УДК 004.042

Современный уровень и тенденции развития средств обеспечения сетевой безопасности систем облачных вычислений

Ю. Г. Емельянова*, Э. Мбайкоджи†, И. В. Соченков†

* *Федеральное государственное бюджетное учреждение науки*
Институт программных систем им. А.К. Айламазяна РАН
ул. Петра I, 4 «а», село Веськово,
Переславский район, Ярославская область, 152021, Россия

† *Кафедра информационных технологий*
Российский университет дружбы народов
ул. Миклухо-Маклая, 6, г. Москва, Россия, 117198
Федеральное государственное бюджетное
учреждение науки Институт системного анализа РАН (ИСА РАН)
просп. 60-летия Октября, 9, Москва, 117312, Россия

В статье рассмотрен современный уровень исследований в области обеспечения сетевой безопасности облачных вычислительных систем. Проанализированы принципы построения и функционирования систем обеспечения безопасности облачных вычислений, а также систем, использующих облачные вычисления для выявления угроз сетевой безопасности. Изучены современные тенденции в этой области.

Ключевые слова: система облачных вычислений, сетевая безопасность, интеллектуальная собственность, обнаружение угроз, информационная безопасность.

1. Введение

Системы облачных вычислений предоставляют услуги обработки и хранения данных в распределённых вычислительных средах в Интернете. На сегодняшний день существует несколько видов облачных сервисов:

- программное обеспечение как сервис (Software as a Service (SaaS)) [1];
- рабочий стол как сервис (Desktop as a Service) [2];
- платформа как сервис (Platform as a Service (PaaS)) [1];
- инфраструктура как сервис (Infrastructure as a Service (IaaS)) [1];
- коммунальные IT-услуги (Utility Computing (UC)) [3];
- облачные web-провайдеры [3];
- управляемые услуги (Managed Service (MS)) [3].

Различные виды существующих архитектур и сервисов облачных вычислений и хранения данных предоставляют готовое решение для широкого класса пользовательских задач. На рис. 1 приведена многоуровневая схема развертывания и взаимосвязь облачных вычислительных сервисов в соответствии с общепринятой международной классификацией.

Различные виды существующих архитектур и сервисов облачных вычислений и хранения данных предоставляют готовое решение для широкого класса пользовательских задач. Механизмы облачных вычислений и заложенные в них принципы обработки, хранения и доступа к информации являются удобными и выгодными для конечных пользователей. ОВС позволяют снизить требования к аппаратному и программному обеспечению на стороне пользователя, которое необходимо для решения задач. Это позволяет избежать расходов на создание и поддержку собственного центра обработки данных. В свою очередь, владельцы облачных вычислительных систем (ОВС) имеют возможность рационально использовать дорогостоящее оборудование центра обработки данных, предоставляя платный доступ сторонним пользователям к собственным вычислительным мощностям.

Рис. 1. Схема развертывания и взаимосвязь облачных вычислительных сервисов

Направление распределённой обработки информации на основе систем облачных вычислений является активно развивающимся. На существующих мощностях распределённых вычислительных систем (РВС) могут быть решены вычислительно трудоёмкие задачи за приемлемое время. Это объясняет популярность технологии облачных вычислений и в то же время ставит перед исследователями и инженерами ряд задач в области создания, развития и поддержки РВС, включая и задачу обеспечения информационной безопасности облачных вычислительных систем.

ОВС предполагают концентрацию большого объема данных в едином информационном пространстве, доступном многим пользователям Интернета. Это может спровоцировать различные преступления против информационной собственности. При использовании облачных вычислительных систем необходимо обеспечивать информационную безопасность и принимать во внимание потенциальные угрозы. С одной стороны, ОВС могут являться объектом сетевой атаки с целью нарушения их работоспособности (например, распределённой атакой «отказ в обслуживании» — DDoS). С другой стороны, РВС сами могут выступать в роли инструмента, с помощью которого осуществляются атаки на другие сервисы Интернета (например, организация DDoS, распределённый перебор паролей к различным сервисам и др.). В обоих случаях потенциальный ущерб от сетевых атак и вторжений может быть весьма значительным.

