УДК 004.056.5:004.75

АНАЛИЗ УГРОЗ И МЕТОДОВ ЗАЩИТЫ ОБЛАЧНЫХ СЕРВИСОВ

Волков В.А.
Харьковский национальный университет радиоэлектроники

Использование облачных сервисов дает множество новых возможностей, но требует тщательной проработки вопросов безопасности. В работе приведено краткое описание моделей SaaS, PaaS и IaaS облачных сервисов. Для каждой из этих моделей исследованы и описаны основные угрозы информационной безопасности. Для каждой угрозы приведены применяемые методы защиты, их сильные и слабые стороны. На основе проведенного в работе анализа выявлено, что наименее защищенной является виртуальная структура облачной системы. Также приведена классификация атак и методов защиты в облачных сервисах, использование которой будет полезно для принятия обоснованных решений о снижении рисков при использовании облачных сервисов.

Ключевые слова: защита информации, угрозы, облачные сервисы, методы защиты, виртуальная инфраструктура, уязвимости.

Постановка проблемы. Новые технологии и модели обслуживания способны изменить деятельность компаний и стать важнейшими стимулами инноваций и сокращения текущих расходов. Облачные вычисления являются одной из них [1]. Работа в облаках обладает огромным потенциалом в бизнес-среде. Зачастую применение облачных вычислений – наилучший способ решения корпоративных задач, на которые не хватает мощности собственной ИТ-инфраструктуры. Помимо существенной экономической выгоды, важным аргументом использования этой технологии для многих компаний может стать возможность доступа к данным из любой точки планеты.

Несмотря на все плюсы облачных сервисов, большинство компаний боятся их использовать по причине недоработки в области информационной безопасности [1-3]. Информация, находящаяся в облачных сервисах, может подвергнуться атаке посредством уязвимостей как непосредственно облачной системы, так и решений, нацеленных на управление сервисами. Таким образом актуальной является задача идентификации угроз информационной безопасности для облачных систем, анализа этих угроз и методов обеспечения информационной безопасности в облачных сервисах.

Анализ последних исследований и публикаций. Исследователи из университета Северной Каролины, университета Висконсина и корпорации RSA исследуют различные угрозы и их влияние на облачные сервисы [2]. В США ассоциация Cloud Security Alliance выпустила Cloud Controls Matrix. Этот документ представляет собой перечень существующих технологий информационной безопасности, которые могут быть использованы в облачных сервисах [4]. В работах Демурачева и Ищенко [6] освещены проблемы обеспечения безопасности при переходе на облачные технологии. В работах Андреева и Корчагина [5] приведен перечень основных угроз безопасности виртуальной инфраструктуры облачных сервисов. В ежегодных отчётах ассоциации Cloud Security Alliance описаны средства защиты данных при использовании облачных технологий.

Выделение не решённых ранее частей общей проблемы. Существуют работы, в которых исследуются угрозы информационной безопасности в облачных сервисах, методы защиты данных, однако эта область является слабо исследованной. Также угрозы и методы защиты данных в виртуальной структуре облачных систем слабо исследованы. Что касается классификации угроз нарушения ИБ в системе облачных вычислений и соответствующих методов защиты от них, то они отсутствуют. Поэтому рассматриваемая в данной работе тематика исследований, направленных на анализ угроз и методов защиты в системе облачных вычислений, и построение их классификации является актуальной.

Цель статьи. Изучение основных угроз информационной безопасности и существующих методов защиты в облачных системах, их классификация, на основании которой возможно представление анализа методов защиты с описанием их использования.

1. Описание моделей облачных сервисов.

Существует три модели облачных сервисов предоставления услуг: «программное обеспечение как сервис» (SaaS, DbaaS, DaaS); «платформа как сервис» (PaaS); «инфраструктура как сервис» (IaaS). Наиболее уязвимыми считаются модели PaaS и IaaS, где пользователям предоставляется больший контроль над инфраструктурой облака, а также больший набор предоставляемых услуг. Именно поэтому в качестве уязвимостей облачных технологий рассматривались уязвимости этих моделей [6].

