УДК 004.5 **DOI: 10.18413/2518-1092-2021-6-1-0-6**

Нестеренко В.Р.
Маслова М.А.

СОВРЕМЕННЫЕ ВЫЗОВЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУБЛИЧНЫХ ОБЛАЧНЫХ РЕШЕНИЙ И СПОСОБЫ РАБОТЫ С НИМИ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: vladimir.nesterenko.workmail@gmail.com, mashechka-81@mail.ru

Аннотация
Некоторые организации используют облачные сервисы для хранения служебной информации, иные организации выстраивают свои бизнес-процессы с использованием облачных решений. По данным Check Point Software Technologies Ltd. (NASDAQ: CHKP), поставщика решений в области кибербезопасности по всему миру, за 2020 год, 39% респондентов отметили важность защиты облачной инфраструктуры компаний, и 52% выделили защиту публичных и гибридных облаков. Разработка методов и средств противодействия угрозам безопасности облачных сервисов – одна из приоритетных задач индустрии. В условиях карантина особенно остро стоят вопросы безопасности облачных сервисов, так как все больше и больше пользователей и организаций хранят важную информацию в облаке, ведут рабочий процесс в облаке, переносят или ассоциируют свои бизнес-процессы с облачными технологиями. Большая часть проблем информационной безопасности облачных сервисов могут быть решены с внедрением криптографической защиты, грамотных административных мер со стороны поставщика и провайдера услуг. Данные меры должны учитывать индивидуальные требования клиента.
Ключевые слова: облачные сервисы, безопасность облачных сервисов, облако, информационная безопасность.
Для цитирования: Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. – Т.6, №1, 2021. – С. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6

Nesterenko R.V.
Maslova M.A

MODERN CHALLENGES AND THREATS INFORMATION SECURITY PUBLIC CLOUD MAKING AND METHODS OF WORK WITH THEM

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: vladimir.nesterenko.workmail@gmail.com, mashechka-81@mail.ru

Abstract
Some organizations use cloud services to store service information, while other organizations build their business processes using cloud solutions. According to Check Point Software Technologies Ltd. (NASDAQ: CHKP), a global cybersecurity solutions provider, for 2020, 39% of respondents noted the importance of protecting their cloud infrastructure, and 52% emphasized protecting public and hybrid clouds. The development of methods and means to counter threats to the security of cloud services is one of the priority tasks of the industry. In a quarantine environment, the security issues of cloud services are especially acute, as more and more users and organizations store important information in the cloud, conduct workflow in the cloud, and migrate or associate their business processes with cloud technologies. Most of the problems of information security of cloud services can be solved with the introduction of cryptographic protection, competent administrative measures on the part of the provider and service provider. These measures should take into account the individual requirements of the client.
Keywords: cloud services, cloud services security, cloud, information security.
For citation: Nesterenko R.V., Maslova M.A. Modern challenges and threats information security public cloud making and methods of work with them // Research result. Information technologies. – T.6, №1, 2021. – P. 48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6

ВВЕДЕНИЕ

За последние несколько лет облачные технологии и сервисы начали широко применяться в работе многих компаний. Некоторые организации используют облачные сервисы для хранения служебной информации, иные организации выстраивают свои бизнес-процессы с использованием облачных решений, как незаменимых систем по информационному обеспечению бизнеса. Кроме выгоды, которую получит организация при внедрении облака, также присутствуют и угрозы.

По данным Check Point Software Technologies Ltd. (NASDAQ: CHKP), поставщика решений в области кибербезопасности по всему миру, за 2020 год, 39% респондентов отметили важность защиты облачной инфраструктуры компаний, и 52% выделили защиту публичных и гибридных облаков одной из приоритетных задач информационной безопасности на следующие два года, наряду с обеспечением безопасности удаленной работы и понижением процента утечек информации с мобильных устройств [1].

ОСНОВНАЯ ЧАСТЬ

Виды облачных сервисов. Прежде чем рассматривать конкретные угрозы для облачных сервисов, необходимо рассмотреть виды и архитектуры облачных сервисов, а также их интеграцию в бизнес-процессы компаний.

