АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
AUTOMATION AND CONTROL

УДК 004.056 **DOI: 10.18413/2518-1092-2022-7-4-0-4**

Маслова М.А.[1,2]

РИСКИ IT-ИНФРАСТРУКТУРЫ И МЕТОДЫ ИХ РЕШЕНИЯ

[1)] Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия
[2)] Ростовский государственный экономический университет (РИНХ), ул. Большая Садовая, д. 69, г. Ростов-на-Дону, 344002, Россия

e-mail: mashechka-81@mail.ru

Аннотация
Изменения мировых трендов в IT–инфраструктуре в бизнесе не стоит на месте и одним из развивающихся направлений есть периферийные и облачные вычисления. Так последние годы на российские рынки из-за санкций многие компании были интегрированы или полностью ушли с рынка, то появилась острая необходимость изменения, доработки и создание новых ИБ-сервисов, которые требуют грамотную, постоянную защиту всей обрабатывающейся информации. Необходимо грамотные финансовые вложения в защиту данного направления. В данной работе будут рассмотрены плюсы и минусы использования облачных сервисов, а также возможные риски, решения и направления развития облачных ИБ-сервисов.
Ключевые слова: риски; ИБ-сервисы; кибератаки; информационная безопасность; облако; IT-инфраструктура; кражи
Для цитирования: Маслова М.А. Риски IT-инфраструктуры и методы их решения // Научный результат. Информационные технологии. – Т.7, №4, 2022. С. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4

Maslova M.A.[1,2]

IT INFRASTRUCTURE RISKS AND METHODS FOR THEIR SOLUTION

[1)] Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia
[2)] Rostov State Economic University (RINH), 69 Bolshaya Sadovaya St., Rostov-on-Don, 344002, Russia

e-mail: mashechka-81@mail.ru

Abstract
Changes in global trends in IT infrastructure in business do not stand still, and one of the developing areas is peripheral and cloud computing. So in recent years, many companies have been integrated into the Russian markets due to sanctions or completely left the market, then there is an urgent need to change, refine and create new information security services that require competent, constant protection of all processed information. It is necessary to make sound financial investments in the protection of this direction. This paper discusses the pros and cons of using cloud services, as well as possible risks, solutions and directions for the development of cloud information security services.
Keywords: risks; information security services; cyber attacks; information security; cloud; IT infrastructure; theft
For citation: Maslova M.A. IT infrastructure risks and methods for their solution // Research result. Information technologies. – T.7, №4, 2022. – P. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4

ВВЕДЕНИЕ

В процессе работы любого предприятия, неотъемлемой его частью работы есть защита от рисков при обмене информацией. Организации имеют корпоративную тайну, государственную тайну и при этом используют в своей работе сети передачи данных, хранение информации на

облачных сервисах, которое используется все в большей мере [1-3]. Информация передается не только корпоративная, финансовая, а и обрабатывается личная информация, которая чаще всего поддается кибератакам, кражам, перепродажам и ее «сливам». Поэтому будь то частная или государственная структура – необходимо заботиться о конфиденциальности и качественной защите при расположении ее на сервисах, что является одной из проблем в данное время. Многие сервисы стремятся только заработать, а вот качественные услуги очень «хромают».

ОСНОВНАЯ ЧАСТЬ (MAIN PART)

Интернет вещи – это одно из продвинутых направлений сегодня, используемое все большим количеством людей на планете, так как это удобно, прогрессивно и самое главное дает дополнительную возможность обезопасить и защитить себя, свой дом, данные от различных угроз и атак, как в повседневной жизни, больших компаниях и разного рода бизнеса.

Всю обрабатываемую и сохраняемую информацию необходимо постоянно контролировать и защищать, так как киберугрозы, появляющиеся атаки, постоянный рост различных рисков не убывает, а наоборот только возрастает [4].

Использование облачного хранения данных услуга очень удобна и мобильна – в любой момент, с любой точки мира пользователь может получить свои данные, зная логин и пароль зайдя с любого устройства, даже если у вас с собой нет своего компьютера; ваши данные не потеряются, если вдруг устройство испортиться или потеряется; постоянное обновление данных выполняется прям в «облаке», а также возможность распределить и разделить информацию, которой можно делиться с друзьями или коллегами для работы в онлайн-режиме; бесплатное хранение данных до определенного размера, в зависимости от сервиса или за небольшую плату предоставление большего размера, что очень удобно.

