УДК: 621.391

МЕТОДЫ ОЦЕНКИ РИСКА НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ В ФИНАНСОВЫХ И БАНКОВСКИХ СИСТЕМАХ

Ж.Б. Балтаев
Доцент кафедры «Информационных систем и цифровых технологий» ТФИ, PhD, доцент
j_baltayev@tfi.uz

С.Д. Арзикулов
Старший преподователь кафедры «Информационные системы и цифровые технологии» ТФИ,
arzikulov.sunnatulla@gmail.com

М.А. Миржамолова
Ассистент кафедры «Информационных систем и цифровых технологий» ТФИ,
dizafa@icloud.com

Ж.Б. Балтаев

Обучался в Ташкентском университете информационных технологий. Закончил бакалавриатуру в 2010 году, а магистратуру в 2013 году. 2020 году защитил диссертацию по специальности «05.04.01 - Телекоммуникационные и компьютерные системы, телекоммуникационные сети и информационные устройства. Распределение информации». Получил научную степень доктора философии по техническим наукам (PhD). Трудовую деятельность начал в Ташкентском университете информационных технологий (2013-2020), продолжил работу в Ташкентский государственный транспортный университет (2020-2023), в данный момент работает в Ташкентском финансовом институте (2023-н.в.).

С.Д. Арзикулов

Обучался в Ташкентском государственном университете (ныне Национальный университет Узбекистана имени Мирзо Улугбека) факультет прикладная математика и механика. Закончил в 1989 году, в специальности прикладной математика. Трудовую деятельность начал в Научном исследовательском институте «Алгоритм» при НПО «Кибернетика» (1989-2004), продолжил работу в Ташкентском университете информационных технологий (2004-2021), в данный момент работает в Ташкентском финансовом институте (2022-н.в.).

М.А. Миржамолова

В 2011 году я училась в Ташкентском Государственном Педагогическом Университете (бакалавр). В 2017 году я училась в Ташкентском университете информационных технологий имени Мухаммад ал Хоразми (степень магистра). С 5 сентября 2022 года работаю ассистентом кафедры «Информационных систем и цифровых технологий» Ташкентского финансового института.

Аннотация: Оценка рисков информационной безопасности (ИБ) в среде облачных вычислений (СОВ) являются важным методом в обеспечении ИБ в целом. Управление рисками ИБ представляет собой непрерывный процесс идентификации, оценки и минимизации рисков от реализации угроз ИБ. За последние несколько лет в отрасли информационных технологий получила развитие новая парадигма – «облачные вычисления». Облачные вычисления -это модель предоставления повсеместного и удобного сетевого доступа (по мере необходимости) к общему пулу конфигурируемых вычислительных ресурсов (например, сетей, серверов, систем хранения, приложений и сервисов), которые могут быть быстро предоставлены и освобождены с минимальными усилиями по управлению и необходимостью взаимодействия с провайдером услуг (сервис-провайдером). Далее по после того как будет произведена оценка, необходимо сопоставить уровень риска и контрмеры которые на дынный момент используются владельцем. После чего принимается решение о критичности положения и необходимости тех или иных действий по безопасности

Ключевые слова: Информационной безопасности, среде облачных вычислений, управление риск, эталонная модель, модель с нарушением, AnyLogic, NetworkEnter, NetworkMoveTo, NetworkRelease, Delay, Selectoutput, Sink

Введение.

В финансовых и банковских системах облачные вычисления - это модель, обеспечивающая (по мере необходимости) повсеместный и удобный сетевой доступ к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, систем хранения, приложений и сервисов), которые могут быть быстро предоставлены и освобождены с минимальными усилиями по управлению и необходимостью взаимодействия с провайдером услуг (сервис-провайдером).

Анализ результатов исследований, ведущихся в направлении обеспечения ИБ в среде облачных вычислений (СОВ) показывает, что в настоящее время не до конца решены вопросы, связанные с оценкой ИБ. В первую очередь это касается используемых моделей и методов оценки ИБ в среде облачных вычислений на основе риск – ориентированного подхода.

Отсутствие показателей оценки ИБ создает неопределенность в понимании того:

–в каком состоянии находится ИБ СОВ;

– какова эффективность методов и средств защиты в отношении

повышения ИБ.

