ФОРМАЛЬНАЯ МОДЕЛЬ ТЕКУЩЕЙ СИТУАЦИИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ГЕОЛОКАЦИОННЫХ СИСТЕМ

УДК 004.986

ШЕРСТЮК Владимир Григорьевич
д.т.н., профессор кафедры информационных технологий Херсонского национального технического университета,
Научные интересы: методы и модели поддержки принятия решений в реальном времени, принятие решений на основе прецедентов, мультиагентные системы, комбинированные логические системы представления знаний.
e-mail v_sherstyuk@bigmir.net,

СКОРИК Сергей Николаевич
аспирант кафедры информационных технологий Херсонского национального технического университета
Научные интересы: облачные системы и сервисы, методы и модели обеспечения безопасности, системы реального времени.
e-mail skorik1992@gmail.com

ПОСТАНОВКА ПРОБЛЕМЫ

На сегодняшний день наблюдается общая тенденция перехода ИТ-индустрии к виртуализированной инфраструктуре и облачным вычислениям. Однако, во многих случаях достаточно остро встает вопрос о безопасности такого перехода. Существует мнение, что виртуализация является более безопасной, чем традиционные корпоративные среды, так как обеспечивает определенную изоляцию между виртуальными машинами, а также вследствие отсутствия информации об успешных атаках на гипервизоры [1]. В то же время, новые виртуальные среды нуждаются в обеспечении безопасности в той же степени, что и традиционные (физические) среды, поэтому в них принято использовать аналогичный, выработанный годами подход к безопасности. Однако, новая среда является значительно более сложной. Виртуальные подходы, индуцированные в уже существующие вычислительные сети, создают совершенно новую сетевую платформу, требующую иного подхода к обеспечению безопасности. Основной причиной возникновения проблем в этом вопросе является недостаточный накопленный опыт работы ИТ-специалистов и специалистов по безопасности с облачными технологиями и системами. Таким образом, разработка научно обоснованных методов и моделей обеспечения безопасности облачных систем представляет собой весьма актуальную научную задачу.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

Облачные вычисления являются сравнительно новой технологией доступа к ресурсам, поэтому вопросы обеспечения их безопасности еще не исследованы в достаточной мере. Основная часть публикаций поверхностно описывает недостатки облачных технологий, практически не затрагивая проблемы безопасности данных в облачных системах [2, 3].

В то же время, при решении практических задач обеспечения безопасности облачных вычислений, первое, что очевидно интересует ИТ-специалистов, - это как будут защищены данные, передаваемые в облако. Хотя использование облачной системы и сопряжено со значительными финансовыми выгодами, оно, как и любая ИТ-инфраструктура, обладает своим набором угроз безопасности. К известным типам угроз обычных корпоративных информационных систем (ИС) (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение) добавились проблемы, связанные с контролем облачной среды (гипервизора), трафика между гостевыми машинами и разграничением прав доступа [4]. В последнее время также усугубились вопросы реализации адекватной политики защиты центров обработки данных (ЦОД) при выполнении нормативных требований внешних регуляторов. Работа современных ЦОД в ряде отраслей требует решения и технических вопросов, связанных с их безопасностью. На протяжении нескольких лет наблюдается рост частоты атак на облака и значительно расширение спектра используемого для этого вредоносного программного обеспечения. С увеличением числа инцидентов, связанных с отслеживанием уязвимостей, угрозами и атаками методом грубой силы, становится критически важно определить типы угроз, характерных для облака, что позволит создать подходящую всестороннюю стратегию безопасности, чтобы защитить облачную экосистему от атак.

Целью работы является обоснование подходов к построению систем обеспечения безопасности облачных вычислений, выполняемых на основе технологии полной виртуализации серверов и виртуализации настольных систем, а также построение формальной модели текущей ситуации для облачной ИС, связанной с наличием и потенциалом угроз ее безопасности.

Существующие проблемы безопасности облачных вычислений

Главной проблемой безопасности облачных вычислений является контроль управления облаками. Никогда не бывает достаточных гарантий того, что все ресурсы облака просчитаны, в нем нет неконтролируемых виртуальных машин, не запущены лишние процессы и не нарушена взаимная конфигурация элементов облака. Перечисленные типы угроз относятся к категории высокоуровневых, т.к. они связаны непосредственно с управляемостью облака как единой информационной системы, для которой общую защиту необходимо строить индивидуально. Для решения данной задачи можно использовать модель управления рисками для облачных инфраструктур.

