре типа IDPS-технологий: сетевые, беспроводные, анализирующие поведение сети и централизованные. В руководстве по безопасности и защите персональных данных при использовании публичных систем облачных вычислений (Guidelines on Security and Privacy in Public Cloud Computing) в том числе дается обзор проблем безопасности и конфиденциальности, имеющих отношение к среде облачных вычислений: обнаружение атак на гипервизор, цели атак, отдельно рассматриваются распределенные сетевые атаки.

3. Краткий анализ состояния исследований

Рост количества целенаправленных атак на корпоративные инфраструктуры, интегрирующие облачные среды, требует четко продуманной стратегии объединения технологий информационной защиты. Одним из действенных подходов является использование средств управления инцидентами и событиями информационной безопасности. Активные работы в области защиты систем облачных вычислений от атак ведутся такими крупными компаниями как Intel, IBM, HP, Sun, Cisco и Symantec. Остановимся на некоторых наиболее значимых исследованиях.

(1) Компания Intel для организации облачных серверов предлагает решение под названием Cloud-in-a-Box [11]. Оно представляет собой миниатюрный сервер для облачных вычислений. Безопасность здесь достигается за счет нескольких механизмов:
   (a) набор команд Intel Advanced Encryption Standard New Instruction (AES-NI) повышает скорость шифрования и расшифровки данных в различных приложениях и при решении различных задач;
   (b) технология Intel Trusted Execution Technology (Intel TXT) на процессорном уровне следит, чтобы серверное оборудование не было скопировано на уровне гипервизора или ниже;
   (c) технология Intelligent Power Node Manager, позволяет увеличить операционную эффективность сервера путем повышения плотности размещения.

   Система Intel Cloud-in-a-Box входит в концепцию Cloud 2015 Vision. Она подразумевает, что облачные дата-центры интегрированы в едином окружении и функционируют автоматически, предоставляя безопасный доступ и оптимальную работу на широком ряде устройств, от смартфонов до ноутбуков. Для реализации этой концепции в Intel считают необходимым внедрение открытых и взаимозаменяемых стандартов. Компания McAfee, дочернее предприятие Intel, разработала продукт Cloud Security Platform [12] — новый подход к обеспечению безопасности облачных технологий, представляющий собой методологию обеспечения безопасной циркуляции информации между корпоративной сетью и облаком, которая включает следующие компоненты:
   - Web Security — обеспечивает двунаправленную защиту http-трафика;

- Mobile Security — обеспечивает защиту мобильных устройств с помощью anti-malware и корпоративных политик фильтрации веб-трафика;
- Cloud Access Control — обеспечивает комплексный контроль доступа к приложениям, которые размещаются в облаке, с использованием корпоративных атрибутов доступа;
- Email Security — обеспечивает полную защиту почты, интегрированную с системой защиты от утечки информации для исходящего трафика.

Каждый из модулей может быть внедрен как устройство, виртуальное устройство или как сервис из облака (Software as a Service) независимо от способа внедрения любого другого модуля.

(2) Компания Symantec разработала программный комплекс Symantec Endpoint Protection 12, ориентированный на обнаружение и блокирование сложнейших угроз. Комплекс использует технологию Insight, которая анализирует анонимные данные о распространении программ более чем на 175 миллионах компьютеров клиентов и автоматически присваивает высокоточные рейтинги безопасности более чем 2,5 миллиардам уникальных файлов. Технология Insight помогает блокировать новые неизвестные угрозы, упущенные другими защитными системами. Блокируя потенциально опасные файлы с плохой репутацией от попадания в сеть организации, пакет Symantec Endpoint Protection служит первой линией защиты. Компания Symantec продолжает тесно сотрудничать с компанией VMware для полного использования всех возможностей виртуализации и самодиагностики, заложенных в технологии VMware vShield$^{\text{TM}}$, а пакет Symantec Endpoint Protection 12 является первым шагом на пути оптимизации виртуальных и «облачных» сред. Пакет Symantec Endpoint Protection обнаруживает больше угроз, чем средства безопасности для виртуальных сред от McAfee или Trend Micro [13, 14].