Среди первоочередных задач по выработке подходов к обеспечению информационной безопасности облаков необходимо отнести следующие:

1. Исследование вопросов наличия уязвимостей виртуальных сред;
2. Построение классификации уязвимостей виртуальных сред;
3. Разработку типовой модели угроз для виртуальных сред;

На сегодняшний день существуют два подхода к оценке ИБ СОВ:

–качественный;

–количественный.

В системе управления процесс оценки риска является составной частью процесса управления рисками. Под управлением рисками понимается оценка и уменьшение рисков, которые могут воздействовать на СОВ.

Качественный подход к оценке рисков ИБ СОВ. Качественные методологии, используемые для оценки ИБ СОВ, исходят из того, что зачастую потенциальные потери неосязаемы, поэтому опасность или риск ИБ СОВ в результате реализации той или иной угрозы нельзя представить в каком-либо выражении.

В настоящее время известно множество методов качественной оценки рисков, большинство из которых построено на использовании табличных методов. Другие подходы предлагают графическое изображение дерева решения, которое показывает распределение вероятностей самых общих случаев.

Ни одно из указанных направлений не способно в отдельности обеспечить получение объективной, представительной и конструктивной оценки ИБ СОВ.

Количественный подход к оценке рисков ИБ СОВ. Рациональное применение разнообразных средств защиты информации в СОВ с учетом критерия экономической эффективности – это сложная научно-техническая задача. Умножая величину ущерба на число вероятных реализаций угрозы, получают грубый уровень риска от данной угрозы.

При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты.

Распространенные методики анализа рисков:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

созданию имитационной модели для оценки рисков ИБ СОВ, основной идеей которой является реализация эксперимента, являющегося одним из методов оценки риска ИБ. Было принято решение произвести оценку риска через атаки, реализуемые в данном эксперименте.

В ходе анализа существующих угроз, уязвимостей и атак было принято решение для сравнительного анализа произвести оценку СОВ с точки зрения ее безопасности (защищенности) смоделировать модель и рассмотреть три случая:

1. «Эталонная модель», указывающую на нормальное функционирование СОВ с отсутствием всяческих воздействий со стороны злоумышленника;
2. «Модель с нарушением ИБ» не удовлетворяющая нормативным уровням защищенности, заданным в ходе моделирования и эксперимента;
3. «Модель с нарушением ИБ» удовлетворяющая нормативным уровням защищенности, заданным в ходе моделирования и эксперимента.

Рассмотрим процесс мультиагентного моделирования в среде имитационного моделирования AnyLogic с целью анализа наиболее распространённых угроз ИБ по средствам таких механизмов, как атаки типа «отказ в обслуживании».

В краткости рассмотрим методику реализации данных атак в среде AnyLogic.

Архитектура исследуемого фрагмента простейшей сети показана на рисунке, и включает в состав: 3 ISP, к которым обращаются 6 пользователей, в том числе 3 злоумышленника, также присутствует система обеспечивающая информационную безопасность СОВ.

Для построения модели используем библиотеку сетевые элементы палитры Enterprise Library. Рассмотрим подробно сеть пользователей и злоумышленников. В пользовательской сети присутствует три клиента, которые генерируют запрос на среду облачных вычислений. Ресурсы каждого клиента отличаются, однако они объединяются в пользовательскую сеть и создают общую нагрузку на систему облачных вычислений.