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличии от физической безопасности, сетевая безопасность в первую очередь требует построения надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра, с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия, которыми могут являться отдельные серверы, доступные из Интернета или серверы внутренних сетей.

В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации [5]. Для сохранения целостности данных и обеспечения защиты необходимо рассмотреть основные из-

вестные угрозы для облачных вычислений [5-7]:

– трудности при перемещении обычных серверов в вычислительное облако. Требования к безопасности облачных вычислений в принципе не отличаются от требований безопасности к центрам обработки данных. Однако, виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз. Доступ через Интернет к управлению вычислительной мощностью является одним из ключевых факторов облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, но в облачных средах они работают через Интернет. Корректное разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

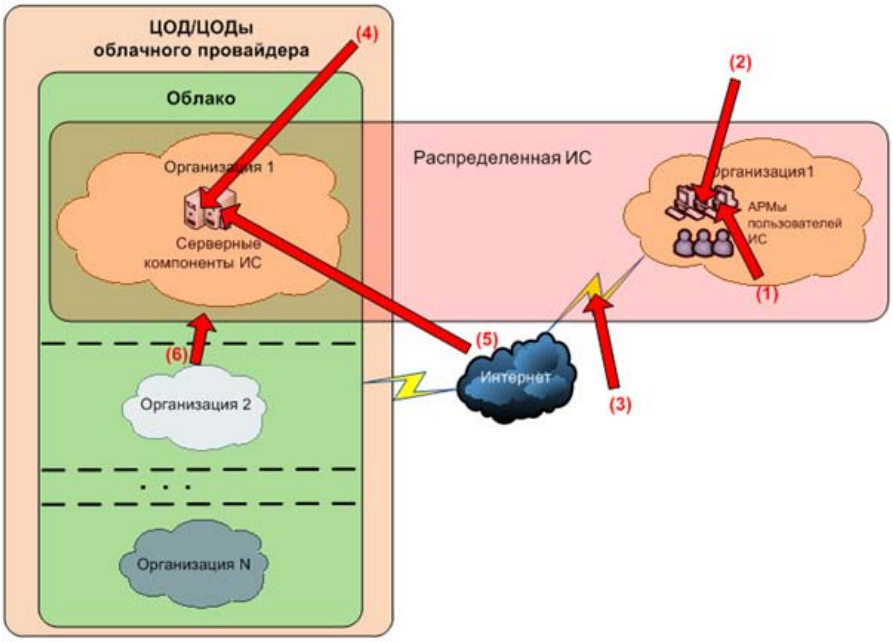

Рисунок 1 – Основные источники угроз для элементов облачной распределенной информационной системы:

1. **Внутренние пользователи организации, реализующие атаки на ресурсы информационной системы (ИС), размещенные на собственной площадке организации.**
2. **Внешние злоумышленники, реализующие атаки на ресурсы ИС, размещенные на площадке организации.**
3. **Внешние злоумышленники, атакующие снаружи канал связи с целью перехвата или искажения сетевого трафика.**
4. **Персонал облачного провайдера, обслуживающий компоненты облака.**
5. **Внешние злоумышленники, реализующие атаки из-за пределов ЦОД облачного провайдера на ресурсы облака и, соответственно, на ресурсы ИС, размещенные в облаке.**
6. **Соседи по облаку, которые используют слабые места платформы для атаки из своей облачной среды.**

– уязвимости внутри виртуальной среды. Серверы облачных вычислений и локальные серверы, как правило, используют одни и те же операционные системы и приложения. Тем не менее, для облачных систем угроза удаленного взлома или заражения вредоносными программами значительно выше. Соответственно, и риски использования виртуальных систем также более высоки. Информационная система обнаружения и предотвращения вторжений (ИСОПВ) должна быть способ-

на обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их пространственного расположения в облачной среде.

– защита бездействующих виртуальных машин. Когда виртуальная машина выключена, она подвергается опасности заражения, при этом обычного доступа к хранилищу образов виртуальных машин через сеть бывает вполне достаточно. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение, и в данном случаи должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

– защита периметра и разграничение сети. При использовании облачных вычислений периметр сети размывается или исчезает. Как следствие, уровень защиты наименее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с различными уровнями доверия в облаке виртуальные машины должны самостоятельно обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине, и корпоративный firewall, который является основным компонентом реализации политики безопасности и разграничения сегментов корпоративной сети, становится не в состоянии повлиять на серверы, размещенные в облачных средах.