Применение облачных сервисов, хранение и обмен информацией на облаке стало одним из обычных способов, т.к. это очень удобно и мобильно, но обратная сторона медали то, что это все равно - опасно. Все чаще в средствах массовой информации мы видим новости и данные статистики по утечки конфиденциальной информации пользователей, их логинов и паролей, и различной корпоративной информации разных организаций, даже их финансовых данных и отчетов. Это все приводит к новым уязвимостям и рискам как по отношению к пользователям, так и падению репутации и финансовой составляющей организаций. При этом что пользователи, что организации продолжают хранить данные на «облаке». И по статистике 85% компаний планирует и дальше использовать облачные технологии [5].

Во время опроса 81 % опрошенных компаний заявили, что считают облачные технологии надежным, защищенными сервисом для хранения своих данных и является одним из доступных решений, мотивируя это тем, что оно защищено хорошо на всех уровнях: дата – центр, защита персональных данных, а также защита от DDoS-атак [12].

Если рассмотреть плюсы использования облачных сервисов, и хранения данных в облаке, то они включают в себя:

– Минимальные затраты на технику – благодаря использованию облака отпадает необходимость вкладывать большие деньги в составляющие компьютера, память, т.к. все вычисления и хранения данных можно делать на облаке;

– Увеличение производительности ПК – программы требуют больших затрат ресурсов ПК, с помощью облака запуск будет производиться удаленно – это снизит нагрузку на ПК в несколько раз;

– Обслуживание ПК и минимизация затрат на покупку ПО – меньше затрат на установку, обновление необходимых программ, все настроено на облаке, нет необходимости в приобретении новых программ;

– Увеличение эффективности IT-инфраструктуры с уменьшение затрат – в организациях обычно есть свои сервера, и они либо не используются даже на треть своей мощности или наоборот ее не хватает. Поэтому при использовании облачных вычислений данная проблема

становится не актуальной. Если организация хочет иметь свое облачное хранилище для более защищенной работы, то она может его приобрести.

– Обновление программ – отпадает необходимость иметь в штате специального сотрудника, который будет следить за обновления программ, с использованием облака - любой сотрудник может запустить любую программу удаленно и быть спокоен о безопасности и обновлении т.к. все настроено и проверено;

– Увеличение мощностей – нет необходимости покупать мощные компьютеры и постоянно их усовершенствовать;

– Неограниченное количество памяти – ПК всегда имеет ограничения памяти, а тем более ноутбук и приходится покупать дополнительные жесткие диски и т.д. На облаке неограниченное количество памяти, которое можно изменять в зависимости от нужд пользователя или организации;

– Совместимость с ОС – при работе с облаком пользователь неограничен и может пользоваться, и обмениваться информацией независимо от того Windows, Unix или это Mac, т.к. доступ к программам происходит через Web – браузер, которые идентично устанавливаются на любую ОС;

– Совместимость форматов документов – просто необходим ПК с Web – браузером;

– Доступ к документам 24/7 – для организации большой плюс, т.к. к любым документам доступ круглосуточно;

– Упрощение совместной работы – постоянное обновление документов, которые видят сразу все рабочие организации;

– Полная доступность – неважно каким гаджетом вы пользуетесь и где вы находитесь в данный момент – подключение с любого устройства в любое время с наличием интернета;

– Защита потери данных или их кражи – при отправке данных на облако, происходит их автоматическое сохранение и создание копий на запасных серверах.

Но как бы ни было все «облачно и прекрасно», всегда есть минусы:

– Доступ к документам 24/7 –для рабочих не всегда является плюсом, т.к. работа также становится круглосуточной если есть интернет;

– Интернет – самая важное условие пользование облаком - наличие постоянной интернет-связи, в противном случае доступ будет только к документам, которые были загружены на локальный компьютер. При этом интернет должен быть качественным и быстрым;

– Медленная работа облачных программ – при передаче больших объемов данных процесс может быть медленным, так же на это может влиять плохой интернет;

– Техника – любая техника – это уже риск, поломка, выход из стоя каких-либо элементов; сбой в системе; отключение света или интернета – все ведет к простою работы и финансовым затратам;

– Программы – к сожалению еще не все программы могут работать удаленным способом;

– Безопасность – все знают, что нет исключительной 100 % безопасности. Поэтому при выборе облака необходимо обращать внимание, на метод защиты, шифрование, которое оно использует и на возможность постоянных резервных копий;

– Потеря данных в облаке – это очень сложно, но всегда возможно.

