www.volsu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В БЕЗОПАСНОСТИ И ТЕЛЕКОММУНИКАЦИЯХ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.3.3

УДК 004.056
ББК 32.927.53

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ОБЛАЧНЫХ СЕРВИСОВ

Наталья Алексеевна Головачева

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
golovacheva.natalya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Максим Сергеевич Романов

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBAS-201_214451@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье представлен анализ механизмов защиты облачных сервисов. Выделены критерии для адекватной оценки этих механизмов. В рамках экспериментальных исследований выявлен наилучший механизм защиты облачных сервисов с учетом требований и потребностей пользователя.

Ключевые слова: информационная система, защита информации, кибербезопасность, облачные вычисления, облачные технологии, облачная система, DDoS-атака, IoT.

В современном информационном обществе каждый человек сталкивается с проблемой безопасного хранения различных паролей, логинов и других данных. Кто-то записывал их в блокноте или просто на бумаге, которая была приклеена к компьютеру, с которого и проходили аутентификацию. Все это давно в прошлом. Любая утечка данных нанесет моральный и материальный вред как простому человеку, так и крупной компании. Сегодня для этого используют облачные вычисления, как основной метод хранения данных на работе или дома. Лидерами в облачных технологиях являются такие интернет-сервисы, как Dropbox, OneDrive, Google Drive, iCloud, Яндекс.Диск, Облако Mail.Ru, МегаДиск, Mega,

BOX, pCloud, Files.fm, WDfiles.ru, wdho.ru, Anonfile.com My-Files.Ru.

Не только провайдеры облачных услуг должны защитить своих клиентов, сетевую инфраструктуру, приложения и платформы, но и сам пользователь должен использовать надежные и индивидуальные пароли и меры аутентификации для обеспечения безопасности своих данных и приложений.

По сути, облачные сервисы представляют собой разновидность кластерных систем. Основное отличие облачных сервисов в том, что основное взаимодействие происходит через сеть Интернет.

Основные функции кластерной системы:

1. Дублирование критически важных компонентов.

2. Автоматический перехват функций.

3. Высокая надежность.

4. Постоянная доступность сервисов и ресурсов (приложений и данных) [2].

При создании кластерных систем используется один из двух подходов.

Первый подход применяется для построения небольших кластерных систем, например, на базе небольших локальных сетей организаций или их подразделений. В таком кластере каждая ВМ продолжает работать как самостоятельная единица, одновременно выполняя функции узла кластерной системы.

Второй подход ориентирован на использование кластерной системы в роли мощного вычислительного ресурса. Узлами кластера служат только системные блоки вычислительных машин, компактно размещаемые в специальных стойках. Управление системой и запуск задач осуществляет полнофункциональный хост-компьютер. Он же поддерживает дисковую подсистему кластера и разнообразное периферийное оборудование. Отсутствие у узлов собственной периферии существенно удешевляет систему [3].

Облачные сервисы предоставляют возможность гибкого управления предоставленной инфраструктурой. Виртуализация позволяет в кратчайшее время осуществить сбор необходимого набора серверов с нужными характеристики производительности. Такие параметры, как RAM, GPU, объем диска и так далее, можно очень быстро настроить. Через панель управления возможно добавить необходимые ресурсы, если настроенная конфигурация не справляется с возложенной на нее нагрузкой. К тому же, автоматизация процесса может быть осуществлена при помощи функции автомасштабирования.

Таким образом, нет необходимости покупать оборудование, которое фактически большую часть времени не будет использоваться. Более рациональной является аренда необходимого оборудования у облачного провайдера. Использование облачных вычислений дает возможность эффективно использовать имеющиеся ресурсы и снижать время, когда оборудование не эксплуатируется [5]. Компании, различающиеся в размерах, типах и отраслях своего функционирования, особое внимание уделяют облачным моделям работы ввиду простоты и эффективности технологии.

Также облачные сервисы дают возможность облегчить организацию информационной системы. Всегда можно получить необходимое число серверов, СУБД или кластеров Kubernetes. Провайдеры облачных услуг выполнят все нужные настройки и обновления. При использовании облачных сервисов мы получаем изменяемую и работоспособную инфраструктуру, которая может быстро включать и выключать виртуальные машины, менять конфигурацию и переносить данные между ними. Наибольшим спросом на рынке пользуются три модели облачных сервисов: IaaS, PaaS и SaaS.