(3) Компания Cisco предлагает следующие технологии обеспечения облачной сетевой безопасности [15]:

- Cisco ScanSafe Web Intelligence Reporting — позволяет предприятию видеть, как используются его веб-ресурсы, и предотвращать отрицательное воздействие второстепенного трафика, не связанного с бизнесом, на критически важные деловые приложения. Работа сетей отслеживается по 87 различным

параметрам, в том числе по словам, используемым для сетевого поиска, и полосе пропускания, занимаемой каждым сотрудником в тот или иной момент времени. Четкое определение типов входящего и исходящего сетевого трафика дает компании уверенность в том, что ее корпоративная информация находится в безопасности, а вредоносные программы и неуместный контент надежно блокируются.

- Cisco IPS Sensor для систем предотвращения вторжений — накапливает глобальные сведения об угрозах, поступающих от большого количества устройств безопасности, и преобразует их в формат динамических обновлений интеллектуальных данных, чтобы впоследствии использовать эти данные в инфраструктуре безопасности корпоративной сети для реализации соответствующих мер защиты. Использование технологии глобальной корреляции позволило почти вдвое повысить эффективность Cisco IPS 7.0 при остановке атак злоумышленников в более короткий срок по сравнению с традиционными технологиями IPS, в которых используются только сигнатуры.

(4) Корпорация IBM в 2011 году представила аппаратно-программный комплекс IBM Network Intrusion Protection System GX7800, предоставляющий организациям возможность защиты своих данных и инфраструктуры от неавторизованного доступа и атак без ущерба для производительности и готовности важнейших бизнес-приложений. В частности, это устройство:

- предоставляет организациям полный комплекс средств обеспечения безопасности, таких как защита web-приложений, без снижения пропускной способности сети;
- распространяет средства обеспечения безопасности на облачные среды для защиты данных;
- использует результаты исследований службы IBM X-Force, помогая компаниям заблаговременно защищаться от угроз.

Эти средства дополняют функциональность традиционных систем IPS такими новыми возможностями, как защита web-приложений, предотвращение потерь данных и технология Virtual Patch, которые могут выполняться одновременно для повышения уровней безопасности [16].

(5) Компания HP на конференции HP DISCOVER (2011, июнь, Лас-Вегас, США) представила архитектуру и семейство решений HP

CloudSystem для развертывания облачных сервисов всех типов в составе частных, публичных и гибридных облаков. В качестве расширений для поставляемых пакетов предлагаются решения по безопасности для физических и виртуальных доменов, обеспечивающие бесшовную безопасность против угроз/нападений на дата-центр, включая гипервизор. С помощью услуги по анализу безопасности облачной среды HP Cloud Security Analysis Service можно проверить уровень защиты облачной инфраструктуры, платформ и приложений. Решение HP Secure Advantage предлагает портфель унифицированных, интегрированных средств, помогающих управлять рисками, защищать критически важную инфраструктуру и обеспечивать высокую доступность сервисов. HP анонсировала два новых сервиса по обеспечению безопасности в облачных средах, направленных на снижение рисков появления уязвимостей и позволяющих избежать высоких расходов, связанных с их устранением. Платформа HP CloudSystem поддерживает многочисленные механизмы защиты, включая идентификацию и аутентификацию, управление доступом, авторизацию и аудит, а также использование безопасных протоколов связи. На настоящий момент вопросы информационной безопасности в составе HP CloudSystem в полной мере могут решаться только с использованием разработок других компаний [17].

Патенты в данной предметной области можно классифицировать по трем категориям:

(1) средства обнаружения и предотвращения распределенных сетевых атак на нераспределенные системы, в том числе патенты на динамическую защиту и идентификацию атак, повышение автоматизации:
   (a) US 8,006,285;
   (b) US 7,921,462;
   (c) WO/2007/142813 и др.;
(2) системы обеспечения безопасности на основе облачных сред, в том числе патенты на облачные брандмауэры, механизмы ограничения использования ресурсов и валидации приложений, построение виртуальных каналов межсетевого взаимодействия, системы агентов наблюдения и облачные антивирусы:
   (a) WO/2011/072289;
   (b) WO/2008/077150;
   (c) US 8,010,085;

(d) WO/2011/010823;
(e) US 2011083179 (A1);
(f) CN 101827104 (A) и др.;

(3) системы, предназначенные для обеспечения безопасности облачных сред, в том числе: патенты на построение архитектур и серверов безопасности; системы эффективной обработки запросов и поддержки обнаружения атак; системы управления доступом и предоставления средств безопасности; методы, устройства и средства для безопасного использования сетевых ресурсов:
(a) WO/2007/015254;
(b) US 2007039053;
(c) US 6,847,995;
(d) WO/2010/030380;
(e) WO/2010/025805;
(f) WO/2005/107204;
(g) US 2011219434 (A1);
(h) US 2011072489 (A1) и др.