По статистике, более 66% компаний используют облачные технологии, находящиеся на продвинутой -33% или промежуточной – 33% стадии их внедрения, остальные же еще остались на: отстающей – 7%, наблюдающей-13%, начинающей – 14% стадиях (см. рис.1) [8].

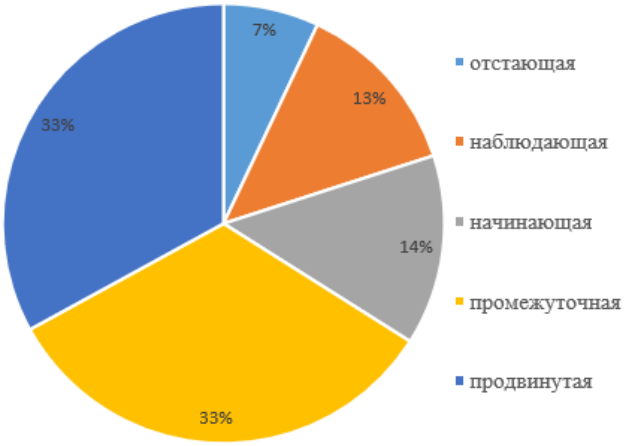

Рис. 1. Стадии внедрения облачных технологий
Fig. 1. Stages of implementation of cloud technologies

Облачный сервис, облачное решение – веб-приложение, реализующее повсеместный доступ сотрудников к ресурсам посредством сети. В [2] дается четкое разделение облачных сервисов по виду предоставляемых услуг и по типу развертывания сервиса на разных инфраструктурах.

По типу предоставляемых услуг облачные сервисы можно разделить на следующие типы:

– приложение, как сервис,
– платформа, как сервис,
– инфраструктура, как сервис.

Приложение как сервис (SaaS) – конечному пользователю предоставляется доступ к приложению, размещенному на серверах провайдера услуги. Возможность конфигурировать инфраструктуру, операционную систему и возможности облачной платформы, провайдер оставляет за собой. Пользователю предоставляется “тонкий” веб-интерфейс, который возможно использовать практически на всех платформах, имеющих браузер за редким исключением. Примером может служить система взаимодействия с клиентами, Битрикс24, а также развернутая на публичных серверах Atlassian инфраструктура для разработчиков (jira + confluence + bitbucket)

Платформа, как сервис (PaaS) – конечному пользователю предоставляется возможность размещать на платформе свои приложения, конфигурировать их, обеспечивать поддержку необходимых языков программирования и библиотек в пределах, устанавливаемых провайдером услуги. Примером может служить хостинг для веб приложений или хостинг для распределенных приложений.

Инфраструктура, как сервис (IaaS) – поставщик не контролирует конечного потребителя. Потребителю предоставляются контроль над вычислительными мощностями, конфигурацией облачной платформы, конфигурацией и установкой операционной системы, а также необходимых приложений.

По доступности облачные сервисы подразделяют на:

– частное облако,
– общественное облако,
– публичное облако,
– гибридное облако.

Частное облако принадлежит одной компании. За все аспекты безопасности облака отвечает данная компания: инфраструктуру облака, доступность и инциденты информационной безопасности несет ответственность только организация. Отсутствует необходимость в доверии к какому-либо провайдеру облачных услуг, доступ к облаку обычно предоставляется только сотрудникам компании, обычно через virtual private network.

Общественное облако (community cloud) – облачная инфраструктура предназначена для использования специфическим сообществом из организаций, которые имеют общие проблемы и задачи. Облачная инфраструктура может принадлежать одной или более организации из данного сообщества. Обеспечение безопасности, доступности и ответственность за сохранность данных несут владельцы облачной инфраструктуры. Между организациями, которые поддерживают облако должно быть доверие.

Публичное облако – облачная инфраструктура, доступная для открытого использования, за безопасность и доступность отвечает провайдер услуг.

Гибридное облако – облачная инфраструктура, являющаяся композицией из описанных выше типов облачных сервисов. Компоненты такого объединения облачных сервисов являются самостоятельными платформами. Для обеспечения доставки запросов к нужному компоненту облака обычно используют стандартизированные или частные технологии, например, балансировщик запросов [3].