У пользователя ОВС, как правило, отсутствуют полные сведения об инфраструктуре, обеспечивающей защиту конфиденциальной информации. Имея собственную ИТ-инфраструктуру, пользователь самостоятельно обеспечивает ее защиту, например, с помощью сетевых фильтров, антивирусного программного обеспечения или путём физического отключения от Интернета — в изолированной локальной вычислительной сети. В противоположность этому, если данные хранятся и обрабатываются во внешней среде, то вопросы безопасности становятся неподконтрольны владельцам данных [4]. В этом случае вся ответственность за выявление угроз, предотвращение и нейтрализацию сетевых атак ложится на владельцев и администраторов распределённых сервисов.

В силу вышесказанного задача обеспечения информационной безопасности облачных вычислительных систем является актуальной и активно исследуемой. Различные решения в этой области активно развиваются, поскольку методы сетевых атак тоже не стоят на месте. ОВС являются, с одной стороны, объектом

защиты от сетевых угроз, с другой стороны, они сами могут выступать в роли программно-аппаратной базы для решения задач выявления сетевых угроз.

2. Средства сетевой защиты систем облачных вычислений

Зачастую основные средства защиты облачных вычислительных систем представляют собой не специализированные инструменты, а классические решения в области сетевой безопасности общего назначения. Они являются подходящим вариантом для инфраструктуры, в которой располагается ОВС, и обеспечивают ей базовый уровень безопасности. Обеспечение безопасности в этом случае реализуется с помощью средств [5]:

- управления и разграничения доступа к системе (физический доступ с консоли, удалённый доступ программно по сети);
- управления и разграничения доступа к данным в приложениях и операционной системе (настройки политики безопасности, прав доступа);
- обеспечения контроля целостности и неизменности программного обеспечения (с помощью средств операционной системы, путём настройки прав доступа, а также антивирусного программного обеспечения);
- криптографической защиты (программы шифрования данных);
- защиты от вторжений извне (сетевые экраны, антивирусное программное обеспечение);
- системы обнаружения вторжений Intrusion-Detection Systems — IDS: программы, выявляющие аномальное поведение вычислительных узлов, отклонения от обычных показателей в сетевом трафике и т.п.);
- протоколирования действий пользователей;
- контроля состояния безопасности системы (программы обнаружения уязвимостей, сканеры портов, эмуляторы известных атак).

Далее рассмотрим наиболее интересные, на наш взгляд, варианты применения вышеуказанных средств в ОВС. В существующих решениях, как правило, сочетается комплекс методов для обеспечения сетевой защиты, учитывающих специфические угрозы и особенности работы РВС.

Одним из базовых средств защиты облачных вычислительных систем является контроль доступа. В зависимости от типов сервисов ОВС и характера задач, решаемых в ней, возможны несколько уровней управления доступом. Самым примитивным является файловый уровень: операционная система устанавливает права для пользователей/групп или формирует списки контроля доступа применительно к каждому файлу системы. Кроме того, в большинстве операционных систем действие процедуры контроля доступа распространяется на процессы и объекты системы. Подобное целевое управление доступом в облачных средах носит базовый и унифицированный характер.

Гораздо более разнообразны методы разграничения доступа на уровне приложений. Предлагаемые механизмы контроля доступа заметно отличаются друг от друга в зависимости от категорий облачных приложений и от конкретных провайдеров [6]. Например, в патенте [7] доступ к сетевым ресурсам контролируется на прикладном уровне через шлюз, имеющий объектно-ориентированную архитектуру обслуживания, основанную на абстрактных интерфейсах прикладного программирования (APIs). Управление доступом осуществляется с помощью логического компонента — обслуживающего контрольного монитора (SRM), который соединен со шлюзом и настроен так, чтобы перехватывать все коммуникации, проходящие между клиентскими приложениями и шлюзом.

Подход, включающий выделенную подсистему обеспечения безопасности, выявления атак и угроз, а также управления правами доступа к данным является достаточно распространённым. Его общая схема приведена на рис. 2.