Плюсов в использовании облачных сервисов намного больше, чем минусов, поэтому все больше пользователей и организаций выбирают их использование. Но как дополнительная безопасность данных – резервное копирование, должно быть обязательным, если данные важные и дорогие. Работу резервного копирования необходимо настроить постоянную, с определенным периодом сохранения и хранения, а также удаления, т.к. это огромное количество информации, которое обязательно надо фильтровать, т.к. это большая нагрузка на сеть.

Очень часто организации стали использовать для хранения информации гибридное облако – в 80% случаях. Компании и организации готовы инвестировать в защищенные облака из-за роста новых угроз, которые направлены на критические системы. По опросам экспертов Stack Group за

последний год общий сегмент облачных ИБ-сервисов по защите данных возрастет до 40 процентов [12].

Если же рассматривать, например, глобальную критическую информационную инфраструктуру (КИИ), то нарушение их работоспособности из-за кибератак или рисковых ситуаций могут принести не только колоссальные ущербы, но и угрозу жизни людей.

Необходимо помнить о возможных рисках, некоторые из них уже были рассмотрены выше в минусах использования облачных сервисов – отключение электроэнергии, поломка ПК или др. устройства для работы; наличие постоянного интернета и онлайн-доступа ко всем сервисам и программам; а также другие возможные риски – человеческий фактор, разглашение умышленное или неумышленное информации; DDoS-атаки, фишинг – атаки, НСД; проникновение злоумышленников в незащищенные сети; отсутствие периметра облака; разрыв договоров на обслуживание; санкции и т.д. [6-10].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Все имеющиеся средства защиты дорабатываться и усовершенствуются по мере появления новых рисков и атак. Например, тартегированные атаки, для них необходимы более новые разработки и защиты в ИБ. Применение аналитических систем, которые будут включать в себя базы знаний по различным существующим индикаторам и техникам, которые применяются в данный момент и внедряются новыми нарушителями, так же обязательно обращая внимание на то, что будет защищаться. Компании, предприятия должны одним из первых шагов определить и проранжировать главные ИБ-риски, методики их определения, управления и защиты от них.

При разработке новых сервисов, защиты и т.д. необходимо помнить о стороне закона, о нормативных актах РФ для той страны, для которой будет разрабатываться и применяться сервис или защита, различных применяемых методик моделирования угроз, безопасности и защите персональных данных. За последние годы в РФ произошло значительное усиление государственных требований в направлении защиты ПД, кибербезопасности, КИИ. Поэтому одним из правил есть то, что бизнес должен обязательно соблюдать нормы регуляторов рынка при применении любых решений для защищенного облака на уровне серверов и виртуализации и тогда это приведет к его устойчивости и непрерывности бизнес-процессов.

Развитие интернета вещей так же дает направление и необходимость принятия новых правовых, нормативных актов регулирования в данной области. Так как различие на рынке типов устройств для интернета вещей так же требуют определенное соответствие нормативным актам от видов используемого устройства, что пока мало реализуемо и поэтому немного затормаживает данный процесс. Для решения данной проблемы необходимо чтоб устройства имели градации и требования защиты в зависимости от использования, имели хорошую систему надежной защиты коммуникаций и защищенные каналы связи от утечек личных данных. Лучшее решение – это комплексный подход, включающий в себя различные решения защиты: межсетевые экраны; брокеры безопасного доступа в облако; DLP системы, которые будут размещены или в инфраструктуре провайдера или локально [2].

Любое соединение должно быть защищено, т.к. существует множество известных рисков, а также и те, о которых пользователь или сотрудник может даже не догадываться и это является одной из главных проблем обеспечения ИБ. Поэтому необходимо в первую очередь читать соглашения или политику использования, дабы не дать добровольное согласие на хранение и использование ваших личных или хранимых данных на облаке, так как условия у всех разные: одни прописывают, что после удаления учетную записи они удаляют ваши данные сразу - по статистике таких поставщиков всего 13,3%, остальные же хранят их еще год, а некоторые провайдеры - бессрочно.