На рис. 2 представлена статистика российского рынка облачных технологий и существующим требованиям закона – «Закон о персональных данных» их использования [8].

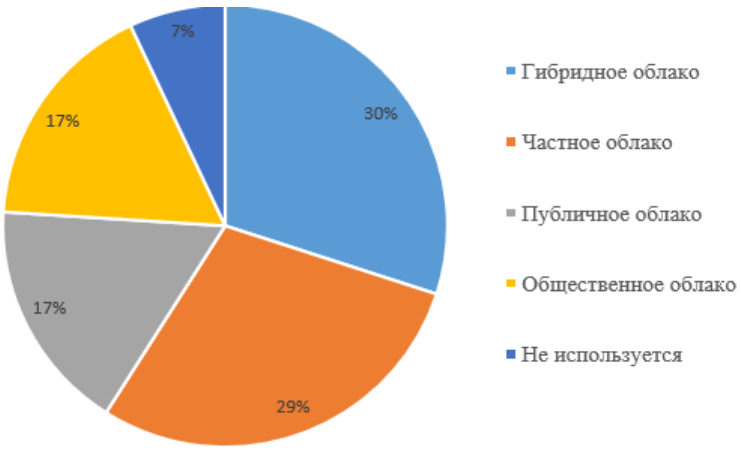

Рис. 2. Доступность облачных сервисов
Fig. 2. Availability of cloud services

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Угрозы безопасности публичных платформ и сервисов. В своем докладе [3] директор компании Huawei по развитию облачных технологий в России, Артур Пярн, выделил следующие основные угрозы:

– утечки данных,
– недостаточное управление доступом, учетными записями пользователей и авторизацией,
– небезопасное использование портов и API,
– эксплоиты и уязвимости используемого ПО,
– взлом аккаунтов,
– инсайдеры злоумышленники,
– APT-угрозы,
– невосполнимая потеря данных,
– недостаточное due diligence провайдера,
– использование облачных сервисов в преступных целях,
– DoS и DDoS проблемы,
– Риски использования совместных ресурсов.

Данные угрозы характерны как для приватных, так и для публичных облачных сервисов.

Причиной утечки данных может стать множество факторов, наиболее опасные из которых – деятельность инсайдеров и неправильная конфигурация облачного сервиса или приложений, расположенных на нем. Также неверная конфигурация веб-интерфейса и ошибки в коде, могут открыть злоумышленнику множество способов получения информации, которая хранится в публичном облаке.

Современные облачные решения реализованы как набор легковесных микросервисов, которые принимают запросы по протоколу http. Архитектура таких микросервисов основана на REST API, что привносит в список угроз все характерные грозы для данного типа архитектуры, например, не криптостойкие генераторы токенов для пользователей, уязвимость “человек в середине” и передача по открытым каналам данных. Для купирования данной угрозы необходимо разрабатывать микросервисы с учетом безопасности при обмене данными. Передавать запросы к REST API микросервиса необходимо только используя зашифрованный канал передачи (SSL/TLS последней стабильной версии).

Множество пользователей постоянно совершают в облаке некоторые действия, среди которых могут быть и действия злоумышленника. Решением данной проблемы должно стать полное описание свойств приложения, которое размещено в облаке, а также логирование всех запросов.

Риски использования совместных ресурсов заключаются в модификации или уничтожении злоумышленником важных ресурсов. Потери от данной угрозы будут особенно велики, так как информация могла принести коммерческую выгоду не одной, а нескольким организациям. Или являлась результатом работы нескольких организаций, что неминуемо повлечет за собой репутационные потери.