В соответствии с моделью IaaS серверы и другие ресурсы предоставляются по мере необходимости через облако. Данная модель обеспечивает самообслуживание и доступ к ИТ-ресурсам по запросу. Это означает, что на создание необходимых инструментов разработчикам может потребоваться всего несколько минут, а не дни, недели или месяцы, как раньше. При работе с моделью IaaS необходимые сервисы взаимодействуют в процессе их использования, а это, в свою очередь, обеспечивает более гладкое протекание операций, которые в любой момент лучше приспосабливаются к потребностям компании.

Другая модель – модель PaaS, в свою очередь, представляет категорию сервисов, обеспечивающих предприятия вычислительной платформой и набором решений в качестве сервисов. В соответствии с ней клиент PaaS разрабатывает программное обеспечение, используя инструмен-

© Волков В.А., 2015

ты и библиотеки провайдера. Клиент управляет развертыванием и настройками программного обеспечения. Провайдер предоставляет сети, серверы и системы хранения. Модель PaaS позволяет развертывать приложения, избегая затрат и сложностей, связанных с приобретением необходимого оборудования и программного обеспечения, и управлением ими.

Рис. 1. Различие между платформами IaaS и PaaS

Важным фактом можно выделить то, что в ряде отраслей работа современных облачных моделей требует закрытия технических вопросов, а также вопросов связанных с их безопасностью. Так как на физическомуровне каждая из моделей представляет собой совокупность серверов, размещенных на одной площадке с целью повышения эффективности и защищённости, а работа и управление ими происходит через сеть, то и защита облачных платформ представляет собой сетевую и физическую защиту, а также отказоустойчивость и надёжное электропитание.

В настоящее время на рынке представлено множество решений для защиты от различных угроз. Их объединяет ориентированность на узкий спектр решаемых задач. Однако спектр этих задач подвергся некоторому расширению вследствие постепенного вытеснения классических аппаратных систем виртуальными платформами. К известным типам угроз (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение) добавились сложности, связанные с контролем среды – гипервизора, разграничением прав доступа и трафиком между гостевыми виртуальными машинами. Проникновение платформ виртуализации достигло того уровня, когда практически все компании, использующие эти системы, весьма серьезно занялись вопросами усиления безопасности в них. Отметим, что буквально пару лет назад интерес был скорее теоретический.

2. Модель PaaS.

Как правило, провайдеры PaaS предоставляют клиентам возможность писать приложения на собственном сценарном языке, а также могут обеспечивать такие сервисы безопасности, как аутентификация пользователей и защита от DDoS-атак. Однако сами базовые компоненты, на которых работает платформа, также могут быть уязвимыми для нападений извне. Сергей Рыжиков, генеральный директор «1С-Битрикс», предупреждает: часто хакеры атакуют не платформы, а базовое программное обеспечение, на котором те работают. Поэтому провайдер должен оградить предлагаемую платформу от подобных атак.

2.1 Атаки на отказ в обслуживании. DDoS-атаки.

Для PaaS эти атаки нацелены не на банальное «затопление» сервера запросами, а использующие конкретную брешь в платформе. В этом случае атака может содержать небольшой поток данных, но приводить к плачевным результатам: зацикливанию платформ, замедлению обработки обычных запросов или даже выводу из строя некоторых важных для системы элементов. Например: массовый перебор паролей для администраторов CMS-систем Joomla и Wordpress. Эффективный механизм защиты от этого типа атак – установленный proxy-сервер с настроенной защитой от разных видов DDoS-атак. Такая настройка должна быть обширной, так как уже устаревшие виды атак стали возвращаться с уже новым, изощрённым применением [4].

2.2 SQL-инъекции и XSS-нападения.

SQL-инъекции это методика, при которой взломщик создаёт или изменяет текущие SQL-запросы для отображения скрытых данных, их изменения, или даже выполнения опасных команд операционной системы на сервере баз данных. Атака выполняется на базе приложения, строящего SQL-запросы из пользовательского ввода и статических параметров.

XSS – это уязвимость на сервере, позволяющая внедрить в генерируемую скриптами на сервере HTML-страницу произвольный код путём передачи его в качестве значения не фильтруемой переменной.Любой метод атак для определённой XSS-уязвимости представляет собой некий контейнер в котором код будет подан жертве.