Но если для определенного устройства, для интернета вещей или личного пользования защиту можно быстро адаптировать, заменить, усовершенствовать, то, например, для государственных сервисов или КИИ полную модификацию или установку лучшей защиты выполнить доставляет достаточно много трудностей, так как это невозможно вывести из строя на

долго или полностью остановить рабочий процесс. Поэтому при разработки таких средств защиты для крупных структур или КИИ необходимо закладывать на будущее улучшенные средства защиты и продумывать их быструю замену или модификацию. Так, как только наличие самого подключения к интернету уже является главным риском для любого предприятия. Уязвимости появляются все новые и риски становятся всеобъемлимыми, поэтому очень важно постоянно хотя бы раз в полгода или раз в год усовершенствовать защиту. Также на государственном уровне необходимо чаще дополнять и разрабатывать политику безопасности, обновлять акты и законодательную базу по защите информационной безопасности. В РФ стали уделять большое внимание средствам защиты, разработки в развитии отраслевых стандартов информационной безопасности и периферийных облачных вычислениях, создании центров разработки, мониторинга и реагирования на инциденты информационной безопасности, а также разработку и усовершенствование правовой и нормативной базы ИБ для различных сфер деятельности и информационных технологий.

При организации работы необходимо заботиться о защите от утечек и угроз во время работы и обмена данных с провайдерами облачных услуг. Обязательно проверять уровень защиты, смотреть наличие шифрования, мер и сервисов, предоставляемых провайдером. Конечно, наличие всех параметров для обычного пользователя, коммерческой компании, большой организации или КИИ будет иметь разные требования и условия [11].

Основные меры защиты от угроз и рисков необходимо выполнять и постоянно регулировать: окупаемость и рентабельность устанавливаемой защиты, защита от НСД, надежность, наличие многоступенчатости, комплексность. Так же защита должна обязательно одна перекрывать другую. Необходимо помнить, что какую бы защиту мы не устанавливали есть один самый важный ключевой фактор – это человеческий.

ЗАКЛЮЧЕНИЕ

Все имеющиеся средства защиты дорабатываться и усовершенствуются по мере появления новых рисков и атак. Например, тартегированные атаки, для них необходимы более новые разработки и защиты в ИБ. Применение аналитических систем, которые будут включать в себя базы знаний по различным существующим индикаторам и техникам, которые применяются в данный момент и внедряются новыми нарушителями, так же обязательно обращая внимание на то, что будет защищаться. Если грамотно и качественно развивать и обеспечивать безопасность в сфере облачных решений в РФ, то использование и покупка их будет расти и даст хорошие перспективы для их использования так как организация информационной безопасности для КИИ, интернет вещей, облачных и периферийных вычислений несет большую значимость для предприятий, которые используют устройства для интернета вещей, эксплуатируют критические инфраструктуры.

БЛАГОДАРНОСТИ

Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

Список литературы

1. Нестеренко В.Р. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними / В.Р. Нестеренко, М.А. Маслова // Научный результат. Информационные технологии. 2021. Т. 6. № 1. С. 48-54.
2. Ожиганова М.И. Методы и средства проведения анализа угроз локальной вычислительной сети предприятия / М.И. Ожиганова, А.О. Шейко, Е.М. Исакова, А.О. Миронова // в сборнике: цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021. С. 264-270.
3. Миронова А.О. Применение методики оценки угроз безопасности информации / А.О. Миронова, Ю.Ю. Гончаренко, А.С. Гоголь, А.Н. Фролова // Энергетические установки и технологии. 2021. Т. 7. № 4. С. 71-75.

4. Маслова М.А. Проблемы облачных сервисов и методы защиты от рисков и угроз / М.А. Маслова, Е.С. Кузьминых // Научный результат. Информационные технологии. 2022. Т. 7. № 3. С. 14-22.

5. Kucherova H. Modeling the stakeholder's behavior on the base of online inquiries about tertiary / H. Kucherova, D. Ocheretin, Y. Honcharenko, O. Mykoliuk // В сборнике: 2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 - Proceedings. 11. 2021. С. 35-40.

6. Аверьянов В.С. Оценка защищенности киберфизических систем на основе общего графа атак / В.С. Аверьянов, И.Н. Карцан // Южно-Сибирский научный вестник. 2022. № 1(41). С. 30-35.

7. Савельев Р.Н. Основные методы выявления нарушения информационной безопасности по данным мониторинга наземного комплекса управления спутниковой сети / Р.Н. Савельев, И.Н. Карцан // В сборнике: Актуальные проблемы авиации и космонавтики. 2021. С. 405-408.

8. Гончаренко Ю.Ю. Качественная оценка методик разработки автоматизированных средств / Ю.Ю. Гончаренко, Г.С. Погуляй, В.В. Пелись, М.Г. Щербаченко // Энергетические установки и технологии. 2022. Т. 8. № 2. С. 79-86.