Задача безопасности облачных сервисов состоит в управлении и контроле облаков – посчитаны ли все ресурсы; нет ли чужих виртуальных машин и процессов; все ли элементы четко между собой взаимодействуют [4].

Учитывая основные угрозы безопасности облачных сервисов необходимо выявить следующие критерии их оценки для оценки механизмов их защиты:

1) обеспечение защищенности от утечки данных (К1);

2) перекрытие угрозы обхода аутентификации (К2);

3) перекрытие угрозы взлома API (К3);

4) нейтрализация уязвимости используемых систем (К4);

5) перекрытие угрозы кражи учетных записей (К5);

6) перекрытие угрозы воздействия инсайдеров (К6);

7) перекрытие угрозы целевых кибератак (К7);

8) обеспечение защищенности от потери данных (К8);

9) перекрытие угрозы DDoS-атаки (К9).

В таблице 1 представлены значения, которые может принимать каждый из механизмов.

Таким образом, выявленные критерии позволяют оценить надежность используемого механизма защиты по отношению к основным угрозам, воздействующих на облачные сервисы.

Различные опросы показали, что еще есть проблемы кибербезопасности облачных сервисов. Особое внимание необходимо уделить защите облачных сервисов на основе свободного ПО, также компании должны регулярно проводить аудит подключенных к Сети хранилищ и заботиться о повышении квалификации администраторов, обслуживающих облачные сервисы [1].

Значительная часть угроз связана с влиянием человеческого фактора, однако это влияние возможно минимизировать путем повышения квалификации администраторов баз данных, грамотного выстраивания процессов контроля за информацией (в том числе аудитов безопасности), использования инструментов администрирования сервисов хранения информации, позволяющих правильно организовать массивы данных и настроить корректные параметры доступа, не забывая об установке ограничений, отслеживания появившихся уязвимостей и своевременной установки патчей.

Кроме того, постоянное подключение к интернету требует новых мер безопасности. В рамках экспериментальных исследований анализируются следующие механизмы защиты информации в облачных сервисах: шифрование (М1), конфигурирование (М2), общие принципы безопасности (М3), сегментация (М4).

На сегодняшний день лучшим способом защиты облачных систем является шифрование (М1): шифрование всех сообщений в облаке; шифрование конфиденциальных (учетных) данных; сквозное шифрование данных.

Еще одно средство защиты облака от элементарной уязвимости – конфигурирование (М2). Ошибки конфигурации, такие как настройка по умолчанию, открытый контейнер облачного хранилища и т. д. очень часто приводят к утечки данных из облака.

Нельзя забывать про общие принципы безопасности (М3): надежные и индивидуальные пароли; защита клиентов; резервное копирование; разграничение доступа; антивирус; VPN и др.

Осуществлять контроль над хранением данных организации и выполнение правовых положений о защите информации поможет разделение данных – сегментация (М4).

Для определения, какие механизмы защиты облачных сервисов более эффективны, необходимо сопоставить их с угрозами (таблица 2).

Из таблицы видно, что ни один из механизмов не обладает наилучшим набором значений критериев, поэтому необходимо разработать программу для автоматизации выбора наилучшего механизма защиты облачных сервисов.

Для оценки качества механизмов защиты облачных сервисов была разработана математическая модель, в которой присвоены числовые значения критериям и введена скалярная величина, равная Евклидову расстоянию между наилучшим вектором и вектором критериев, полученным для оцениваемого механизма. Механизм, для которого расстояние до наилучшего

Таблица 1

Критерии оценки

Критерий	Значение		
1	2		
Обеспечение защищенности от утечки данных	Отсутствует (0)	Частично (0,5)	Полное (1)
Перекрытие угрозы обхода аутентификации			
Перекрытие угрозы взлома API			
Нейтрализация уязвимости используемых систем			
Перекрытие угрозы кражи учетных записей			
Перекрытие угрозы воздействия инсайдеров			
Перекрытие угрозы целевых кибератак			
Обеспечение защищенности от потери данных			
Перекрытие угрозы DDoS-атаки			

вектора окажется наименьшим, можно считать наилучшим механизмом защиты облачных сервисов. Разработаны архитектура программы и интерфейс программного для выбора наилучшего механизма защиты облачных сервисов.