Методы и система анализа данных, передаваемых в ОВС, на предмет наличия вредоносного содержания предложены в заявке на изобретение [8]. Архитектура

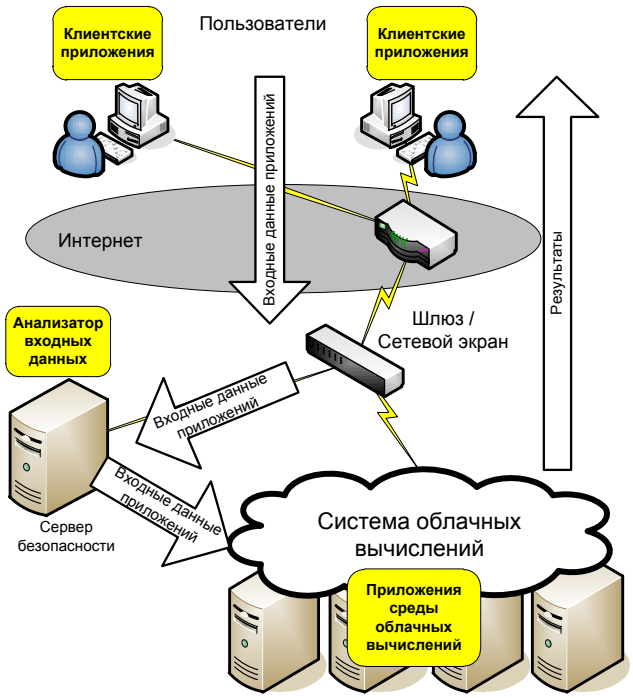

Рис. 2. Схема сетевой защиты системы облачных вычислений от внешних угроз

системы представлена на рис. 3, а общая блок-схема алгоритма её работы представлена на рис. 4. Схожие принципы реализованы в техническом решении, представленном в патенте [9]: компонент безопасности фильтрует клиентские приложения, чтобы предотвратить нежелательное поведение. Например, приложения могут быть ограничены в использовании ресурсов сети, а также проверены и запрещены для исполнения в системе облачных вычислений, чтобы предотвратить выполнение вредоносного кода.

Подсистема обеспечения безопасности, как правило, не только выявляет атаки и угрозы, но и автоматически блокирует их. Так, в патентах [10, 11] описаны принципы анализа и фильтрации пакетов сетевого трафика на предмет выявления DDoS атаки и её блокирования путём отбрасывания пакетов, не предназначенных целевой системе.

Для защиты больших ОВС применяется комплекс сетевых экранов, обеспечивающих фильтрацию данных, поступающих в систему через несколько каналов связи (см., например, патент [12]). Это позволяет распределить нагрузку между различными физическими устройствами, что обеспечивает отказоустойчивость системы, а также расширяет пропускную способность.

Рассматриваемые далее решения обеспечения безопасности ОВС позволяют защитить конфиденциальную информацию на уровне приложений и являются прямой альтернативой системе разграничения доступа на основе файловой инфраструктуры.

Многопользовательское решение для управления идентификационными данными и доступом предлагает компания Novell [13]. Это решение обеспечивает функции контроля доступа к ресурсам в ОВС, аутентификации, авторизации и соблюдения нормативных требований при работе с её сервисами. Все изменения, которые клиенты системы вносят в учетные записи своих пользователей или подразделений, немедленно реплицируются, гарантируя единую среду идентификационных данных и политик безопасности, независимо от того, на каких узлах распределённой системы физически происходят вычисления.

