УДК 004.056

ТЕХНОЛОГИЯ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ НА БАЗЕ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Волков С.Д.

Московский государственный лингвистический университет,
г. Москва, Российская Федерация

Научный руководитель: Царегородцев А.В. – д-р техн.наук, профессор, профессор кафедры международной информационной безопасности Института информационных наук ФГБОУ ВО МГЛУ, проректор по развитию и информатизации ФГБОУ ВО МГЛУ

Аннотация. В статье предлагается технология организации противодействия компьютерным атакам на информационно-телекоммуникационные системы на базе технологии облачных вычислений, для чего рассматривается типовой порядок действий нарушителя по реализации компьютерной атаки. В целях определения противодействия компьютерным атакам формулируются принцип разработки подходов и моделей к выявлению и противодействия компьютерным атакам. На его основе предлагается способ оценки устойчивости систем в условиях реализации компьютерных атак. Предложенная технология организации противодействия позволяет обеспечить динамический мониторинг состояния системы на основе выявления сценариев развития компьютерных атак.

Ключевые слова: информационная безопасность, облачные вычисления, компьютерные атаки.

Введение. Мировое сообщество каждый день сталкивается с новыми вызовами в киберпространстве. Угрозы кибербезопасности могут исходить от самых различных лиц и групп. Это могут быть лица, которые проводят атаки ради развлечения, а могут быть крупные группировки с распределенной сетью (организованная преступность), которые действуют с целью получения выгоды. Обнаружение на ранней стадии развития атаки позволит предотвратить нанесение крупного ущерба организации.

Вместе с этим, в настоящее время наблюдается повышенный спрос на информационные продукты и услуги, интегрирующие в своей базе технологию облачных вычислений.

ГОСТ ИСО/МЭК 17788-2016 дает следующую формулировку технологии облачных вычислений: «облачные вычисления – парадигма для предоставления возможности сетевого доступа к масштабируемому и эластичному пулу общих физических или виртуальных ресурсов с предоставлением самообслуживания и администрированием по требованию» [8].

По данным *IDC* и *Gartner,* с 2016 года рынок облачных сервисов вырос более чем вдвое. Это подчеркивает растущую зависимость от облачной инфраструктуры и платформ, используемых организациями. По данным 2020 года, в 2019 году объём отрасли облачных вычислений в денежном выражении составил $233,4 млрд. Это на четверть (26 %) больше по сравнению с результатом за 2018-й, когда доход равнялся $185,2 млрд. [2].

Кроме того, на фоне пандемии новой коронавирусной инфекции *COVID*-19 в 2020 году, многие компании оказались ограничены в финансовых ресурсах, в результате чего были вынуждены решать проблему оптимизации затрат [3]. Использование облачных сервисов стало для них прекрасным решением проблемы: приобретая облачные сервисы, нет нужды тратить большие средства на создание собственных центров обработки данных, лицензионное программное обеспечение и квалифицированный персонал. Однако данное преимущество, при всем его удобстве, приводит к возникновению новых актуальных угроз информационной безопасности, связанных, прежде всего, с уменьшением возможности контроля процессов обработки информации, а также с динамичностью модели предоставления ресурсов [4]. Таким образом, при внедрении и переходе на использование облачных вычислений возникает

противоречие между увеличением эффективности основных производственных процессов в организации, с одной стороны, и возникновением новых угроз информационной безопасности – с другой. Реализация угроз информационной безопасности – компьютерных атак, приводит к финансовым и репутационным потерям для любой организации. Именно поэтому организация противодействия компьютерным атакам является первостепенной задачей при построении системы защиты информации как в организации-поставщике облачных сервисов, так и в организации-потребителе.

Технология облачных вычислений несмотря на то, что считается дальнейшим развитием технологии распределенных («грид») вычислений, имеет существенные особенности.

Технология распределенных («грид») вычислений представляет собой вычислительную архитектуру, в которой вычислительные ресурсы используются в совместной модели для параллельной обработки процессов, направленных на решение одной конкретной задачи или определенного блока задач. При этом каждый вычислительный ресурс является общим для всех элементов модели в сети и позволяет равноправно использовать всю доступную вычислительную мощность.

По словам автора термина «грид вычисления», Яна Фостера, эволюция технологии облачных вычислений заключается в том, что вместо предоставления «сырых» вычислительных ресурсов и ресурсов хранения, эта технология предоставляет ресурсы в виде сервисов.