Несмотря на множество возникающих проблем, часть из которых перечислена выше, облачные вычисления могут обеспечивать приемлемый уровень безопасности, который зависит от механизма развертывания и примененных мер безопасности. Тем не менее, слабая политика безопасности, а также отсутствие обучения персонала, могут стать веской причиной возникновения проблем и уязвимостей, что в свою очередь приведет к значительному риску.

Будем считать, что облачная система содержит ряд информационных объектов, имеющих определенную пространственную конфигурацию в облаках и требующих обеспечения некоторого допустимого уровня безопасности. Будем также считать, что имеется ряд субъектов обеспечения безопасности (СОБ), в задачи которых входит анализ уязвимостей облачной системы, выявление и анализ текущих и потенциальных угроз, а также выполнение определенных сценариев противодействия при обнаружении угрозы в рамках ИСОПВ, решающей задачи адаптивного планирования и координации взаимодействия СОБ с целью предотвращения различных угроз.

Надежность геолокационных облачных систем

Вопрос информационной безопасности может быть рассмотрен на примере облачных геолокационных сервисов. Одним из наиболее распространенных программных продуктов в данной сфере приложений является облачный сервис ArcGis Online [8]**.** С помощью ArcGIS Online можно создавать и использовать готовые карты и сцены, получать доступ к готовым слоям и инструментам, публиковать размещенные сервисы, распространять и получать доступ к картам с любого устройства, создавать карты на основе данных бизнес-таблиц.

ArcGIS Online реализует интерактивные карты и сцены, позволяющие пользователям просматривать, изучать и анализировать географические данные. Стратегия построения безопасных систем основана на промышленных стандартах, включающих системы эшелонированной защиты, предоставляющие возможность контролировать безопасность на любом уровне,

по каждому пользователю, включая приложения, сетевой уровень и материальную базу. Строгое соответствие приложений этим принципам позволяет получить уверенность в том, что ArcGIS Online предоставляет конфиденциальный, целостный и полный доступ к данным.

Исходя из данной стратегии, ArcGIS Online **предоставляет следующие меры безопасности:**

– все сотрудники, работающие с облачными ресурсами, находятся под постоянным наблюдением;

– доступ к базе данных пользователей ограничен списком специально отобранных сотрудников;

– состояние и доступность сервисов отображаются на web-странице.

Идентификация пользователя выполняется при помощи процедуры авторизации, которая всегда выполняется по защищенному протоколу HTTPS, разработанному как промышленный стандарт для обмена закрытой информацией. Программа использует облачную инфраструктуру, соответствующую международным стандартам безопасности ISO 27001 и SAS 70 Type 2.

Для поддержки принятия решений СОБ по обеспечению безопасности объектов облачных систем могут быть использованы сценарно-прецедентный подход [9] и позиционно-целевой метод управления [10].

ФОРМАЛИЗАЦИЯ ОПИСАНИЯ СИТУАЦИЙ ПРИ ВОЗНИКНОВЕНИИ УГРОЗЫ БЕЗОПАСНОСТИ

В соответствии со сценарно-прецедентным подходом в основу системы управления безопасностью облачных геолокационных систем могут быть положены следующие понятия: позиция, время, действие, сценарий, план, прецедент, проблемная ситуация [11].

Позиция описывает местонахождение объекта (субъекта) в заданной двух(трех)-мерной системе координат, и представляется в форме пары (тройки) вида $p=(\xi,\chi)$, где ξ, χ – координаты по соответствующим осям.

Время задается отсчетами t относительно начального значения t_0 на заданной временной шкале T, упорядоченной по $<_T$.

Пусть заданы множество угроз Ψ, множество субъектов обеспечения безопасности (СОБ) $Z=\{A,B,D,F\}$ и множество допустимых действий СОБ U. Каждый из СОБ $z\in Z$ в момент времени t выполняет некоторое действие $a_{z(t)}\in U$.

Триадой назовем кортеж вида $\langle p,t,a_{z(t)}\rangle$.

Триада является элементарным фрагментом планов и сценариев противодействия угрозам, триадой также может быть задана цель сценария (цель может состоять в достижении позиции p к моменту t, тогда $a_{z(t)}$ может быть нулевым).

Активность СОБ $z\in Z$ представлена его выполняемым сценарием Σ_z.