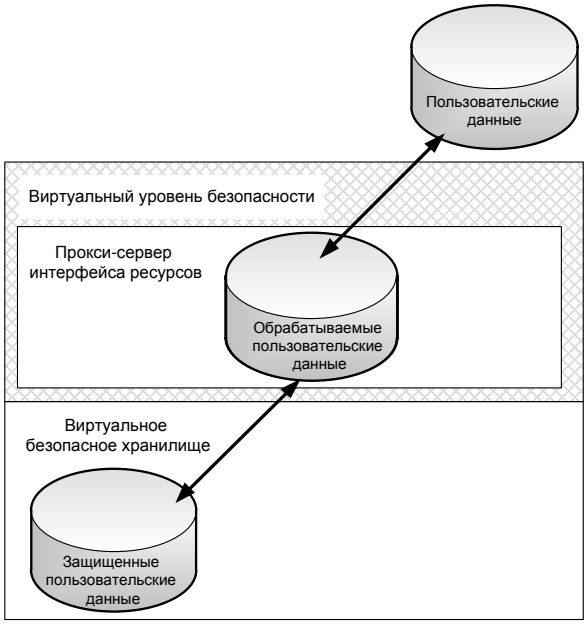

Рис. 3. Архитектура системы защиты облачных вычислений

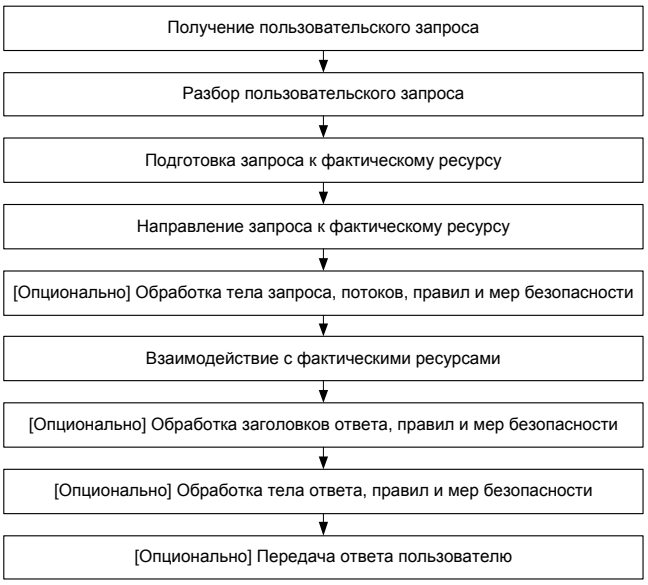

Рис. 4. Блок-схема алгоритма работы системы защиты облачных вычислений

Другой подход к обеспечению безопасности ОВС предлагает компания Microsoft. Здесь как модель безопасности выступает стандартизация. Для защиты приложений Microsoft используется специализированные физические и логические устройства, такие как балансировщики нагрузок, межсетевые экраны и системы обнаружения вторжений. Технологии Microsoft прошли аттестацию SAS70 типов I и II [14] и сертификацию ISO/IEC 27001:2005 [15].

Решение компании Trend Micro, предназначенное для защиты информации в частных облачных средах и общедоступных средах типа SaaS, — платформа

SecureCloud, которая представляет собой SaaS-услугу [16]. В этом решении используются методы управления ключами доступа на основе политик безопасности, системы шифрования, и виртуальный сервер аутентификации. Подобно аналогам SecureCloud реализует подсистему управления доступом в виде отдельного компонента, не зависимого от конкретных поставщиков сервисов облачных вычислений. Платформа SecureCloud также обеспечивает соответствие стандартам безопасности (HITECH [17], PCI DSS [18] и GLBA [19]), предоставляет защиту конфиденциальной и персональной информации с помощью шифрования [16].

Другим решением в области обеспечения безопасности на основе облачных сред является платформа Symantec O3, разработанная компанией Symantec [20]. Платформа создает отдельный сервис контроля безопасности, обеспечивая единообразную идентификацию и защиту информации для всех остальных сервисов. Symantec O3 предоставляет три ключевых уровня защиты: уровень облачного контроля, уровень защиты информации, уровень отслеживания.

Уровень контроля доступа использует инфраструктуру аутентификации на компьютере пользователя, осуществляя интеграцию с политиками безопасности в ОВС. Уровень защиты информации опирается на технологии Symantec в области защиты от утечек данных (DLP) и шифрования (PGP), обеспечивая автоматическое обнаружение, блокирование и шифрование конфиденциальной информации перед ее размещением в облаке. Обрабатывая все данные, проходящие через ОВС, уровень отслеживания Symantec O3 агрегирует все инциденты безопасности, предоставляя возможность для внедрения решений по аудиту безопасности [20].

Наряду с рассмотренными выше системами для обеспечения защиты облачных вычислений применяются также системы обнаружения вторжений, например, SNORT [21], BRO [22], а также ряд фирменных продуктов обеспечения безопасности, которые базируются на подобных принципах. Целесообразно осуществлять анализ трафика, как внешнего по отношению к системе облачных вычислений, так и внутреннего, необходимого для обмена информацией между узлами внутри подсетей. Методы анализа трафика и его агрегатных характеристик, а также схемы развёртывания сетевых сенсоров и организации каналов связи являются темой отдельного исследования (см., например, работы [23, 24].

3. Системы обеспечения безопасности на основе систем облачных вычислений

Системы облачных вычислений предоставляют широкие возможности по выявлению и предотвращению сетевых атак и вторжений. Их распределённые вычислительные мощности могут быть использованы для защиты как других систем, так и компьютеров отдельных пользователей. Например, в антивирусных приложениях ОВС служат для выявления новых вирусных сигнатур, формирования и поддержки актуального состояния баз данных вирусных сигнатур путём их автоматического обновления на компьютерах пользователей через Интернет.