Модель облачных вычислений включает в себя пять основных характеристик, три модели сервиса и четыре модели развёртывания [1, 8].

Во-первых, облачные вычисления подразумевают самообслуживание «по-требованию». Потребители могут в одностороннем порядке получить вычислительные ресурсы (такие как процессорное время или сетевое хранилище) когда это требуется автоматически без необходимости взаимодействия с каждым сетевым провайдером.

Во-вторых, вычислительные ресурсы доступны повсюду в сети, доступ осуществляется при помощи стандартных механизмов, которые содействуют использованию разнородных тонких и толстых клиентских платформ (например, мобильные телефоны, планшетные и настольные компьютеры, ноутбуки).

В-третьих, вычислительные ресурсы провайдера объединяются для обслуживания множества потребителей, используя многопользовательскую модель с различными физическими и виртуальными ресурсами, назначаемыми и переназначаемыми динамически в зависимости от запросов потребителя. Складывается ощущение физической независимости, в котором потребители, главным образом, не контролируют или не знают о настоящем местоположении предоставляемых ресурсов, но местоположение может быть указано на высоком уровне абстракции (например, страна, штат или центр обработки данных). Примеры таких ресурсов включают хранилища данных, процессорное время, память и пропускную способность сети.

В-четвертых, вычислительные ресурсы могут быть динамически выделены, переданы и освобождены автоматически, в соответствии с требованиями потребителя. Для потребителя вычислительные возможности, пригодные для резервирования, часто кажутся неограниченными и могут быть выделены в любом количестве в любое время.

В-пятых, облачные системы автоматически контролируют и оптимизируют ресурсы, используя измерение вычислительных ресурсов на некотором уровне абстракции в зависимости от типа обслуживания (например, хранилище данных, время на обработку, пропускная способность и активные учетные записи пользователей). Информация об использующихся ресурсах может собираться, контролироваться, формироваться в отчёт, предоставляя прозрачность как для провайдера, так и для потребителя использованного сервиса [7].

В соответствии с используемой в настоящее время моделью, облачные вычисления могут предоставляться в следующем виде:

– программное обеспечение как сервис (*Software as a Service, SaaS*). Вычислительные ресурсы, предоставляемые потребителям, используют приложения поставщиков услуг, которые запущены в облачной инфраструктуре. Приложения доступны с различных устройств клиентов (как правило, через веб-браузер). Потребители не могут управлять и контролировать лежащую в основе облака инфраструктуру, включая сеть, серверы, операционные системы, хранилища данных или возможности конкретного приложения;

– платформа как сервис (*Platform as a Service, PaaS*). Вычислительные ресурсы, предоставляемые потребителям, базируются на облачной инфраструктуре, созданной самим потребителем, или полученных приложениях, созданных с использованием языков программирования, библиотек, инструментов, поддерживаемых провайдером. Потребители не управляют и/или не контролируют лежащую в основе облака инфраструктуру, включая сеть, сервера, операционные системы или хранилища данных, но они контролируют другие разворачиваемые приложения и возможные настройки конфигурации для среды размещённых приложений;

– инфраструктура как сервис (*Infrastructure as a Service, IaaS*). Вычислительные ресурсы, предоставляемые потребителям, – это время обработки, хранилища данных, сети и другие фундаментальные компьютерные ресурсы, с помощью которых потребители могут развёртывать и запускать произвольное программное обеспечение, которое может включать операционные системы и приложения. Потребители не могут управлять или контролировать лежащую в основе облака инфраструктуру, но имеют контроль над операционными системами, хранилищами данных и развёртываемыми приложениями.

Модель определяет способы развертывания облачных технологий [7]:

– частное облако. Инфраструктура облака предоставляется в исключительное пользование одной организации, содержащей несколько потребителей (например, ими могут быть сотрудники организации). Оно может принадлежать, администрироваться и использоваться организацией, третьим лицом или некоторым их сочетанием. Облако может размещаться в территориальных пределах организации или независимо от неё;

– публичное облако. Инфраструктура облака предоставляется в открытое использование для всех. Оно может принадлежать, администрироваться и использоваться компаниями, университетами, государственными организациями, или их некоторым сочетанием. Облако размещается в помещениях поставщика услуг;