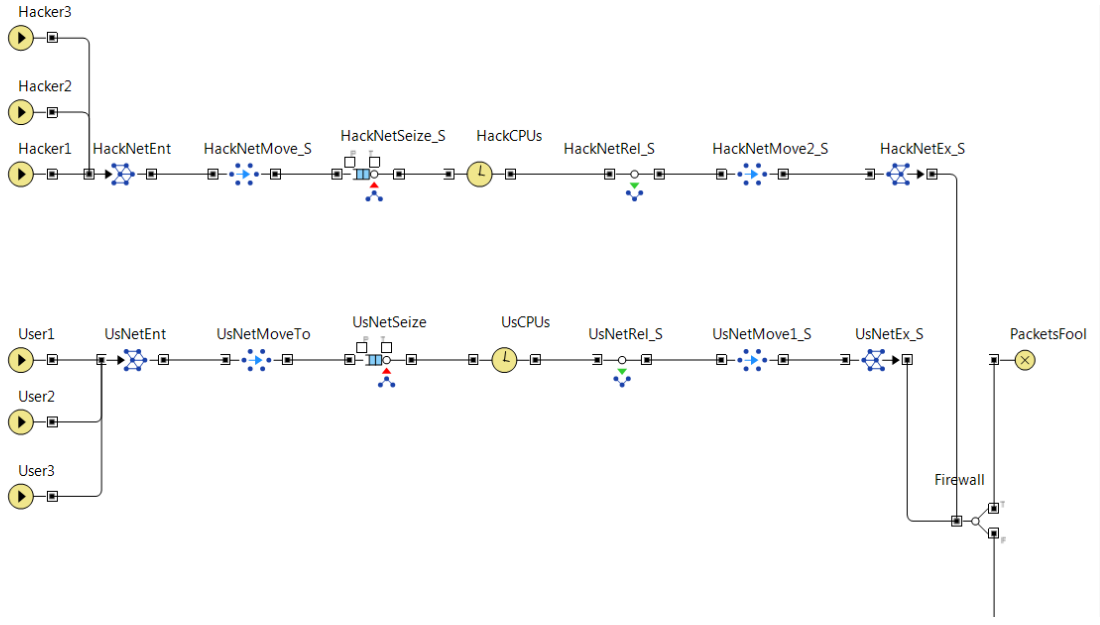

Рисунок 1. Пользовательскаясеть и сеть злоумышленников в AnyLogic

Для генерации запросов используется элемент Source, который генерирует запросы. При помощи данного объекта можно сконфигурировать объект так, чтобы он создавал заявки других типов, указав конструктор нужного класса в параметре Новая заявка, а также задать действие, которое должно выполняться перед тем, как новая заявка покинет объект, и связать с заявкой

определенную фигуру анимации. Есть несколько способов задания того, сколько заявок и когда должен создавать этот объект.

Элемент NetworkEnter. Регистрирует заявку в сети и помещает ее в заданный узел сети. После добавления в сеть заявка может перемещаться по сети и использовать сетевые ресурсы. Заявка не может одновременно находиться сразу в нескольких сетях, поэтому перед добавлением в другую сеть она должна быть вначале удалена из текущей сети с помощью объекта NetworkExit.

NetworkMoveTo. Перемещает заявку в новое место сети. Если к заявке присоединены какие-то ресурсы, то они перемещаются вместе с заявкой. При этом независимо от скорости ресурсов перемещаться такая группа из заявки иее ресурсов будет со скоростью заявки. Время, которое заявка проведет в этом объекте, будет равно длине кратчайшего из возможных путей из текущего местоположения заявки в узел назначения, поделенной на скорость заявки.

NetworkSeize. Объект захватывает для заявки заданное количество сетевых ресурсов. При необходимости может пересылать захваченные ресурсы в заданное место сети и присоединять их к заявке. Объект можно рассматривать как очередь Queue заявок, ожидающих ресурсов, за которой могут следовать объекты NetworkSendTo и NetworkAttach.

Delay. Задерживает заявки на заданный период времени. Время задержки вычисляется динамически, может быть случайным, зависеть от текущей заявки или от каких-то других условий. Одновременно могут быть задержаны сразу несколько заявок. Заявки задерживаются независимо друг от друга – время задержки вычисляется отдельно для каждой заявки. Как только время задержки истекает, заявка тут же покидает объект. Если объект Delay заполнен полностью, то новую заявку он не примет, и в этом случае.

NetworkRelease. Освобождает все или какие-то определенные сетевые ресурсы (ранее захваченные заявкой с помощью объекта NetworkSeize). В случае освобождения каких-то определенных ресурсов, они выбираются из общего числа захваченных ресурсов согласно заданному Списку ресурсов. Если освобождается движущийся ресурс, Вы можете как оставить его в текущем узле сети, так и вернуть его в его базовое местоположение. Сразу после освобождения сеть проверит, не были ли только что освобожденные ресурсы запрошены другими заявками, и если да, то движущийся ресурс будет тут же захвачен другой заявкой и не отправится в свое базовое местоположение, даже если у объекта будет выбрана соответствующая опция.