9. Рябушей Ю.Н. Применение искусственных нейронных сетей в области защиты информации / Ю.Н. Рябушей, А.В. Лебеденко, Ю.Ю. Гончаренко // В сборнике: Современные проблемы радиоэлектроники и телекоммуникаций "РТ-2017". 2017. С. 284.

10. Жуков А.О. Информационная безопасность для проекта "Умный город" / А.О. Жуков, И.Н. Карцан, В.С. Аверьянов // Информационные и телекоммуникационные технологии. 2021. № 51. С. 39-45.

11. Серёдкин, С. П. Безопасность критической информационной инфраструктуры (краткий обзор современных подходов) // Информационные технологии и математическое моделирование в управлении сложными системами. 2021. № 4 (12). С. 30-38.

12. Главные угрозы безопасности в облаке (tadviser.ru) [Электронный ресурс]: – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D1%8B%D0%B5_%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%B2_%D0%BE%D0%B1%D0%BB%D0%B0%D0%BA%D0%B5.

References

1. Nesterenko V.R. Modern challenges and threats to the information security of public cloud solutions and ways of working with them / V.R. Nesterenko, M.A. Maslova // Scientific result. Information technology. 2021. T. 6. № 1. P. 48-54.

2. Ozhiganova M.I. Methods and means of analyzing threats to the local computer network of the enterprise / M.I. Ozhiganova, A.O. Sheiko, E.M. Isakova, A.O. Mironova//in the collection: digital transformation of science and education. Collection of scientific works of the II International Scientific and Practical Conference. 2021. P. 264-270.

3. Mironova A.O. Application of the methodology for assessing threats to information security / A.O. Mironova, Yu.Yu. Goncharenko, A.S. Gogol, A.N. Frolova // Energy installations and technologies. 2021. T. 7. № 4. P. 71-75.

4. Maslova M.A. Problems of cloud services and methods of protection against risks and threats / M.A. Maslova, E.S. Kuzminykh // Research result. Information technology. 2022. T. 7. № 3. P. 14-22

5. Kucherova H. Modeling the stakeholder's behavior on the base of online inquiries about tertiary / H. Kucherova, D. Ocheretin, Y. Honcharenko, O. Mykoliuk // В сборнике: 2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 – Proceedings. 11. 2021. P. 35-40.

6. Averyanov V.S. Assessment of the security of cyberphysical systems based on the general attack graph / V.S. Averyanov, I.N. Kartsan // South Siberian Scientific Bulletin. 2022. № 1(41). P. 30-35.

7. Savelyev R.N. The main methods of detecting information security violations according to monitoring data of the satellite network ground control complex / R.N. Savelyev, I.N. Kartsan // In the collection: Actual problems of aviation and cosmonautics. 2021. P. 405-408.

8. Goncharenko Yu.Yu. Qualitative assessment of methods for the development of automated means / Yu.Yu. Goncharenko, G.S. Pogulyay, V.V. Pelis, M.G. Shcherbachenko // Energy installations and technologies. 2022. T. 8. № 2. P. 79-86.

9. Ryabushey Yu.N. Application of artificial neural networks in the field of information protection / Yu.N. Ryabushey, A.V. Lebedenko, Yu.Yu. Goncharenko // In the collection: Modern problems of radio electronics and telecommunications "RT-2017." 2017. P. 284.

10. Zhukov A.O. Information security for the Smart City project / A.O. Zhukov, I.N. Kartsan, V.S. Averyanov // Information and telecommunication technologies. 2021. № 51. P. 39-45.

11. Seredkin S.P. Security of critical information infrastructure (a brief overview of modern approaches) // Information technologies and mathematical modeling in the management of complex systems. 2021. № 4 (12). P. 30-38.

12. Cloud Top Security Threats (tadviser.ru) [Electronic Resource]: - Accesss Mode: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:% D0% 93% D0% BB% D0% B0% D0% B2% D0% BD% D1% 8B% D0% B5 _% D1% 83% D0% B3% D1% 80% D0% BE% D0% B7% D1% 8B _% D0% B1% D0% B5% D0% B7% D0% BE% D0% BF% D0% B0% D1% 81% D0% BD% D0% BE% D1% 81% D1% 82% D0% B8 _% D0% B2 _% D0% BE% D0% B1% D0% BB% D0% B0% D0% BA% D0% B5.

Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института информационных технологий, аспирант, младший научный сотрудник Ростовского государственного экономического университета (РИНХ)

Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security Institute of Information Technologies, postgraduate student, junior researcher Rostov State Economic University (RINH)