Для защиты от атак на уязвимости платформы хорошо работает инструмент, который называется «экран уровня приложений». Этот компонент платформы анализирует входящий и исходящий трафик, блокируя попытки эксплуатации известных уязвимостей. Более эффективным инструментом защиты платформы от уязвимостей являются специальные анализаторы исходных кодов для сценарных языков платформы. Они позволяют проверить загружаемый в платформу код на наличие в нем типичных ошибок программирования, а иногда и специально вставляемых закладок. Правильно перед внесением любых изменений в код приложения проверить его на подобном анализаторе.

2.3 Распространение вредоносных программ.

Для этого типа атак используют популярные платформы CMS(ContentManagementSystem). Делается это так: взламывается сервер со свободно распространяемой CMS и в нее инсталлируется модуль, который вставляет в коды страниц ссылки на вредоносные ресурсы. Есть также модули для удалённого исполнения любых команд на сервере, которые могут быть встроены, например, в тему сайта.

Эффективным инструментом защиты будут служить «CMS-антивирусы». Администраторам CMS стоит использовать специальные сканеры кодов, которые в уже развернутом сайте обнаруживают подобные вредоносные фрагменты. Также есть инструменты с открытым кодом, однако неизвестно, насколько быстро в них обновляются сигнатуры таких вставок.

2.4 Атаки на API платформы.

Пользователь часто не знает, на какой именно операционной системе и базе данных работает платформа, хакеры, тем не менее, могут атаковать не саму платформу, а через нее – базовые компоненты.

Опасность таких атак зависит от набора интерфейсов, которые предоставляет платформа для приложений, поскольку именно через них хакеры, в конце концов, и нападут на операционную систему или базу данных.

Поэтому платформа должна иметь как можно меньший выбор инструментов прямого доступа к базовым элементам и всячески защищаться от попыток использования подобного прямого общения [4].

2.5 Атаки на передаваемые данные.

Данного типа атаки подразумевают, что злоумышленник будет совершать нападение на сети между клиентом и провайдером. Атаки являются потенциально опасными, так как клиент при работе с облаком передаёт конфиденциальную информацию.

Для провайдеров важно обеспечить защиту данных при передаче посредством использования защищенного соединения, также при обмене данными с провайдерами PaaS рекомендуется использовать шифрование. Должной защитой можно назвать использование таких алгоритмов и надёжных протоколов, как AES, TLS, IPsec и другие [2].

Отдельно следует сказать и о шифровании данных на клиенте. В частности, когда речь идет о соблюдении требований закона о персональных данных, то не всегда имеет смысл шифровать все данные – достаточно зашифровать только собственно персональные данные, поскольку в большинстве информационных систем совсем не обязательно, чтобы они обрабатывались в открытом виде. В этом случае в облачные базы данных помещается частично зашифрованная информация – поля с персональными данными или конфиденциальной информацией шифруются на клиенте и ключ дешифровки в облачную инфраструктуру не передается. Таким образом, даже при использовании облачных инфраструктур и шифровании можно соблюсти требования регулятора по защите регулируемых законом сведений.

2.6 Атаки на клиента.

Здесь рассматриваются такие атаки, как CrossSitScripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и другие. Провайдерам облачных технологий требуется организовать доверительные отношения пользователь – облачный провайдер. Для этого необходимо прибегнуть к более надёжной аутентификации пользователя на сервере предоставления услуг.

Защитой от данного вида атак является правильная аутентификация и использование шифрованного соединения – TLS, SSL. В достижении требуемой надёжной аутентификации помогут такие средства, как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протоколы LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language) [4].

Во время разработки механизмов обеспечения шифрования и надежной аутентификации важно помнить, что использование облачных технологий возрождают давно забытые атаки типа: Heartbleed, Poodle и другие. Поэтому стоит оградить себя от использования скомпрометировавших себя механизмов.

3. Модель IaaS.