APT-угроза – угроза постепенного внедрения, сбора информации и атак по нескольким векторам злоумышленника в облачном сервисе компании почти не отличается от обычных APT-атак. Для предотвращения таких атак необходимо реализовать комплекс мер и средств по обеспечению безопасности: административные, технические, программные. Однако, как следует из доклада ведущих специалистов по организации безопасности [5], не бывает идеальной защиты, а все предпринятые меры по защите облачных сервисов не могут считаться достаточно надежными, если в процесс взлома включен злоумышленник, имеющий средства, знания, а главное – время для исследования структуры сервиса и поиска его слабых мест. Существуют решения для предотвращения таких атак, но и они не могут считаться достаточно надежными

ввиду того, что все чаще и чаще исследователи уязвимостей находят ту или иную уязвимость в протоколе или в самом веб-приложении. Невозможно учесть все слабые стороны сложной архитектуры облачного сервиса.

В случае с данным видом угроз, основным способом обезопасить себя будет своевременное реагирование на действия злоумышленника, а также принятие концепции “никто не доверяет никому без необходимости, и ничего не разрешено по умолчанию” при проектировании облачных решений.

Максимальная защита от данной угрозы может быть достигнута при организации следующих мер и в системном применении следующих средств [6]: организация мониторинга дисков, логов, памяти, кода; применение средств обнаружения аномалий в системе, например средств, основанных на нейронных сетях и подходах, предполагающих машинное обучение [7].

Недостаточное due diligence провайдера – недостаточно детальный анализ провайдера, его вычислительных мощностей и услуг. Данная угроза может стать причиной отказа в обслуживании пользователей и потери информации.

В среднем защита данных в облаке распределяется следующим образом: 48% - подключение к облаку через защищенные каналы связи; 39% с помощью служб безопасности, предлагаемые облачным провайдером; 41% шифрование и токенизация (рис. 3) [8].

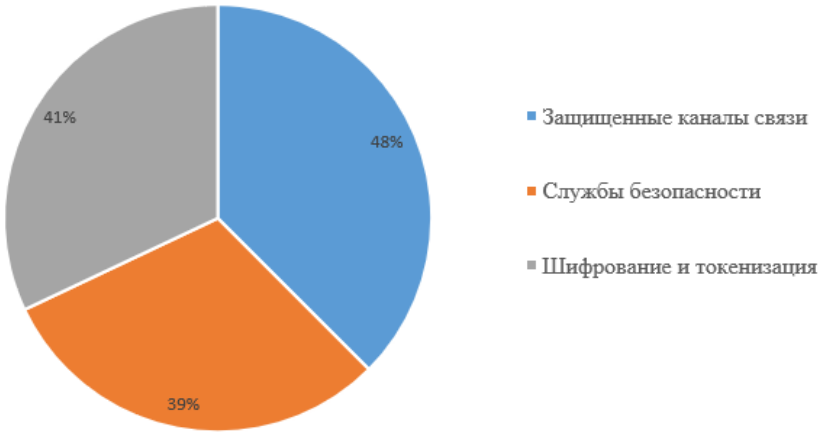

Рис. 3. Защита данных в облаке
Fig. 3. Data protection in the cloud

Большинство проблем защиты информации пользователя в облаке может быть решено на основе использования существующих методов криптографической защиты информации, административных мер со стороны как поставщика облачных услуг, так и пользователя, заключение договоров на предоставление услуг, учитывающих индивидуальные потребности клиентов, принятие международных стандартов в отрасли, введение контроля со стороны государства и создания независимых экспертов в этой отрасли [3].

Для обеспечения целостности и конфиденциальности хранимой в облаке информации необходимо использовать современные алгоритмы шифрования из международных стандартов, а также алгоритмы цифровой подписи. Проблема с получением доступа к аккаунтам пользователей может быть решена с введением двухфакторной аутентификации. Для обеспечения приемлемого уровня безопасности аутентификации можно использовать google authenticator как на стороне сервисов и веб приложений провайдера, так и на стороне пользователя. Данное решение будет являться оптимальным, так как поддерживается и обновляется большой компанией, а также предоставляет пользователям удобный интерфейс и возможность использовать мобильное приложение для генерации кода, как второго фактора аутентификации.

В настоящее время большинство поставщиков имеют свой собственный, иногда даже хорошо документированный интерфейс для программирования, но это приводит к невозможности перехода пользователей от одного поставщика услуг к другому. Практика в таких вопросах

показывает, что лишь разработка открытого единственного международного стандарта может решить этот вопрос.