Было проведено 4 эксперимента (табл. 3).

Эксперимент 1. Шифрование.

Согласно характеристикам, полученным в результате анализа, механизм обладает следующими частными показателями: К1 = 1; К2 = 0; К3 = 0; К4 = 0,5; К5 = 0; К6 = 0; К7 = 1; К8 = 0; К9 = 0.

В результате оценка шифрования будет иметь значение:

$$P = \sqrt{\sum_{j=1}^{9}(K_j - K_j^i)^2} =$$

$$= \sqrt{(1-1)^2 + 1^2 + 1^2 + (1-0{,}5)^2 + 1^2 + 1^2 +}$$

$$\sqrt{+ (1-1)^2 + 1^2 + 1^2} = 2{,}5.$$

В соответствии с характеристиками, полученными в результате анализа, в форму программы были введены данные, и результат вычислений оценки механизма с помощью формулы совпадает с результатом, полученным в разработанной программе.

Эксперимент 2. Конфигурирование (табл. 4).

Таблица 2

Значения критериев оценки для каждого механизма

Критерий	Механизм			
	М1	М2	М3	М4
Обеспечение защищенности от утечки данных	Полное	Отсутствует	Отсутствует	Частичное
Перекрытие угрозы обхода аутентификации	Отсутствует	Отсутствует	Полное	Частичное
Перекрытие угрозы взлома API	Отсутствует	Отсутствует	Полное	Частичное
Нейтрализация уязвимости используемых систем	Частичное	Полное	Частичное	Отсутствует
Перекрытие угрозы кражи учетных записей	Отсутствует	Отсутствует	Полное	Частичное
Перекрытие угрозы воздействия инсайдеров	Отсутствует	Отсутствует	Полное	Частичное
Перекрытие угрозы целевых кибератак	Полное	Отсутствует	Частичное	Частичное
Обеспечение защищенности от потери данных	Отсутствует	Отсутствует	Полное	Отсутствует
Перекрытие угрозы DDoS-атаки	Отсутствует	Частичное	Отсутствует	Полное

Таблица 3

Характеристики шифрования

Критерий	Значение
1	2
Обеспечение защищенности от утечки данных	Полное
Перекрытие угрозы обхода аутентификации	Отсутствует
Перекрытие угрозы взлома API	Отсутствует
Нейтрализация уязвимости используемых систем	Частичное
Перекрытие угрозы кражи учетных записей	Отсутствует
Перекрытие угрозы воздействия инсайдеров	Отсутствует
Перекрытие угрозы целевых кибератак	Полное
Обеспечение защищенности от потери данных	Отсутствует
Перекрытие угрозы DDoS-атаки	Отсутствует

Таблица 4

Характеристики конфигурирования

Критерий	Значение
1	2
Обеспечение защищенности от утечки данных	Отсутствует
Перекрытие угрозы обхода аутентификации	Отсутствует
Перекрытие угрозы взлома API	Отсутствует
Нейтрализация уязвимости используемых систем	Полное
Перекрытие угрозы кражи учетных записей	Отсутствует
Перекрытие угрозы воздействия инсайдеров	Отсутствует
Перекрытие угрозы целевых кибератак	Отсутствует
Обеспечение защищенности от потери данных	Отсутствует
Перекрытие угрозы DDoS-атаки	Частичное

Согласно характеристикам, полученным в результате анализа, механизм обладает следующими частными показателями: К1 = 0; К2 = 0; К3 = 0; К4 = 1; К5 = 0; К6 = 0; К7 = 0; К8 = 0; К9 = 0,5.