– гибридное (смешанное) облако. Инфраструктура облака состоит из двух или более облачных инфраструктур (частное облако, коллективное облако или публичное облако), которые остаются уникальными сущностями, но, тем не менее, связаны между собой стандартизованными или запатентованными технологиями, которые могут включать портативность данных и приложений [9];

– коллективное облако (облако для сообществ). Инфраструктура облака предоставляется в исключительное пользование некоторому сообществу потребителей из организаций, которые имеют общие интересы (например, общие задачи, требования по безопасности, политику или совместное обслуживание). Оно может принадлежать, администрироваться и использоваться одной или более организациями в сообществе, третьими лицами или некоторым их сочетанием. Облако может размещаться в территориальных пределах организации или независимо от неё [7].

Структура модели облачных вычислений будет иметь вид, представленный на рис. 1.

Рисунок 1 – Модель облачных вычислений

Таким образом, легко понять, что технология облачных вычислений обеспечивает более высокий уровень абстракции (в сравнении с технологией «грид вычислений»), предоставляя вычислительные ресурсы конечным пользователям (будь то частные клиенты или организации) в виде сервисов в требуемом им количестве и объеме.

Организация противодействия компьютерным атакам. Для организации противодействия компьютерным атакам предлагается рассмотреть взаимосвязь способов выявления компьютерных атак на информационно-телекоммуникационные системы на базе облачных вычислений, анализа принципов функционирования таких систем и поиска уязвимых мест в технологии их функционирования, а также оценки устойчивости функционирования систем в условиях воздействия компьютерных атак [5].

При применении такого подхода, технология организации противодействия компьютерным атакам на информационные системы на базе облачных вычислений будет включать в себя:

1. Способы оценки действий нарушителя и выявления возможных сценариев развития компьютерных атак;
2. Способы оценки текущего состояния защищенности системы на базе облачных вычислений;
3. Подходы и модели к выявлению и противодействия компьютерным атакам;
4. Способы оценки устойчивости функционирования систем на базе облачных вычислений.

Способ оценки действий нарушителя и выявления возможных сценариев развития компьютерных атак. Для оценки действий нарушителя и выявления возможных сценариев развития компьютерных атак предлагается рассмотреть жизненный цикл атаки, представленный на рис. 2.

Рисунок 2 – Жизненный цикл атаки

Атака на информационные системы, как и любой другой вид воздействия, имеет свой жизненный цикл, состоящий из нескольких этапов [6].

Этап первый – подготовка. В ходе этого этапа нарушитель пытается добыть как можно больше информации об информационной системе, как объекте атаки. На основе анализа данной информации нарушитель может планировать свои дальнейшие действия. Такой информацией, например, может выступать информация о типе и версии операционной системы, список пользователей информационной системы, перечень используемого прикладного программного обеспечения и т.д.

Этап второй – вторжение. В ходе этого этапа нарушитель пытается получить несанкционированный доступ к ресурсам атакуемой информационной системы. Он может делать это в том числе и для сбора дополнительной информации об информационной системе.

Этап третий – атакующее воздействие. В рамках этого этапа нарушитель реализует свои корыстные цели, ради которых он совершал атаку. Примерами таких воздействий являются любые нарушения конфиденциальности, целости и доступности информации, циркулирующей в системе. Например, это могут быть нарушение работы информационной системы, кража конфиденциальной информации, модификация, блокирование, удаление данных из системы; а применительно к системам облачных вычислений к примерам воздействий можно отнести: атаки типа «отказ в обслуживании» (не являются специфичными для облачных вычислений, однако все равно широко распространены), перехват передаваемых данных, повышение прав доступа, несанкционированный доступ к виртуальной машине, на которой запущен облачный сервис, нарушение работы гипервизора или его компонентов, нарушение изоляции виртуальной машины, внедрение вредоносного кода в виртуальную машину или облачный сервис и др.

Этап четвертый – развитие атаки. Атакующий злоумышленник может стремиться атаковать и другие объекты, расположенные, к примеру, в той же локальной вычислительной сети, чтобы продолжить достижение своих целей по нарушению конфиденциальности, целостности и доступности данных информационной системы.