Можно выделить несколько способов организации работы ОВС, ориентированных на выявление и ликвидацию вирусных угроз [25]:

1) работа с метаданными и хеш-функциями исполняемых файлов. Их анализ в системе облачных вычислений с применением экспертных систем и других методов обнаружения вредоносного содержания [26];
2) передача актуальных вирусных сигнатур частыми и малыми порциями на компьютеры пользователя [27];
3) сбор статистики и анализ пользовательских оценок действий приложений (SONAR [28], Comodo Firewall [29] и др.), а также потенциально опасных web-страниц [30].

Обобщением рассмотренных положений служит схема работы распределённых антивирусных систем, приведенная на рис. 5.

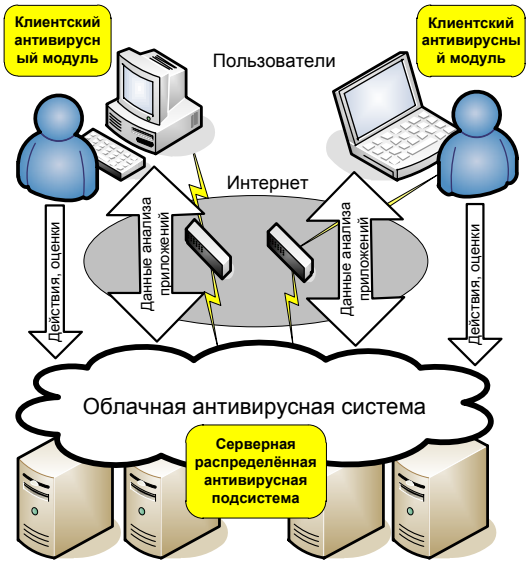

Рис. 5. Схема работы распределённых антивирусных систем

С компьютеров пользователей в систему направляются запросы об обнаруженной подозрительной активности, в частности, о программах, ссылках, ресурсах и других источниках. Система безопасности анализирует запрос с применением облачных вычислений и сообщает антивирусу, установленному на компьютере пользователя, о результатах анализа. В результате выявленные угрозы в виде приложений или web-контента будут заблокированы. Таким образом, все компьютеры, подключенные к облачной антивирусной системе, сообщают ей информацию об обнаруженной подозрительной активности. После обработки полученная информация становится доступной другим компьютерам, подключенным к этой антивирусной системе. Таким образом, информация об атаках и их источниках распространяется между пользователями через распределенную антивирусную сеть. Описанный подход получает всё большее распространение: он защищён рядом патентов [31] и активно применяется в современных антивирусных системах. Значительным преимуществом подхода является возможность динамически, в момент запуска приложения или запроса web-страницы (или другого web-ресурса, изображения, скриптовой программы и т.д.) определить наличие вредоносного содержания.

Примером реализации облачной антивирусной системы может служить продукт Kaspersky Security Network (KSN) [26]. Антивирус отправляет на серверы ОВС следующие данные:

– информацию о заражениях, либо атаках на пользователя;
– информацию о подозрительной активности исполняемых файлов на компьютере пользователя.

Экспертная система выявляет угрозы и проверяет качество принятых решений на ошибки, после чего ищет источники распространения угроз. Найденные источники также проходят автоматическую контрольную проверку с целью исключить ложные срабатывания. Данные о заражениях используются для самообучения экспертной системы, вследствие чего она быстро реагирует на новые разработки злоумышленников и в автоматическом режиме выявляет активные угрозы на компьютерах пользователей. Данные, необходимые для блокирования атаки, передаются остальным пользователям, что позволяет предотвращать последующие заражения [26].

По схожему принципу функционирует антивирусное обеспечение Panda Cloud Office Protection [32]. Технически Panda Cloud Office Protection представляет собой

решение, в котором вся программная инфраструктура располагается в ОВС, а на пользовательских компьютерах устанавливаются антивирусные модули. Система содержит сетевой экран (управляемый пользователем или автоматически), также предлагает защиту для файлов, электронной почты, HTTP/FTP и служб обмена мгновенными сообщениями [33].

4. Заключение

Для обнаружения потенциальных сетевых угроз в ОВС используется широкий спектр специализированных и универсальных систем. Так, при решении проблем диагностики сетей применяются анализаторы сетевых протоколов, системы нагрузочного тестирования, системы сетевого мониторинга. Проблемы защиты информационных ресурсов сетей решаются с помощью межсетевых экранов, антивирусов, систем обнаружения атак, систем контроля целостности, криптографических средств защиты и других стандартных средств. Повышению защищенности от внешних угроз способствует введение фильтров входящих сообщений, которые проверяют правомерность сообщений. Важным является также анализ как внешнего, так и внутреннего трафика для полноты обнаружения угроз различных типов.