Сценарий Σ_z СОБ z представляет собой кортеж вида

$$\Sigma_z=\langle t_s,t_r,[...,\langle t_i,p_i,a_i\rangle,...],g\rangle, \qquad (1)$$

где $[...,\langle t_i,p_i,a_i\rangle,...]$ – упорядоченная последовательность триад, такая что $t_i <_T t_{i+1}$;

t_s – момент запуска выполнения сценария;

t_r – планируемый момент запуска;

$g=\langle t_e,p_e,a_e\rangle$ – конечная цель выполнения сценария,

t_e – конечный момент времени;

p_e – конечная позиция;

a_e – действие, выполняемое по дости-

жению конечной позиции $\langle t_e, p_e \rangle$.

Соответственно, для каждого СОБ $z \in Z$ в любой момент времени $t \in T$ можно получить его местоположение $p_{z(t)}$, выполняемый им сценарий Σ_z и, зная t_s, конкретное выполняемое действие $a_{z(t)}$.

Представленный способ формализации позволяет корректировать назначенную любому из СОБ $z \in Z$ цель g_z и/или выполняемый сценарий Σ_z «на лету», без перезапуска цикла функционирования ИСОПВ.

Угроза $\psi \in \Psi$ может быть представлена классом K_ψ и множеством нарушителей L, для каждого из которых $l \in L$ в любой момент времени $t \in T$ известно его местоположение $p_{l(t)}$

$$\psi_t = \left\langle K_\psi, \left\{ \left(l, p_{l(t)} \right), ... \right\} \right\rangle \ \forall l \in L. \qquad (2)$$

Позиционный контекст угрозы ψ_p описывается перечислением множества текущих позиций нарушителей $\psi_p = \left\{ \left(l, p_l \right), ... \right\} \ \forall l \in L$.

Каждой тактической операции Ω, выполняемой в ответ на угрозу $\psi \in \Psi$, соответствует множество участвующих в ней СОБ $Z_\Omega \subseteq Z$ и *план* мероприятий Π_Ω, представляющий собой кортеж вида

$$\Pi_\Omega = \left\langle \psi, Z_\Omega, \left\{ ..., \left(z(k), \Sigma_{z(k)} \right), ... \right\} \right\rangle, \qquad (3)$$

где $\left\{ ..., \left(z(k), \Sigma_{z(k)} \right), ... \right\}$ – множество выполняемых сценариев $\Sigma_{z(k)}$ для каждого СОБ $z(k) \in Z_\Omega$.

Позиционный контекст ситуации s_p содержит занимаемые СОБ $z \in Z$ позиции:

$$s_p = \left\{ ..., \left(z_i, p_{z_i} \right), ... \right\} \ \forall z_i \in Z. \qquad (4)$$

Операционный контекст ситуации s_Ω содержит множество выполняемых операций $\left\{ \Omega_j \right\}$, планов выполняемых операций $\left\{ \Pi_{\Omega(j)} \right\}$, множество участвующих СОБ $z\left(k_j\right) \in Z_{\Omega(j)}$ и соответствующих сценариев $\Sigma_{k(j)}$ для каждого из них [12]:

$$s_\Omega = \left\langle \left\{ \Omega_j \right\}, \left\{ \Pi_{\Omega(j)} \right\}, \left\{ Z_{\Omega(j)} \right\}, \left\{ \Sigma_{k(j)} \right\} \right\rangle \ \forall z\left(k_j\right) \in Z_{\Omega(j)}. \qquad (5)$$

Ограничением является то, что каждый из СОБ $z_k \in Z$ в любой момент времени t может выполнять один и только один сценарий Σ_{kj}, соответствующий плану Π_{Ω_j} операции $\Omega_j \in \Omega$, такой что $z\left(k_j\right) \in Z_{\Omega(j)}$. В случае, если в момент времени t СОБ $z(m) \in Z$ не участвует ни в одной из операций $\Omega_j \in \Omega$, т.е. $\forall j \ z\left(m_j\right) \notin Z_{\Omega(j)}$, считаем, что $z(m)$ выполняет заданный штатный сценарий $\Sigma_{z(m0)}$.

Тогда текущая *ситуация* s_t описывается конфигурацией угроз, текущими позиционным и операционным контекстами:

$$s_t = \left\langle s_{p(t)}, s_{\Omega(t)}, \left\{ \psi_{m(t)} \right\} \right\rangle \ \forall \psi_m \in \Psi. \qquad (6)$$

Представленный формализм описания ситуаций учитывает возможность возникновения множественных угроз, т.к. конфигурация угроз и операционный контекст описывают множества угроз и, соответственно, выполняемых операций противодействия.