Selectoutput используется как Firewall. Используется как система безопасности к ресурсам облачных вычислений. Обрабатывает запросы и с определенной вероятностью перехватывает хакерский трафик и блокирует его.

Sink. Используем для сбора статистических данных. Уничтожает поступившие заявки. Обычно используется в качестве конечной точки потока заявок. Для того, чтобы заявки удалялись из модели и уничтожались, нужно соединить выходной порт последнего блока процессной диаграммы с портом объекта Sink.

Оценка временного риска по результатам исследования системы в трех случаях:

- «Эталонная модель», указывающую на нормальное функционирование СОВ с отсутствием всяческих воздействий со стороны злоумышленника;
- «Модель с нарушением ИБ» не удовлетворяющая нормативным уровням защищенности, заданным в ходе моделирования и эксперимента;
- «Модель с нарушением ИБ» удовлетворяющая нормативным уровням защищенности, заданным в ходе моделирования и эксперимента.

Полученные результаты запишем в сводную таблицу соответственно.

Таблица 1. Результаты исследования

Параметр	Характеристика		
$P_{УГР}$ 1	0,03	0,12	0,46
Всего полезных запросов	70	62	46
Перехваченные firewall'ом хакерские запросы	2	18	38
Всего пройдено хакерских запросов		17	24
$P_{риск}$	0,05	0,2	0,77
$P_{без}$	0,95	0,8	0,23

По результатам моделирования можем наблюдать, что в условиях реализации угроз через модель нарушителя можно получить количественные оценки ИБ, в частности риски нарушений, реализуемость угрозы. Благодаря построенной модели можно оценить риск с учетом временных характеристик. Полученные результаты довольно критичны, их необходимо более детально изучить. Полученная количественная оценка рисков ИБ позволило установить категории риска и установить наиболее приемлемые характеристики.

Таким образом, в таблице укажем категории риска, то есть признаки, по которым можно будет в дальнейшем численно характеризовать ИБ СПД. Введем четыре базовых категорий, выраженные через ущерб и угрозы соответственно.

Таблица 2. Категорирование рисков нарушения ИБ СПД

Качественная градация	Количественная градация, $P_{риск}$	Управление	Количественная градация, $P_{без}$
Риск отсутствует	до 0,05	допустимый	от 0,95 до 0,999
Низкий уровень	от 0,0501 до 0,1	допустимый	до 0,9
Средний уровень	от 0,101 до 0,2	не допустимый	от 0,899 до 0,8
Высокий уровень	от 0,2 до 0,779	не допустимый	0,799 до 0,221
Критический Риск	от 0,779 до 0,999	не допустимый	0,221 до 0,001

Далее по после того как будет произведена оценка, необходимо сопоставить уровень риска и контрмеры которые на дынный момент используются владельцем. После чего принимается решение о критичности положения и необходимости тех или иных действий по безопасности.

Список литературы

[1]. Baltayev, J., Boltayev, S. (2023). Model and Methods for Detecting Undetected Errors Us-ing a Signature Analyzer. In: Guda, A. (eds) Networked Control Systems for Connected and Automated Vehicles. NN 2022. Lecture Notes in Networks and Systems, vol 509. Springer, Cham. https://doi.org/10.1007/978-3-031-11058-0_112

[2]. Djuraev R.X., Baltaev J.B., Xasanov O.A. Increasing the efficiency of diagnosing micro-processor devices based on multichannel signal analysis means. Тошкент, ICISCT2020.

[3]. Djuraev R.X., Baltaev J.B., Badalov J.I. Study of the method of compact testing of technical means of data transmission networks Toshkent, ICISCT2020

[4]. Amirsaidov U.B., Abbasxanova X.Yu., Baltaev J.B. Metodi otsenki nadejnosti seti peredachi dannix s uchyotom vozdeystviya vneshnix faktorov VESTNIK TashGTU, 4/2014g., str 27-31

[5]. Djuraev R.X., Djabbarov Sh.Yu., Baltaev J.B. «Sistemi texnicheskogo obslujivaniya i ek-spluatatsii setey telekommunikatsii». Uchebnik.-T.: "Aloqachi".2019, 234 s.