Для обнаружения и предотвращения атак на ОВС целесообразно использовать распределенные системы защиты, установленные на различных узлах вычислительной системы. Кроме того, большое распространение получают специальные серверы защиты от атак и серверы безопасности.

Перспективным представляется выявление угроз и атак на сетевые системы с использованием облачных вычислений и предоставлением услуг по технологии SaaS. Предлагаемая авторами структурная схема системы обнаружения сетевых угроз и пресечения сетевых атак, организованная по принципу SaaS, представлена на рис. 6.

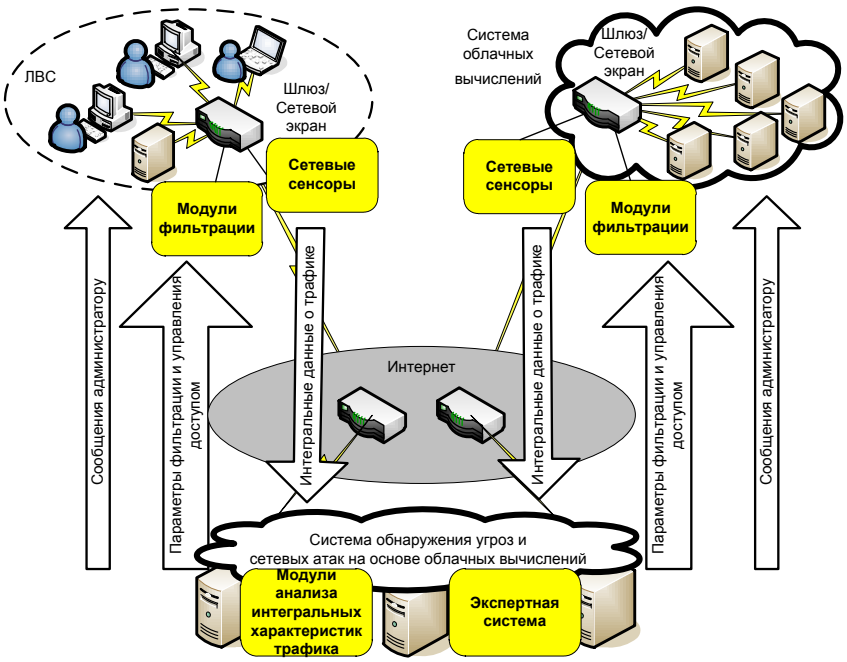

Рис. 6. Структурная схема системы обнаружения сетевых угроз и пресечения сетевых атак, организованная по принципу SaaS

В настоящее время владельцы и администраторы локальных вычислительных сетей и систем распределённых вычислений вынуждены самостоятельно решать все проблемы безопасности. При этом, несмотря на наличие на рынке комплексных многофункциональных решений в этой области, полноценная защита возможна только с применением, нескольких программных и аппаратных продуктов. Вместе с тем, тонкая настройка и развёртывание отдельных компонент защиты (например, SNORT) является нетривиальной задачей даже для опытного администратора. Неслучайно многие компании поручают построение системы безопасности своих вычислительных ресурсов сторонним фирмам — системным интеграторам. При этом система защиты требует дополнительных мощностей и оборудования (помимо существующей сетевой инфраструктуры). Не менее важным является поддержание системы защиты в актуальном состоянии, что не всегда удаётся делать полностью автоматически. Сказанное означает, что в будущем возможно появление и развитие систем, предоставляющих часть услуг по обеспечению сетевой безопасности в виде сервисов приложений — SaaS, подобно тому, как облачные вычисления становятся стандартом «де-факто» для антивирусных систем.

Для решения проблем информационной безопасности облачных вычислительных систем необходим подход, сочетающий в себе сильные стороны различных подходов и предоставляющий возможность развития и разработки новых методов, направленных против новых видов сетевых атак.