ЗАКЛЮЧЕНИЕ

Разработка методов и средств противодействия угрозам безопасности облачных сервисов – одна из приоритетных задач индустрии. В условиях карантина особенно остро стоят вопросы безопасности облачных сервисов, так как все больше и больше пользователей и организаций хранят важную информацию в облаке, ведут рабочий процесс в облаке, переносят или ассоциируют свои бизнес-процессы с облачными технологиями.

Большая часть проблем информационной безопасности облачных сервисов могут быть решены с внедрением криптографической защиты, грамотных административных мер со стороны поставщика и провайдера услуг. Данные меры должны учитывать индивидуальные требования клиента. Также важно вводить международные стандарты безопасности облачных сервисов, контролировать то, как данные стандарты выполняются клиентами и провайдерами услуг.

Из программных средств и методов можно выделить полное описание и учет всех функций, создание защищенного REST API для своих микросервисов, размещенных в облаке.

Угроза инсайдерской утечки информации – наиболее серьезная угроза может быть если не предотвращена, то разрешена впоследствии, если облачные сервисы клиента или сам провайдер предоставляет логирование всех действий пользователя в системе.

Список литературы

1. Информационная безопасность в компаниях, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8
2. NIST SP 800-145, The NIST Definition of Cloud Computing. NIST Special publications
3. Довгаль Виталий Анатольевич Облачные вычисления и анализ вопросов информационной безопасности в облаке // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2015. №2 (161). URL: https://cyberleninka.ru/article/n/oblachnye-vychisleniya-i-analiz-voprosov- informatsionnoy-bezopasnosti-v-oblake (дата обращения: 23.01.2021).
4. https://ict.moscow/static/pdf/files/10_%D0%9F%D1%8F%D1%80%D0%BD.pdf
5. https://lib.itsec.ru/articles2/cloud-security/oblachnye-vychisleniya-v-rossii-vozmozhnosti--vyzovy-i-riski
6. Alshamrani, Adel & Myneni, Sowmya & Chowdhary, Ankur & Huang, Dijiang. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2019.2891891.
7. Большев А.К., Яновский В.В. Применение нейронных сетей для обнаружения вторжений в компьютерные сети // Вестник СПбГУ. Серия 10. Прикладная математика. Информатика. Процессы управления. 2010. №1. URL: https://cyberleninka.ru/article/n/primenenie-neyronnyh-setey-dlya-obnaruzheniya-vtorzheniy-v-kompyuternye-seti (дата обращения: 06.02.2021).
8. Исследование PwC «Страх облаков» Аналитическое исследование, октябрь 2020 pwc-cloud-fear-survey.pdf

References

1. Information security in companies, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8
2. NIST SP 800-145, The NIST Definition of Cloud Computing. NIST Special publications

3. Dovgal Vitaly Anatolyevich Cloud computing and analysis of information security issues in the cloud / / Bulletin of the Adygeya State University. Series

4. https://ict.moscow/static/pdf/files/10_%D0%9F%D1%8F%D1%80%D0%BD.pdf

5. https://lib.itsec.ru/articles2/cloud-security/oblachnye-vychisleniya-v-rossii-vozmozhnosti--vyzovy-i-riski

6.Alshamrani, Adel & Myneni, Sowmya & Chowdhary, Ankur & Huang, Dijiang. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2019.2891891.

7. Bolshev Alexander Konstantinovich, Yanovsky Vladislav Vasilyevich Application of neural networks for detecting intrusions into computer networks // Bulletin of St. Petersburg State University. Series 10. Applied mathematics. Computer science. Management processes. 2010. No. 1. URL: https://cyberleninka.ru/article/n/primenenie-neyronnyh-setey-dlya-obnaruzheniya-vtorzheniy-v-kompyuternye-seti (accessed: 06.02.2021).

8. PwC "Fear of the Clouds" Analytical study, October 2020 pwc-cloud-fear-survey. pdf

Нестеренко Владимир Романович, студент второго курса магистратуры кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Nesterenko Vladimir Romanovich, second-year master's student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security