Модель IaaS, несомненно, самая сложная с точки зрения защиты от атак. В самом деле, пользователь IaaS имеет гораздо больше свободы, чем в других сервисах. Также крайне важной архитектурной особенностью этой модели является виртуализация, её использование делает системы подверженными новым видам атак. При всё более обширном внедрении в использование облачных технологий, в сфере обеспечения должного качества виртуализации появляются новые угрозы (рис. 2).

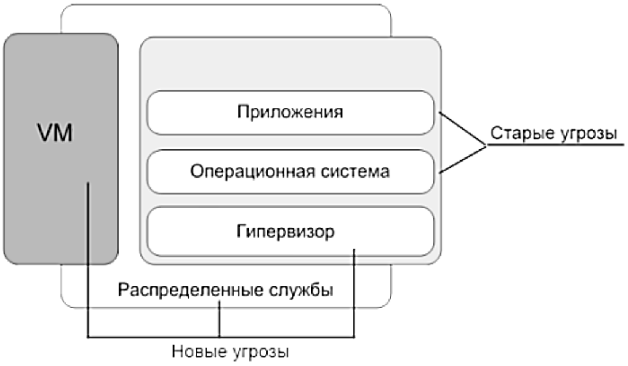

Рис. 2. Старые и новые угрозы виртуальной среды

Следующая существенная проблема связана с управлением ресурсами облака. Любое систематическое управление ресурсами, в отличие от управления по ситуации, требует существования управляющих компонентов предназначенных для реализации нескольких классов политик: управления доступом, выделения ресурсов, балансирования ресурсов, оптимизации энергопотребления и предоставление качества обслуживания.

3.1 Атаки на клиента.

Так как уязвимости модели PaaS, через которые совершаются атаки этого типа, присутствуют и в модели IaaS, то важность защиты от них не стоит упускать.

Обеспечение защиты платформы IaaS от таких атак, по сравнению с защитой платформы PaaS, отличается тем, что пользователь имеет возможность самостоятельно организовать защиту. Клиент может арендовать инфраструктуру и установить в него собственные инструменты защиты, неподконтрольные сервисной службе оператора. В этом случае поддерживать такую защиту будет служба безопасности клиента, и контроль над собственными данными будет лучше. Для реализации подобной стратегии можно использовать защитные продукты, которые поставляются в виде образов виртуальных машин [4].

3.2 Традиционные атаки на ПО.

К таким атакам можно отнести атаки на уязвимости операционной системы, модульные компоненты, сетевые протоколы и другие.Николай Арефьев, старший инженер-проектировщик по ИБ Центра информационной безопасности компании «ИнфосистемыДжет», предупреждает: «Часто провайдеры облачных услуг используют

для предоставляемых сервисов IaaS неактуальные (с точки зрения критических обновлений безопасности) образы предустановленного системного программного обеспечения. Эксплуатация уязвимостей в таком программном обеспечении чревата удаленными сетевыми атаками, в результате которых внедряется и исполняется на стороне сервиса произвольный код нарушителя. Это, в свою очередь, ведет к компрометации самого сервиса и облака в целом, нарушению доступности сервисов и получению доступа к конфиденциальной информации».

Обычно для защиты от таких атак достаточно установить межсетевой экран, firewall, антивирус, IPS и другие компоненты, решающие данную проблему. При этом важно, чтобы данные средства защиты эффективно работали в условиях виртуализации [1].

3.3 Функциональные атаки на элементы облака.

Облако представляет собой многослойную структуру, где общая защита системы равна защите самого слабого элемента в ней. Другими словами, к примеру, успешная атака на межсетевой экран или proxy-сервер, стоящий на границе облака и выходом в Интернет, заблокирует доступ ко всем ресурсам, тем не менее, связи внутри него будут сохраняться.

Эффективной защитой от функциональных атак будет использование для каждой части облака следующих средств защиты: для proxy-сервера – эффективную защиту от DDoS, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для систем управления базами данных – защиту от SQL-инъекций, для системы хранения данных – правильно настроенныепрограммы резервного копирования, а также разграничение доступа [2].

3.4 Атаки на виртуальную инфраструктуру.