Литература

1. *Клементьев И. П., Устинов В. А.* Введение в Облачные вычисления. — УГУ, 2009. — С. 233. [*Klementjev I. P., Ustinov V. A.* Vvedenie v Oblachnihe vihchisleniya. — UGU, 2009. — C. 233.]
2. *Мешалкин В.* От SaaS к DaaS // ИКС. — 2009. — № 7. — С. 47. — http://www.iks-media.ru/articles/2823303.html. [*Meshalkin V.* Ot SaaS k DaaS // IKS. — 2009. — No 7. — C. 47. — http://www.iks-media.ru/articles/2823303.html.]
3. *Валентинова Т.* Что в действительности представляют собой облачные сервисы. — 2009. — http://www.hwp.ru/articles/CHto_v_deystvitelnosti_predstavlyayut_soboy_oblachnie_servisi/. [*Valentinova T.* Chto v deyjstviteljnosti predstavlyayut soboyj oblachnihe servisih. — 2009. — http://www.hwp.ru/articles/CHto_v_deystvitelnosti_predstavlyayut_soboy_oblachnie_servisi/.]
4. Облачные вычисления. Размышления на тему безопасности. — 2010. — cloudzone.ru/articles/analytics/5.html. [Oblachnihe vihchisleniya. Razmihshleniya na temu bezopasnosti. — 2010. — cloudzone.ru/articles/analytics/5.html.]
5. Виртуальная энциклопедия «Linux по-русски»: Программные средства обеспечения безопасности. — 2012. — http://www.linuxcenter.ru/enc/sec2.phtml. [Virtualjnaya ehnciklopediya «Linux po-russki»: Programmnihe sredstva obespecheniya bezopasnosti. — 2012. — http://www.linuxcenter.ru/enc/sec2.phtml.]
6. *Тейбер Д.* Насколько безопасен провайдер облачных сервисов? Поговорим о доступе. — 2011. — http://www.osp.ru/cloud/2011/0311/13007657/. [*Teyjber D.* Naskoljko bezopasen provayjder oblachnihkh servisov? Pogovorim o dostupe. — 2011. — http://www.osp.ru/cloud/2011/0311/13007657/.]
7. Patent 2005107204. Method and System for Access Control in Distributed Object-Oriented Systems. — 2005. — http://www.wipo.int/patentscope/search/en/WO2005107204.
8. Patent 2011072489. Method, Devises and Media for Securely Utilizing a Non-Secured, Distributed, Virtualized Network Resource with Applications to Clod-Computing Security and Management. — 2011. — http://www.faqs.org/

patents/app/20110072489.
9. Patent 2008077150. Secure Service Computation. — 2008. — http://www.wipo.int/patentscope/search/en/WO2008077150.
10. Patent 2011083179. System and Method for Mitigating a Denial of Service Attack Using Cloud Computing. — 2007. — http://www.faqs.org/patents/app/20110083179.
11. Patent 2011010823. Method for Detecting and Preventing a DDOS Attack Using Cloud Computing and Server. — 2011. — http://www.wipo.int/patentscope/search/en/detail.jsf?docId=WO2011010823.
12. Patent 2011072289. Cloud-Based Firewall System and Service. — 2011. — http://www.wipo.int/patentscope/search/en/detail.jsf?docId=WO2011072289.
13. Securing the Cloud from the Inside. — 2012. — http://www.novell.com/products/cloud-security-service/.
14. SAS 70 Overview. — 2012. — http://sas70.com/sas70_overview.html.
15. ISO/IEC 27001:2005(E). Information Technology — Security Techniques — Information Security Management Systems — Requirements. — 2005.
16. Trend Micro SecureCloud. — 2011. — http://www.tadviser.ru/index.php. [Trend Micro SecureCloud. — 2011. — http://www.tadviser.ru/index.php.]
17. HITECH Act Enforcement Interim Final Rule. — http://www.hhs.gov/. [HITECH Act Enforcement Interim Final Rule. — http://www.hhs.gov/.]
18. PCI Standards Documents. — 2012. — https://www.pcisecuritystandards.org.
19. GLBA Security Standards. — http://rusecure.rutgers.edu/content/glba-security-standards.
20. Symantec анонсировала платформу O3 для контроля и защиты корпоративных облачных сервисов. — 2012. — http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20111010_01. [Symantec anonsirovala platformu O3 dlya kontrolya i zathitih korporativnihkh oblachnihkh servisov. — 2012. — http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20111010_01.]
21. *Roesch M.* Snort — Lightweight Intrusion Detection for Networks. — 1999. — http://www.snort.org/.
22. The Bro Network Security Monitor. — 2011. — http://bro-ids.org/.
23. *Емельянова Ю. Г., Фраленко В. П.* 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. — С. 17–31. — http://psta.psiras.ru/read/psta2011_4_17-31.pdf. [*Emeljyanova Yu. G., Fralenko V. P.* Analiz problem i perspektivih sozdaniya intellektualjnoyj sistemih obnaruzheniya i predotvratheniya setevihkh atak na oblachnihe vihchisleniya // Programmnihe sistemih: teoriya i prilozheniya: ehlektron. nauchn. zhurn. — 2011. — No 4. — S. 17–31. — http://psta.psiras.ru/read/psta2011_4_17-31.pdf.]
24. Комплексная защита крупных корпоративных сетей передачи данных / С. Д. Белов, О. Л. Жижимов, А. М. Федотов и др. // Третья Международная конференция «Системный анализ и информационные технологии» САИТ-2009 (14-18 сентября 2009 г., Звенигород, Россия). — 2009. [Kompleksnaya zathita krupnihkh korporativnihkh seteyj peredachi dannihkh / S. D. Belov, O. L. Zhizhimov, A. M. Fedotov и др. // Tretjya Mezhdunarodnaya konferenciya «Sistemnihyj analiz i informacionnihe tekhnologii» SAIT-2009 (14-18 sentyabrya 2009 g., Zvenigorod, Rossiya). — 2009.]
25. Вирусы (и антивирусы). — 2011. — http://habrahabr.ru/blogs/virus/121197/. [Virusih (i antivirusih). — 2011. — http://habrahabr.ru/blogs/virus/121197/.]
26. *Машевский Ю.* Антивирусный прогноз погоды: облачно. — 2010. — http://www.antivirus-navigator.com/articles/kaspersky-cloud.htm. [*Mashevskiyj Yu.* Antivirusnihyj prognoz pogodih: oblachno. — 2010. —