Таким образом, выявление возможных сценариев развития компьютерных атак строится на анализе множества возможных действий нарушителя, т.е. его потенциала (см. рис. 3):

Рисунок 3 – Схема оценки действий нарушителя

Способ оценки текущего состояния защищенности системы на базе облачных вычислений. Для оценки текущего состояния защищенности системы на базе облачных

вычислений предлагается проводить мониторинг уязвимых мест в технологии функционирования систем на базе облачных вычислений (см. рис. 4). Для этого существует несколько способов. Один из них основан на вероятностной методике, и при его применении в общем виде нужно опираться на следующие факторы:

– потенциал злоумышленника (рассчитывается на основе экспертной оценки в соответствии с моделями угроз и нарушителя);

– источник угрозы (где возможна атака, в зоне видимости или за ее пределами);

– метод воздействия (сетевой, аппаратный или социальный);

– объект угрозы (корпоративные данные, средства для шифрования, передачи, работы с ними или сотрудники компании).

Рисунок 4 – Схема оценки состояния защищенности системы

В процессе мониторинга уязвимых мест в системе крайне важно учитывать возможные «точки входа» нарушителя (ошибки в процессе исполнения системного и прикладного программного обеспечения, позволяющие получить несанкционированный доступ к системе, осуществить повышение привилегий, выйти за пределы «песочницы» и др.).

Организация такого мониторинга предполагает использование специализированного программного обеспечения, осуществляющего мониторинг на основе как вручную заданных параметров (потенциал злоумышленника, источник угрозы, метод воздействия, объект угрозы), так и автоматически собираемых системных свойств (версии системного и прикладного программного обеспечения, установленные обновления и др.).

Принцип разработки подходов и моделей к выявлению и противодействия компьютерным атакам. Защищенность системы на базе облачных вычислений определяется сегодня не только применением как традиционных организационных и технических подходов к защите информации, но и использованием систем обнаружения или предотвращения компьютерных атак.

Среди них выделим такие, как Snort, *Suricata, Bro, OSSEC, STAT* и *Prelude*. Все эти системы можно разделить на два класса – сетевые (*network-based, NIDS*) и узловые (*host-based, HIDS*). Сетевые системы (например. *Snort, Suricata, Bro*) основаны на принципе анализа сетевых пакетов данных. Такие системы просматривают сетевой трафик защищаемого сетевого сегмента, защищая тем самым входящие в этот сегмент информационные системы. Узловые системы (например, *OSSEC, STAT*) анализируют информацию, расположенную на конкретной информационной системе. Это позволяет определять только те системные процессы, которые имеют отношение к конкретной атаке, что повышает эффективность работы системы [6].

Разработка подходов и моделей к выявлению и противодействию компьютерным атакам для систем на базе облачных вычислений производится на основе анализа состояния защищенности системы и анализа действий нарушителя. Подход к выявлению и противодействию компьютерным атакам предусматривает выявление признаков компьютерных атак, анализ сценариев развития атак и выработку действий по реакции на выявленные атаки. Модель выявления и противодействия компьютерным атакам включает в себя описание функционирования системы на базе технологии облачных вычислений в ходе

сбора, обработки и передачи информации, топологию сети передачи данных, возможные сценарии атак и реакцию средств противодействия на них соотнесенные с действиями по противодействию выявленным атакам (см. рис. 5).

Рисунок 5 – Принцип разработки подходов и моделей к выявлению и противодействия компьютерным атакам

Способ оценки устойчивости функционирования информационно-телекоммуникационных систем на базе облачных вычислений. Под устойчивостью функционирования информационных систем на базе облачных вычислений понимается способность системы обеспечивать штатное исполнение заданных функций в условиях воздействия компьютерных атак.

В условиях воздействия компьютерных атак на систему на базе облачных вычислений существует потенциальная опасность невыполнения системой процессов системного или прикладного программного обеспечения. Следствием подобных воздействий будет срыв (некачественное выполнение) установленного порядка обработки информации в системе.

Для оценки устойчивости функционирования систем на базе облачных вычислений предлагается способ, основанный на критериях ГОСТ Р ИСО 22301-2014 «Системы менеджмента непрерывности бизнеса. Общие требования» [7].

В ходе штатного функционирования системы, время, затрачиваемое системой на исполнение того или иного процесса можно обозначить как $T_{штат}$.