В результате оценка конфигурирования будет иметь значение:

$$P = \sqrt{1^2 + 1^2 + 1^2 + (1-1)^2 + \sqrt{+1^2 + 1^2 + 1^2 + 1^2 + (1-0{,}5)^2}} = 2{,}693.$$

В соответствии с характеристиками, полученными в результате анализа, в форму программы были введены данные, и результат вычислений оценки механизма с помощью формулы совпадает с результатом, полученным в разработанной программе.

Эксперимент 3. Общие принципы безопасности (табл. 5).

Согласно характеристикам, полученным в результате анализа, механизм обладает следующими частными показателями: К1 = 0; К2 = 1; К3 = 1; К4 = 0,5; К5 = 1; К6 = 1; К7 = 0,5; К8 = 1; К9 = 0.

В результате оценка общих принципов безопасности будет иметь значение:

$$P = \sqrt{1^2 + (1-1)^2 + (1-1)^2 + (1-0{,}5)^2 + (1-1)^2 + \sqrt{+(1-1)^2 + (1-0{,}5)^2 + (1-1)^2 + 1^2}} = 1{,}581.$$

В соответствии с характеристиками, полученными в результате анализа, в форму программы были введены данные, и результат вычислений оценки механизма с помощью формулы совпадает с результатом, полученным в разработанной программе.

Эксперимент 4. Сегментация (табл. 6).

Согласно характеристикам, полученным в результате анализа, механизм обладает следующими частными показателями: К1 = 0,5; К2 = 0,5; К3 = 0,5; К4 = 0; К5 = 0,5; К6 = 0,5; К7 = 0,5; К8 = 0; К9 = 1.

В результате оценка сегментации будет иметь значение:

$$P = \sqrt{(1-0{,}5)^2 + (1-0{,}5)^2 + (1-0{,}5)^2 + 1 + (1-0{,}5)^2 + \sqrt{+(1-0{,}5)^2 + (1-0{,}5)^2 + 1 + (1-1)^2}} = 1{,}871.$$

В соответствии с характеристиками, полученными в результате анализа, в форму программы были введены данные, и результат вычислений оценки механизма с помощью

Таблица 5

Характеристики общих принципов безопасности

Критерий	Значение
1	2
Обеспечение защищенности от утечки данных	Отсутствует
Перекрытие угрозы обхода аутентификации	Полное
Перекрытие угрозы взлома API	Полное
Нейтрализация уязвимости используемых систем	Частичное
Перекрытие угрозы кражи учетных записей	Полное
Перекрытие угрозы воздействия инсайдеров	Полное
Перекрытие угрозы целевых кибератак	Частичное
Обеспечение защищенности от потери данных	Полное
Перекрытие угрозы DDoS-атаки	Отсутствует

Таблица 6

Характеристики сегментации

Критерий	Значение
1	2
Обеспечение защищенности от утечки данных	Частичное
Перекрытие угрозы обхода аутентификации	Частичное
Перекрытие угрозы взлома API	Частичное
Нейтрализация уязвимости используемых систем	Отсутствует
Перекрытие угрозы кражи учетных записей	Частичное
Перекрытие угрозы воздействия инсайдеров	Частичное
Перекрытие угрозы целевых кибератак	Частичное
Обеспечение защищенности от потери данных	Отсутствует
Перекрытие угрозы DDoS-атаки	Полное

формулы совпадает с результатом, полученным в разработанной программе.

В результате экспериментов получены следующие обобщенные оценки, изображенные на рисунке, механизмов защиты облачных сервисов:

а) шифрование – 2,5;

б) конфигурирование – 2,693;

в) общие принципы безопасности – 1,581;

г) сегментация – 1,871.

Был проведен анализ результатов экспериментов, в ходе которого выяснилось, что наилучшим механизмом защиты облачных сервисов является механизм использования общих принципов безопасности с результатом 1,581, к которым можно отнести:

1) использование надежных паролей;

2) защита конечных клиентов;

3) резервное копирование;

4) разграничение доступа;

5) использование антивирусной защиты;

6) использование VPN.

СПИСОК ЛИТЕРАТУРЫ

1. Более половины конфиденциальной информации в мире утекает из облачных сервисов // InfoWatch. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/company/presscenter/news/26622. – Загл. с экрана.

2. Кластерные системы // Platformix. – Электрон. текстовые дан. – Режим доступа: https://platformix.ru/node/68. – Загл. с экрана.