Из такого рода атак можно выделить несколько основных типов:

3.4.1. Атаки на виртуальную машину путём:

а) атаки из другой виртуальной машины;

б) атаки на диск и файлы конфигурации виртуальной машины;

в) атаки на сеть репликации виртуальной машины;

г) атаки на сеть и систему хранения данных содержащую файлы виртуальной машины;

д) атаки на средства резервного копирования виртуальной машины.

3.4.2. Атаки на хост виртуализации путём:

а) атаки из физической сети;

б) атаки средствами скомпрометированного сервера управления виртуальной инфраструктуры;

в) атаки на виртуальные сервисы гипервизора SSH, WEB, TELNET;

г) атаки на агенты гипервизора от сторонних производителей.

3.4.3. Атаки на сервер управления виртуальными машинами путём:

а) атаки на операционную систему обеспечения функционирования управляющих сервисов;

б) атаки на систему управления базами данных сервера управления;

в) атаки на базу учётных записей;

г) сетевой атаки на сервис взаимодействия и мониторинга с хостами виртуализации.

3.4.4. Атаки на ресурсы хоста виртуализации путём:

а) неконтролируемого роста числа виртуальных машин;

б) некорректного планирования разграничения пулов ресурсов;

в) некорректного планирования растущих по мере заполнения виртуальных дисков виртуальных машин;

г) некорректного разграничения прав пользователей и групп виртуальной инфраструктуры.

На сегодняшний день уже существуют специализированные системы защиты виртуальной инфраструктуры, которые можно разделить на следующие классы:

1) Программные продукты для анализа трафика и предотвращения вторжений, разработанные специально для виртуальной среды.

2) Программное обеспечение для разграничения прав доступа в виртуальной инфраструктуре.

3) Программное обеспечение для проведения аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности.

В качестве стандартных методов защиты рекомендуется применять специальные продукты для виртуальных сред, интеграцию хост – серверов со службой AD, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам [5].

3.5 Атаки с использованием смежной уязвимости.

В любой модели облачного сервиса существует угроза уязвимости через общие ресурсы. Если ключевой компонент совместноиспользуемой технологии будет взломан, то это подвергнет риску не только пострадавшего заказчика.

Защитой от такого рода атак является использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развёрнуты с применением таких технологий, как VPN (VirtualPrivateNetwork), VLAN (VirtualLocalAreaNetwork) и VPLS (VirtualPrivateLocalService). Часто провайдеры изолируют пользователей друг от друга за счёт изменения данных кода в сценариях собственной единой программной среды.

3.6 Атаки на системы управления.

Большое количество виртуальных машин, используемых в облаках, требует наличия систем управления, способных надёжно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в системы управления может привести к появлению виртуальных машин «невидимок», способных блокировать одни виртуальные машины и поставлять другие. Всё это позволяет злоумышленникам получать информацию из облака или захватывать его части или всё облако целиком.

Провайдерам облачных сервисов для устранения уязвимостей, связанных с этим типом атак, требуется организовать отслеживание изменений файлов: касается важных конфигурационных файлов управляемой инфраструктуры; отслеживание логов и их анализ: централизованное отслеживание событий посредством логфайлов и анализ событий для оценки и обнаружения вредоносной активности.

4. Классификация методов защиты.

По результатам исследований была выведенасхема классификации атак и соответствующих механизмов защиты, которая представлена на рисунке 3. Выдержки из данной классификации, подтверждающие её, находят своё отображение в ежегодных отчётах таких организаций, как Cloud Security Alliance, занимающихся вопросами облачной безопасности.

Как видно из рисунка 3, некоторые механизмы защиты могут обеспечивать защиту от нескольких видов атак, а другие реализуют защиту только от определённых. В зависимости от таких условий и нужно строить свою систему обеспечения безопасности облачного сервиса.

Наиболее непроработанными и опасными являются атаки на виртуальную составляющую облаков, это высокоуровневый тип угроз, так как он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. Появление виртуализации стало актуальной причиной масштабной миграции большинства систем на виртуальные машины, однако решение задач обеспечения безопасности, связанных с эксплуатацией приложений в новой среде, требует особого подхода.