Обозначим $T_{крит}$ максимальное время исполнения процесса в системе. Если для исполнения процесса системе требуется время, превышающее $T_{крит}$, следует говорить о снижении или потере устойчивости функционирования системы. В терминологии ГОСТ Р ИСО 22301-2014 применяется формулировка «максимально приемлемый период нарушения» (*MTPD*), то есть время, по истечении которого неблагоприятные последствия, возникшие в результате необеспечения поставок продукции/услуг или невыполнения деятельности, становятся неприемлемыми.

При обнаружении атаки система обнаружения вторжений должна потратить время на противодействие атаки. В это время исполнение системного процесса может быть замедлено или приостановлено. Обозначим время, затрачиваемое системой на противодействие атаке как $T_{прот}$. В терминологии ГОСТ Р ИСО 22301-2014 применяется формулировка «целевое время восстановления» (*RTO*) то есть период времени, установленный для возобновления поставок продукции или услуг, возобновления деятельности или восполнения ресурсов после инцидента.

Схема оценки устойчивости функционирования систем на базе облачных вычислений приведена на рис. 6.

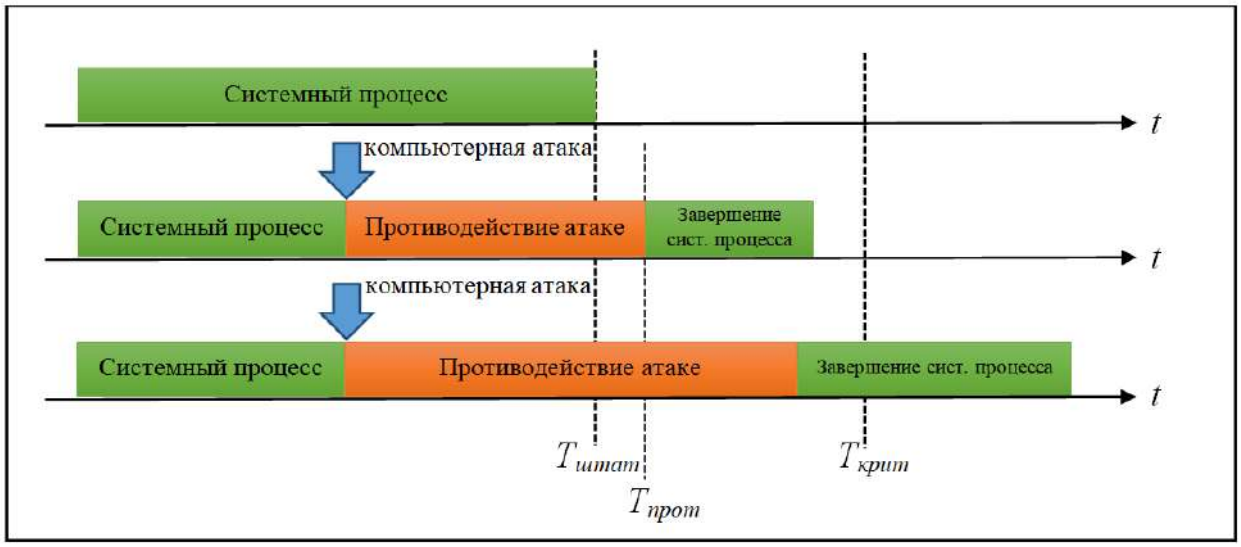

Рисунок 6 - Схема оценки устойчивости функционирования систем на базе облачных вычислений

Тогда, для обеспечения устойчивости функционирования системы необходимо чтобы выполнялись следующие условия:

$$\begin{cases} T_{\text{прот}} \to min \\ T_{\text{прот}} < T_{\text{крит}} \end{cases}.$$

Для повышения устойчивости функционирования систем на базе технологии облачных вычислений необходим комбинированный метод противодействия компьютерным атакам, который гибко использует элементы сигнатурного анализа, выявления аномалий и анализа динамически выполняемых функций системы [10].

Методы сигнатурного анализа, используемые в системах противодействия компьютерным атакам, основаны на постоянном мониторинге пакетов данных в сети с целью последующего их сравнения с заранее определенной в защищаемой системой базой данных сигнатур атак. К достоинствам данных методов следует отнести низкие требования к вычислительным ресурсам защищаемой системы, высокую скорость работы и высокий уровень достоверности распознавания компьютерных атак. Основным недостатком данных методов является невозможность обнаружения новых (не определенных в базе данных сигнатур) компьютерных атак, что может создать угрозу безопасности в случае применения систем противодействия компьютерным атакам, основанных исключительно на данном методе. Обобщенная структура метода сигнатурного анализа (для систем обнаружения компьютерных атак) приведена на рис. 7.