3. Орлов, С. А. Организация ЭВМ и систем : учебник / С. А. Орлов, Б. Я. Цилькер. – СПб. : Питер, 2021. – 688 с.

4. Что такое безопасность облака? // Лаборатория Касперского. – Электрон. текстовые дан. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security. – Загл. с экрана.

5. Что такое облачные вычисления. Обзор // Yandex Cloud. – Электрон. текстовые дан. – Режим доступа: https://cloud.yandex.ru/blog/posts/2022/04/cloud-computing. – Загл. с экрана.

REFERENCES

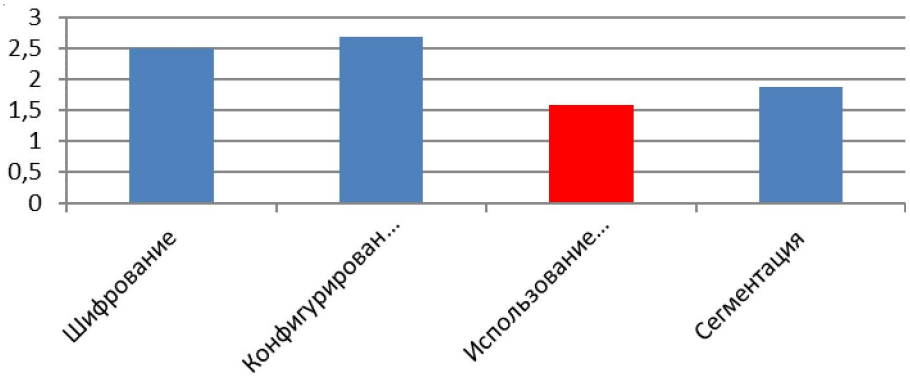
1. Bolee poloviny konfidencial'noj informacii v mire utekaet iz oblachnyh servisov [More Than Half of Confidential Information in the World Leaks from Cloud Services]. *InfoWatch* [InfoWatch]. URL: https://www.infowatch.ru/company/presscenter/news/26622

2. Klasternye sistemy [Cluster Systems]. *Platformix*. URL: https://platformix.ru/node/68

3. Orlov S.A., Zilker B.Ya. *Organizacija EVM i sistem: uchebnik* [Organization of Computers and Systems. Textbook]. Saint Petersburg, Piter Publ., 2021. 688 p.

4. Chto takoe bezopasnost oblaka? [What Is Cloud Security?]. *Laboratorija Kasperskogo* [Kaspersky Lab]. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security

5. Chto takoe oblachnye vychislenija. Obzor [What Is Cloud Computing. Overview]. *Yandex Cloud*. URL: https://cloud.yandex.ru/blog/posts/2022/04/cloud-computing



Гистограмма обобщенных оценок

STUDY OF SECURITY MECHANISMS CLOUD SERVICES

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
golovacheva.natalya@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Maxim S. Romanov

Student, Department of Information Security,
Volgograd State University
IBAS-201_214451@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article analyzes the protection mechanisms of cloud services. Criteria for adequate evaluation of these mechanisms are identified. In the framework of experimental research, the best mechanism of cloud service protection is identified, taking into account the requirements and needs of the user. In the modern information society, everyone is faced with the problem of securely storing various passwords, logins and other data. Someone wrote them down in a notebook or just on a piece of paper that was glued to the computer from which they authenticated. All this is long in the past. Any data leak will cause moral and material harm to both an ordinary person and a large company. Today, cloud computing is used for this as the main method of storing data at work or at home. The leaders in cloud technologies are the following Internet services: Dropbox, OneDrive, Google Drive, iCloud, Yandex.Disk, Cloud Mail.Ru, MegaDisk, Mega, BOX, pCloud, Files.fm, WDfiles.ru, wdho.ru, Anonfile.com, My-Files.Ru. Not only must cloud service providers protect their customers, network infrastructure, applications and platforms, but the user himself must ensure the security of his data and applications using strong passwords and authentication measures.

Key words: information system, information security, cybersecurity, cloud computing, cloud technology, cloud system, DDoS attack, IoT.