[6]. Djuraev R.X.,Baltaev J.B., Alimov U.B. Methods of Determining Reference Signals for One and Multichannel Signatural Analyzer of Microprocessor Systems, Science Publishing Group, Communications USA № 6(1) 2018. –R. 20-24

[7]. Djuraev R.X., Baltaev J.B. Investigated Methods of Improving the Yefficiency of Diagnos-ing Microprocessor Devices of Data Transmission Systems Based on Multi-Channel Signa-ture Analysis, Science Publishing Group, Communications USA № 7(1) 2019. –R. 13-24 rr.

[8]. Djuraev R.X., Djabbarov Sh.No, it's not., Baltaev J.B. It is a modeling program for diagnos-ing digital devices using an eight-channel signature method. Agency of property of the Re-public of Uzbekistan. Certificate of official registration of the program created for electronic computing machines. № DGU 04123. 16.12.2016 y.

[9]. Djuraev R.X., Djabbarov Sh.Yu., Baltaev J.B. It is a modeling program for diagnosing digi-tal devices using the sixteen-channel signature method. Agency of property of the Republic of Uzbekistan. Certificate of official registration of the program created for electronic compu-ting machines №DGU 04124. 16.12.2016 y.

[10]. Djuraev R.X., Baltaev J.B., Toshtemirov T.Q. Program of detection of errors not detected by the signature analyzer "Agency of real estate of the Ministry of Justice of the Republic of Uzbekistan" DGU 10922.

[11]. Анкудинов И.В. Микропротсессорние системи. Архитектура и проектирование. Учебное пособие. Санкт-Петербург 2003

[12]. Антошина И.В., Котов Ю.Т. Микропротсессори и микропротсессорние системи (аналитический обзор). Москва 2005 г

[13]. Безуглов Д.А., И.В. Калиенко И.В. сифровие устройства и микропротсессори. – Ростов – на – Дону: Феникс, 2006. – 480 с.

[14]. Заиналабедин Наваби, Дигитал Сйстем Тест анд Тестабле Десигн: Усинг ХДЛ Моделс анд Ар-читестурес, Спрингер, 2011.

[15]. Бестугин А. Р., Богданова А. Ф., Стогов Г. В. Контрол и диагностирование телекомму-никатсионних сетей - СПб: Политехника, 2003. 174 с.: ил.

METHODS FOR ASSESSING THE RISK OF INFORMATION SECURITY BREACHES IN CLOUD COMPUTING IN FINANCIAL AND BANKING SYSTEMS

J.B. Baltayev
PhD, Associate Professor "Information Systems and Digital Technologies" of the TFI

S.D. Arzikulov
Senior lecturer of the Department "Information Systems and Digital Technologies" of the, TFI

M.A. Mirjamolova
Assistant of the Department of "Information Systems and Digital Technologies" of the TFI

Department of Information Systems and Digital Technologies
Faculty of taxes and insurance
Tashkent Financial Institute, Republic of Uzbekistan
E-mail: j_baltayev@tfi.uz

Abstract: Information security risk assessment (IS) in the cloud computing environment (SOV) is an important method in ensuring information security in general. Information security risk management is a continuous process of identification, assessment and minimization of risks from the implementation of information security threats. Over the past few years, a new paradigm has been developed in the information technology industry – "cloud computing". Cloud computing is a model for providing ubiquitous and convenient network access (as needed) to a common pool of configurable computing resources (for example, networks, servers, storage systems, applications and services) that can be quickly provided and released with minimal management effort and the need to interact with a service provider (service provider). Further, after the assessment is made, it is necessary to compare the level of risk and the countermeasures that are currently being used by the owner. After that, a decision is made on the criticality of the situation and the need for certain security actions

Keywords: Information security, cloud computing environment, risk management, Reference model, model with violation, AnyLogic, NetworkEnter, NetworkMoveTo, NetworkRelease, Delay, Selectoutput, Sink