Методы выявления аномалий основаны на использовании математических моделей для описания штатного функционирования защищаемой системы и последующей фиксации отклонений от него. В зависимости от выявления отклонения принимается решение об обнаружении атаки. Чаще всего применяются статистические модели (вероятностные модели, кластерный анализ), модели марковских цепей, модели конечных автоматов и модели на основе искусственных нейронных сетей (приведена в качестве примера на рис. 8).

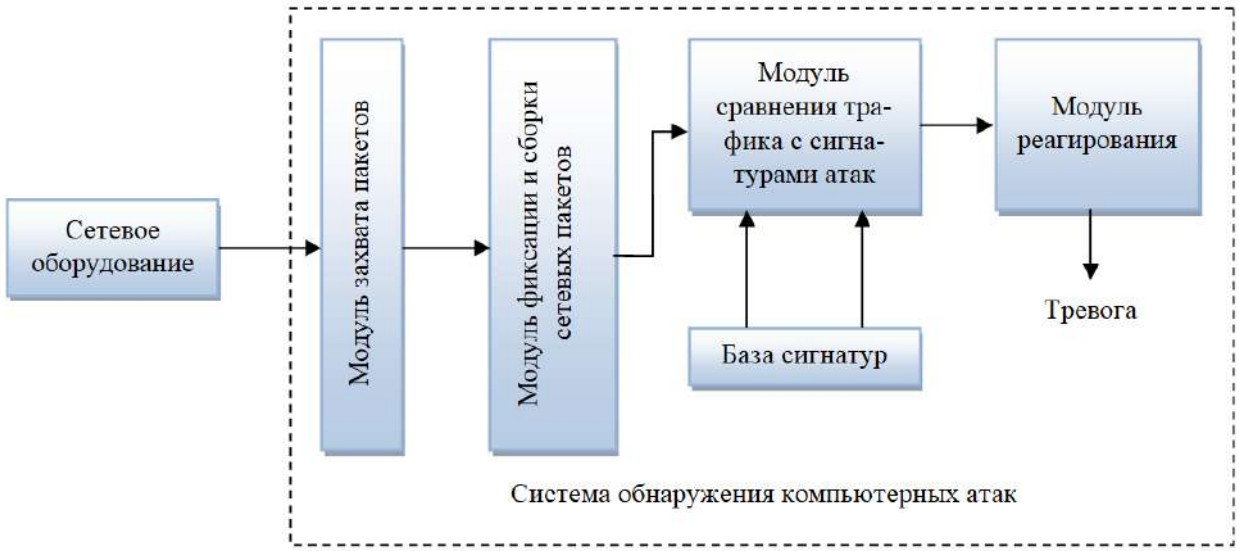

Рисунок 7 – Обобщенная структура метода сигнатурного анализа (на примере системы обнаружения компьютерных атак)

Преимуществом данных методов является способность обнаруживать компьютерные атаки, не определенные в системе, то есть не известные ей. Существенными недостатками данного метода являются высокие требования к аппаратному обеспечению, а также высокая сложность при создании выборки данных (обучающая выборка), описывающих штатное функционирование защищаемой системы.

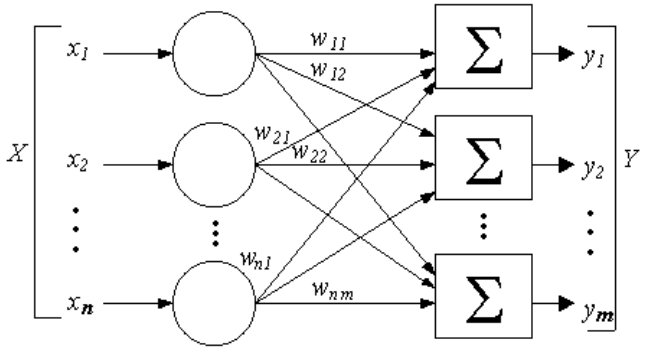

Рисунок 8 – Структура метода выявления аномалий (на примере искусственных нейронных сетей).
X – множество признаков компьютерных атак, Y – множество вероятностей обнаружения компьютерных атак, W – множество весовых коэффициентов каждого нейрона сети, Σ - функция активации

Заключение. В настоящее время отсутствуют унифицированные решения по противодействию компьютерным атакам и обнаружению аномального поведения применительно к системам, функционирующих на основе технологии облачных вычислений.