http://www.antivirus-navigator.com/articles/kaspersky-cloud.htm.]
27. *Крупин А.* Облачные антивирусы в теории и на практике. — 2010. — www.3dnews.ru/software/cloud-ativiruses-1. [*Krupin A.* Oblachnihe antivirusih v teorii i na praktike. — 2010. — www.3dnews.ru/software/cloud-ativiruses-1.]
28. *Ильин С.* Облачные вычисления против вирусов. На что способен Norton Internet Security? // Хакер. — — № 10/09 (130). — www.xakep.ru/magazine/xa/130/034/1.asp. [*Iljin S.* Oblachnihe vihchisleniya protiv virusov. Na chto sposoben Norton Internet Security? // Khaker. — — No 10/09 (130). — www.xakep.ru/magazine/xa/130/034/1.asp.]
29. Comodo Firewall. — 2012. — http://www.comodo.com/home/internet-security/firewall.php.
30. Антивирус AVAST! — 2011. — http://support.avast.com. [Antivirus AVAST! — 2011. — http://support.avast.com.]
31. Patent 2007015254. Security Server in a Cloud. — 2007. — http://www.wipo.int/patentscope/search/en/detail.jsf?docId=WO2007015254.
32. SaaS Service for PCs, Laptops and File Servers: the Light, Safe, Simple and Complete Solution. — 2012. — http://www.pandasecurity.com/enterprise/solutions/cloud-office-protection/.
33. Panda Cloud Office Protection // PC Magazine/Russian Edition. — 2007. — http://www.pcmag.ru/software/detail_rev.php?ID=44521.

UDC 004.042

The Modern Level and Development Trends of Network Security for Cloud Computing System

J. G. Emelyanova[*], E. Mbaykodzhi[†], I. V. Sochencov[†]

[*] *Organization of Russian Academy of Sciences*
Ailamazyan Program Systems Institute of RAS
Petra I str., 4a, selo Veskovo, Pereslavl-Zalesskij,
Yaroslavskaya oblast', 152021, Russia

[†] *Information Technologies Department*
Peoples' Friendship University of Russia
Miklukho-Maklaya str., 6, Moscow, Russia, 117198
Institute for Systems Analysis of Russian Academy of Sciences (ISA RAS)
prosp. 60-let Octyabria, 9, Moscow, 117312, Russia

The article considers the modern level of researches in the field of cloud computing network security. The structure and functioning principles of cloud computing security systems, as well as cloud-based security system were analyzed. The modern trends in this field were studied.

Key words and phrases: cloud computing system, network security, intellectual property, intrusion detection, information security.