Из проведенного обзора можно сделать следующие выводы:

(1) во всем мире наблюдается повышенный интерес к проблеме защиты систем облачных вычислений, связанный с ростом их популярности и одновременным увеличением потока атак, ведущих к большим материальным потерям;
(2) существует достаточно много зарубежных систем, так или иначе классифицирующих сетевые потоки данных и выявляющих атаки на системы облачных вычислений, причем патентуются как методы и концепции выявления аномальных сетевых потоков данных, так и большие распределенные системы обнаружения вторжений, для которых выявление аномальной активности является только одной из мер защиты;
(3) в результате патентного поиска не было найдено запатентованных инструментов обнаружения/предотвращения распределенных атак на распределенные/облачные среды, что позволяет говорить о новизне проводимого исследования;
(4) практически отсутствуют отечественные промышленные разработки в области защиты систем облачных вычислений, что вынуждает покупать дорогостоящие зарубежные программные продукты с закрытой функциональностью, на которые даже отсутствуют ключевые патенты.

Сказанное определяет актуальность создания эффективной отечественной технологии. Ниже представлены некоторые особенности интеллектуальной системы автоматизированного обнаружения и предотвращения распределенных сетевых атак на облачные вычисления, разрабатываемой в ИПС им. А.К.Айламазяна РАН.

4. Предложения по созданию экспериментального образца интеллектуальной системы защиты от атак

Разрабатываемый экспериментальный образец интеллектуальной программной системы (ЭО ИПС) защиты систем облачных вычислений от атак содержит:

(1) Программные сенсоры сбора информации о пакетах данных, циркулирующих в сети, на основе библиотеки libpcap (осуществляет собственно перехват пакетов), в качестве базовой программной системы может быть использована хорошо зарекомендовавшая себя система обнаружения и предупреждения вторжений Snort [18].

(2) Блок анализа ситуаций, использующий информацию от программных сетевых сенсоров и базы знаний системы, состоящий из модуля корреляционного анализа и модуля принятия решения на основе методов искусственного интеллекта; предназначен для обработки собранных сенсорами данных с целью обнаружения информационных атак и вторжений.

(3) Модуль реакции на обнаруженные атаки и вторжения, осуществляющий оперативное реагирование на возникшие угрозы (сетевые атаки, вирусная активность и пр.) согласно профилю сетевой безопасности (отсылка уведомлений в графический интерфейс визуализации обнаруженных атак и вторжений, информирование ответственных лиц по электронной почте, SMS и др.).

(4) Модуль управления компонентами средств обнаружения атак, который представляет собой графический интерфейс для визуализации обнаруженных атак и вторжений, и управления функционированием ЭО ИПС обнаружения и предотвращения распределенных сетевых атак.

(5) Модуль хранения, основанный на системе управления базами данных, который позволяет обеспечить доступ модулей ЭО ИПС к целевой информации: истории обнаружения сетевых атак, базе настроек и профилей безопасности, обучающей выборке и др.

Впервые будет разработан и реализован программный комплекс нейросетевого мониторинга сетевых атак на системы облачных вычислений с включением конвейерно-параллельной обработки. В качестве основных алгоритмов классификации предлагается использовать многослойные сети прямого распространения, ИНС Кохонена, полиномиальное расстояние Евклида-Махаланобиса и метод опорных векторов. База данных сетевых атак KDD-99 [19] предполагается в качестве обучающей выборки для машинного обучения ИНС и других механизмов выявления аномального поведения сети. Развитие исследований основывается на полученных ранее результатах ИПС им. А.К.Айламазяна РАН в области защиты компьютерных систем от сетевых атак [20–24].

5. Заключение

Проведенный обзор показал актуальность проведения новых работ в области защиты облачных вычислений. Возможности разрабатываемой интеллектуальной системы автоматизированного обнаружения и предотвращения распределенных сетевых атак на облачные вычисления позволят повысить уровень информационной безопасности как имеющихся, так и перспективных корпоративных инфраструктур, интегрирующих облачные среды. Исследования проводятся в рамках работ по Государственному контракту № 07.514.11.4048 по теме «Разработка интеллектуальных методов автоматизированного обнаружения и предотвращения распределенных сетевых атак и их реализация в современных системах облачных вычислений» (шифр заявки «2011–1.4–514–017–004»).