Применение ПО виртуализации требует существенного изменения в подходах к обеспечению информационной безопасности систем. Необходимо отметить появление нового принципиально важного объекта виртуальной инфраструктуры – гипервизора, который на практике часто игнорируется и не защищается при помощи специализированных средств [3].

По данным исследования компании Garthner, изложенные в ее пресс-релизе в январе 2013 г.: к концу 2014 года 60% виртуальных серверов окажутся менее защищенными, чем физические сервера. Одна из основных причин такого положения, указанная в релизе: «40% виртуальных машин устанавливаются без участия специалистов по информационной безопасности. На предприятиях в уже существующих инфраструктурах большими темпами успешно виртуализируются различного рода информационные системы, однако методы и подходы защиты информации при этом, как правило, используются те же, что предусмотрены для физических серверов».

Действительно виртуальная инфраструктура требует нового подхода к обеспечению безопасности информации. Уже сейчас разработчики систем виртуализации тратят огромные ресурсы на усовершенствование защиты своих продуктов. Подводя итоги проведенных исследований, однозначно следует согласиться с тем, что контроль и управление облаками – является основной проблемой безопасности [5].

Эдуард Бавижев, руководитель группы виртуализации DataLine, приводит пример собственной системы безопасности, которая включает в себя виртуальные сети и туннели, устойчивые алгоритмы шифрования, разграничение доступа к порталу заказчика с использованием различных методов фильтрации, за-