Предложенный в данной работе подход к организации противодействия компьютерным атакам на информационные системы на базе облачных вычислений позволяет осуществлять динамический мониторинг и анализ состояний защищаемой системы на основе анализа сетевых потоков данных, раннего выявления признаков атак как исходя из сигнатурного анализа, так и по обнаружению аномального поведения на основе выявления сценариев развития компьютерных атак.

Однако для эффективного применения предложенной технологии противодействия компьютерным атакам и минимизации вычислительных ресурсов при её применении целесообразна разработка типовых сигнатур для технического описания характеристик атак, специфичных для облачной среды, а также разработка типовых характеристик функционирования гипервизоров.

Список литературы

1. *Tsaregorodotsev, A. V., Lvovich, I. Ya., Shikhaliev, M. S., Zelenina, A. N., Choporov, O. N. Information security management for cloud infrastructure. International Journal on Information Technologies and Security, 2019, Vol. 11, № 3, pp. 91-100.*

2. *Облачные вычисления (мировой рынок) [сайт] / URL: https://www.tadviser.ru/index.php/Статья:Облачные_вычисления_(мировой_рынок), свободный. – Дата обращения 14.03.2022.*

3. *Обзор: Облачные сервисы 2020 [сайт] / Режим доступа: https://www.cnews.ru/reviews/oblachnye_servisy_2020/articles/pandemiya_rasshirila_dorogu_v_oblaka, свободный. – Дата обращения 14.03.2022.*

4. *Волков С.Д., Царегородцев А.В. Один из подходов к обеспечению защиты от компьютерных атак при реализации информационной функции государства на внутреннем уровне // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2020. № 36. С. 159-174.*

5. *Климов С.М. Методы и модели противодействия компьютерным атакам. Люберцы: КАТАЛИТ, 2008. СС. 64-64.*

6. *Волков С.Д. Обзор подходов к построению систем обнаружения компьютерных атак для информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений // Collegium Linguisticum - 2017. Материалы ежегодной конференции студенческого научного общества МГЛУ. 2017. М.: ФГБОУ ВО МГЛУ. С. 442-447.*

7. *ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200113802, свободный. – Дата обращения 14.03.2022.*

8. *ГОСТ ISO/IEC 17788-2016 Межгосударственный стандарт. Информационные технологии. Облачные вычисления. Общие положения и терминология. — Текст : электронный // Электронный фонд правовых и нормативно-технических документов : [сайт]. — URL: https://docs.cntd.ru/document/1200141425 (дата обращения: 14.03.2022).*

9. *Царегородцев А.В., Мухин И.Н., Боридько С.И. Один из подходов к построению информационной инфраструктуры организации на базе гибридной облачной среды // Информация и безопасность. Воронеж: Воронежский государственный технический университет, 2015. Т. 18(3). СС. 400-403.*

10. *Логинова А.О. Классификация существующих методов выявления инцидентов информационной безопасности // Информационные технологии в науке, бизнесе и образовании. Сборник трудов IX Международной научно-практической конференции студентов, аспирантов и молодых ученых. 2017. М.: ФГБОУ ВО МГЛУ. С. 40-44.*

UDC 004.056

TECHNOLOGY OF RESPONSE ORGANIZATION TO COMPUTER ATTACKS ON INFORMATION AND TELECOMMUNICATION SYSTEMS BASED ON CLOUD COMPUTING TECHNOLOGY

Volkov S.D.

Moscow State Linguistic University, Moscow, Russia

Tsaregorodtsev A.V. – Dr. Tech. Sc., professor, professor of the Department of Information Security, Vice-rector for Development and Informatization of Moscow State Linguistic University

Abstract. The article proposes a technology of response organization to computer attacks on information and telecommunication systems based on cloud computing technology. A typical procedure of the intruder's actions to implement a computer attack is proposed. In order to determine computer attacks response actions, the principle of development of approaches and models for computer attacks detecting and responding is formulated. Based on it, a method for assessing the stability of systems under the conditions of computer attacks is proposed. The proposed technology of response organization makes it possible to provide dynamic monitoring of the state of the system based on the identification of scenarios of computer attacks development.

Keywords: information security, cloud computing, computer attacks.