В момент возникновения угрозы для облачных систем складывается *проблемная ситуация*, требующая своего разрешения путем выполнения операций предупреждения или противодействия.

Управление безопасностью облачной системы в проблемной ситуации возлагается на сценарно-прецедентную интеллектуальную систему.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

В статье проведен анализ работ в области обеспечения безопасности облачных вычислений, обоснована актуальность проблемы безопасности виртуальных систем. Перечислен ряд проблем**, с**вязанных с безопасностью и защитой облачных систем.

Рассмотрены средства и инструменты обеспечения безопасности для геолокационного облачного сервиса. В соответствии со сценарно-прецедентным подходом предложена формализация описания ситуаций при возникновении угроз безопасности, которая может быть использована для анализа, противодействия и предотвращения проблемных ситуаций в информационной системе обнаружения и предотвращения вторжений. Использование представленного в статье подхода помогает избегать серьезных атак на облачную систему и, как следствие, снизить риск ее применения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Makarov S.V. Social'no-jekonomicheskie aspekty oblachnyh vychislenij. – M.: CJeMI RAN, 2010.
2. Kovalenko O.S. Obzor problem i sostojanij oblachnyh vychislenij i servisov / O.S. Kovalenko, V.M. Kurejchik // Izvestija JuFU. Tehnicheskie nauki. – 2012. – №7. – S.146-153.
3. Shirokova E.A. Oblachnye tehnologii / E.A. Shirokova // Sovremennye tendencii tehnicheskih nauk: materialy mezhdunar. nauch. konf. – Ufa: Leto, 2011. – S.30-33.
4. Janjushkin V.V. Programmnye komponenty i arhitekturnye reshenija raspredelennyh informacionnyh sistem na osnove primenenija tehnologij cloud computing i WCF / V.V. Janjushkin // Perspektivy razvitija sredstv i kompleksov svjazi. Podgotovka specialistov svjazi: mat. mezhvuz. nauchn.-tehn. konf. – Novocherkassk: NVVKUS, 2009. – S.239-241.
5. Gul'tjaev A.K. Virtual'nye mashiny: neskol'ko komp'juterov v odnom / A.K. Gul'tjaev. – SPb.: Piter, 2006. – 224 s.
6. Sejtvelieva S.N. Oblachnye reshenija v biznese / S.N. Sejtvelieva // Razvitie nacional'noj jekonomicheskoj sistemy v uslovijah globalizacii: materialy vseukr. konf. – Simferopol': OAO «Simferopol'skaja gorodskaja tipografija», 2011. – S.355-356.
7. Solov'ev A.V. Ot reglamentov tradicionnogo formal'nogo obrazovanija k «zolotym kletkam» virtual'nyh uchebnyh sred i svobode oblachnyh servisov / A.V. Solov'ev, A.A. Men'shikova // Distancionnoe i virtual'noe obuchenie. – 2011. – №12. – S.12-23.
8. Gohman V.V. ArcGIS v oblake / V.V. Gohman // ArcReview. – 2010. – №3(54).
9. Sherstjuk V.G. Osnovy teorii dinamicheskih scenarno-precedentnyh intellektual'nyh sistem / V.G. Sherstjuk. – Herson: Feniks, 2012. – 476 s.
10. Sherstjuk V.G. Pozicionno-celevoe upravlenie podvizhnymi obektami v polijergaticheskih sistemah / V.G. Sherstjuk // Vestnik Hersonskogo nacional'nogo tehnicheskogo universiteta. – 2012. – №1(44). – S.18-26.
11. Sherstjuk V.G. Scenarno-precedentnoe upravlenie jergaticheskimi dinamicheskimi obektami / V.G. Sherstjuk. – Saarbrucken, Deutschland: Lambert Academic Publishing, 2013. – 407 p.
12. Sherstjuk V.G. Scenarno-precedentnoe upravlenie bezopasnost'ju territorial'no raspredelennogo obekta / V.G. Sherstjuk, N.A. Kozub // Vestnik Hersonskogo nacional'nogo tehnicheskogo universiteta. – 2013. – №1(46). – S.243-251.

Рецензент: д.т.н., проф. Рудакова А.В.
Херсонский национальный технический университет