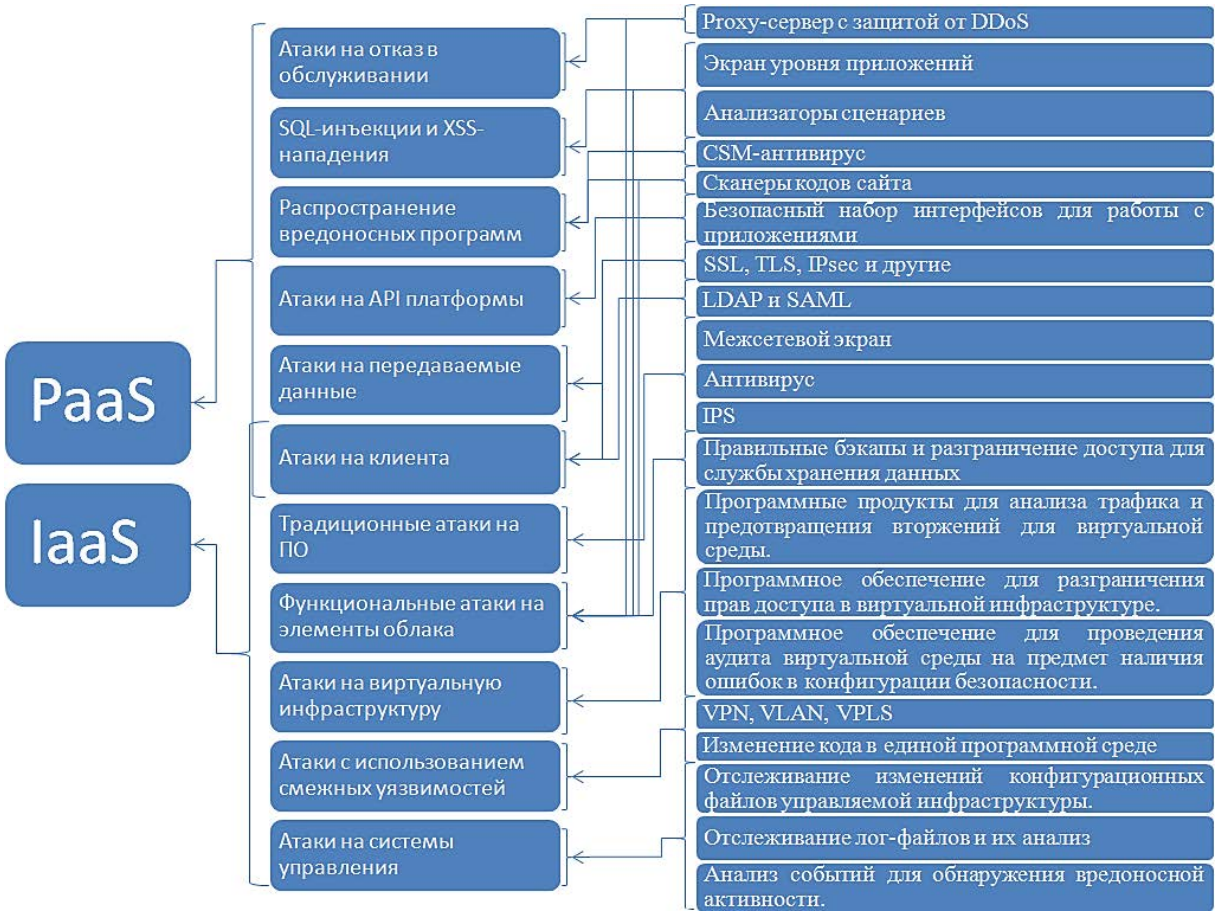

Рис. 3. Классификация атак и методов защиты

щиту периметра виртуального дата-центра, антивирусную защиту виртуальных машин, защиту от DDoS-атак и т.д. [1].

Выводы и предложения. В данной работе проведен анализ основных угроз информационной безопасности и существующих методов защиты от них в облачных системах. На основе проведенного анализа показано, что наиболее опасными являются атаки на виртуальную структуру облачной системы. Также приведена классификация, на основании которой возможно представление анализа методов защиты с описанием их использования. В дальнейшей работе необходимо провести детальный анализ защищённости виртуальной инфраструктуры облачной системы и построить комплексную модель противодействия угрозам.

Список литературы:

1. 8 шагов к безопасным облачным системам // Журнал «Information Security / Информационная безопасность», 2013. – С. 28-29.
2. Dan C. Marinescu. Cloud Computing: Theory and Practice // Newnes. – 2013. – P. 416.
3. Mickey Iqbal, Mithkal Smadi, Chris Molloy, Jim Rymarczyk. IT Virtualization Best Practices: A Lean, Green Virtualized Data Center // Publisher: Mc Press; 1st edition. – January 1, 2011.
4. Top Threats Working Group. Cloud Security Alliance. The Notorious Nine Cloud Computing Top Threats. – 2013.
5. Андреев В. Защита виртуальной инфраструктуры / В. Андреев, І. Корчагин, А. Ковязин; IT-Expert. – Вип. 6, 2011. – С. 64-69.
6. Демурчев Н. Г. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления / Н. Г. Демурчев, С. О. Ищенко; Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. Таганрог: Изд-во ТТИ ЮФУ, 2010.

Волков В.А.
Харківський національний університет радіоелектроніки

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

Анотація
Використання хмарних сервісів дає безліч нових можливостей, але вимагає ретельного опрацювання питань безпеки. У роботі наведено короткий опис моделей SaaS, PaaS і IaaS хмарних сервісів. Для кожної з цих моделей досліджені і описані основні загрози інформаційної безпеки. Для кожної загрози наведені застосовувані методи захисту, їх сильні і слабкі сторони. На основі проведеного в роботі аналізу виявлено, що найменш захищеною є віртуальна структура хмарної системи. Також наведено класифікацію атак і методів захисту в хмарних сервісах, використання якої буде корисно для прийняття обґрунтованих рішень щодо зниження ризиків при використанні хмарних сервісів.
Ключові слова: захист інформації, загрози, хмарні сервіси, методи захисту, віртуальна інфраструктура, уразливості.

Volkov V.A.
Kharkov National University of Radio Electronics

ANALYSIS OF THREATS AND METHODS OF PROTECTION OF CLOUD SERVICES

Summary
The use of cloud service provides many new features, but it requires careful consideration of safety issues. The paper gives a brief description of models SaaS, PaaS and IaaS cloud services. The major threats of information security are investigated and described for each of these models. Securing methods are described for each threat, advantages and drawbacks of each type of the methods are shown. Based on the performed analysis it was revealed that the most vulnerable is a virtual structure of the cloud system. Also, classification attacks and methods of protection in the cloud services are described. The use of classification is useful for making informed decisions on risk reduction when using cloud services.
Keywords: information security, threats, cloud services, security methods, virtual infrastructure, and vulnerability.