Список литературы

[1] GDV Data Protection Blog, URL: http://www.globaldatavault.com/blog/for-magnolia-not-so-well-done/. ↑1

[2] Материалы WindowSecurity.com, URL: http://www.windowsecurity.com/search.asp?s=cloud. ↑1

[3] Зегжда Д. П., Ивашко А. М. *Как построить защищенную информационную систему* — СПб : Мир и семья, 1997 ISBN 5-88857-010X, с. 312 ↑1

[4] Press Release. Major Standards Development Organizations Collaborate to Further Adoption of Cloud Standards, URL: http://cloud-standards.org/wiki/index.php?title=Press_Release. ↑2

[5] Cloud Standards Summit. OMG Standards in Government & NGO's Workshop, URL: http://www.omg.org/news/meetings/GOV-WS/css/index.htm. ↑2

[6] Cloud Security Alliance, URL: https://cloudsecurityalliance.org/. ↑2

[7] Organization for the Advancement of Structured Information Standards, URL: http://www.oasis-open.org/org/. ↑2

[8] Open Data Center Alliance, URL: http://www.opendatacenteralliance.org/. ↑2

[9] National Institute of Standards and Technology, URL: http://www.nist.go/. ↑2

[10] CNews Cloud. Опубликованы два документа, направленных на стандартизацию облачной безопасности, URL: http://cloud.cnews.ru/news/line/index.shtml?2011/06/09/443475. ↑2

[11] Cloud-in-a-Box, URL: http://newsroom.intel.com/docs/DOC-2194. ↑1

[12] Cloud Security Platform, URL: http://itnews.com.ua/60064.html. ↑1

[13] Virtual desktop malware defence, URL: http://www.dennistechnologylabs.com/reports/security/anti-malware/symantec/DTL_SYM_VDI.pdf. ↑2

[14] Symantec Endpoint Protection 12.1, URL: URL: http://www.symantec.com/content/ru/ru/enterprise/fact_sheets/ru-Symantec_Endpoint_Protection_SEP_Datasheet.pdf. ↑2

[15] Cisco выпустила решения для обеспечения безопасности cloud-сервисов, URL: http://www.securitylab.ru/news/378170.php. ↑3

[16] IBM Security NetworkIntrusion Prevention System, URL: http://public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/WGD03002USEN.PDF. ↑4

[17] Облачные сервисы на платформе HP CloudSystem, URL: http://storagenews.ru/46/HP_CloudService_46.pdf. ↑5

[18] Русская группа пользователей Snort, URL: http://www.snortgroup.ru/. ↑1

[19] Fifth ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. ↑4

[20] Фраленко В. П. *Нейросетевое шифрование с применением архитектуры «кодер/декодер»* // Нейрокомпьютеры: разработка и применение, 2010, № 5, с. 11–16 ↑4

[21] Фраленко В. П. *Нейросетевая технология обнаружения сетевых атак на информационные ресурсы* // III Всероссийская научно-техническая конференция «Актуальные проблемы ракетно-космического приборостроения и информационных технологий». — Москва : Изд-во Радиотехника, 2011 ISBN 978–5–88070–299–2, с. 479–488 ↑

[22] Свидетельство о государственной регистрации программы для ЭВМ №2011611277, Модуль мониторинга аномальной сетевой активности на основе искусственных нейронных сетей — «Эгида-НС». ↑

[23] Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. *Нейросетевая технология обнаружения сетевых атак на информационные ресурсы* // Программные системы: теория и приложения, 2011. **2**, № 3(7), с. 3–15, URL: http://psta.psiras.ru/read/psta2011_3_3-15.pdf ↑

[24] Талалаев А. А., Тищенко И. П., Хачумов В. М., Фраленко В. П. *Разработка нейросетевого модуля мониторинга аномальной сетевой активности* // Нейрокомпьютеры: разработка и применение, 2011, № 7, с. 32–38 ↑4

J. G. Emelyanova, V. P. Fralenko. *Problems and prospects analysis for cloud computing network attacks detection and prevention intelligent system creation.*

Abstract. National and international organizations activity in cloud security systems standardization review is performed. Most relevant studies and patents are analyzed. Cloud computing problems and vulnerabilities are disclosed. Concrete proposals on intellectual intrusion defense experimental model are submitted.

Key Words and Phrases: cloud computing, network attack, defense, standardization, patent.

Образец ссылки на статью:

Ю. Г. Емельянова, В. П. Фраленко. *Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления* // Программные системы: теория и приложения : электрон. научн. журн. 2011. № 4(8), с. 17–31. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf