DOI: 10.18372/2410-7840.22.14870
УДК 334.71:661-036.21

ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ В ПЕРІОД ПАНДЕМІЇ

Дмитро Мехед, Катерина Мехед, Михайло Шелест

Економіка всього світу сьогодні зазнає суттєвих збитків через пандемію, і шукає адекватні рішення як реагувати на загрозу COVID-19. 11 березня уряд України вийшов на стежку війни з COVID-19 і опублікував програму щодо запобігання поширенню коронавірусу в країні. Заборонили відвідування навчальних закладів; проведення всіх масових заходів, у яких бере участь понад 200 осіб. Була обмежена кількість пунктів пропуску через державний кордон. Компанії мали захищати здоров'я своїх співробітників і мінімізувати вплив на свій бізнес за допомогою надійного планування безперервності бізнесу. Існують різні події, в тому числі поточна пандемія коронавірусу, які здатні викликати значні збої в роботі бізнесу. Ці збої можуть призвести до тимчасової або постійної втрати критично важливих даних, включаючи життєво важливі записи, IT-інфраструктуру і персонал, необхідний для виконання бізнес-операцій. Щоб впоратися з хвильовим ефектом COVID-19 IT-фахівці повинні оцінити свої уразливості - і, якщо його ще немає, скласти плани дій в надзвичайних ситуаціях в разі серйозних збоїв обладнання. Складність в тому, що тут IT-фахівці повинні робити все можливе, поки вони працюють вдома або віддалено. Недостатньо досліджено питання виявлення нових загроз, викликаних пандемією COVID-19 для забезпечення безперервності бізнесу та виокремлення заходів протидії їм. Важливим є визначення ряду ключових моментів які повинні бути частиною плану забезпечення безперервності бізнесу на період пандемії для IT-фахівців. Метою проведеного дослідження було привернути увагу вчених, фахівців та працівників до вирішення питань забезпечення безперервності бізнесу в період пандемії.

Ключові слова: *Забезпечення безперервності бізнесу, IT-фахівці, ризики. пандемія, карантин.*

Вступ. Заходи по боротьбі з розповсюдженням коронавірусної хвороби у 2019-2020 роках (COVID-19) чинили безпрецедентний вплив на життя людей в усьому світі. Результати проведеного дослідження покликані допомогти зрозуміти сучасному бізнесу загрозу пандемічного спалаху в нашій країні. Карантинні заходи виявили проблеми, які необхідно вирішити, та визначили дії, які керівництво компаній має вжити на робочих місцях, щоб підготуватися до пандемії. Для того, щоб бути готовим, важливо чітке розуміння пандемії та її впливу на бізнес.

Аналіз останніх досліджень і публікацій. Були розглянуті останні публікації у відкритому доступі, включаючи публікації із забезпечення інформаційної безпеки під час віддаленої роботи у період карантину. Забезпеченню безперервності бізнесу, сутності понять «інформаційна безпека» та «кібербезпека» присвячено чимало наукових праць. Серед сучасних українських публікацій слід зазначити колективну монографію О Корченка, І Терейковського, Н Карпинського та С Тинимбаєва присвячену методам і засобам оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем. Забезпечення безперервності бізнесу розглядається значною групою вітчизняних (В. Ситниченко, Г. Кісельова, Є. Стоякін, В. Борсуковський, Ю. Борсуковський, В. Оніщенко) та зарубіжних дослідників, серед яких найвідоміші – Jahmiah Ferdinand-Hodkin, Tom Laureys , Jan Seidl, Jakub Hol, Steve Bassine, Blair Nimmo, Steve McGowan та ін.

Управління безперервністю бізнесу визначається як розширене планування і підготовка організації до підтримки бізнес-функцій або швидке відновлення роботи після аварії. Це також включає визначення потенційних ризиків, включаючи пожежі, повені, епідемії та пандемії або кібератаки [1]. Управління безперервністю - це не просто реакція на стихійне лихо або кібератаку. Вона починається з планування політики і процедур, розроблених, протестованих і використовуваних ще до виникнення інциденту. Політика визначає область дії програми, ключові блоки і структуру управління. Необхідно чітко сформулювати, чому необхідна безперервність бізнесу, а управління на цьому етапі має вирішальне значення.

Для забезпечення безперервності бізнесу вкрай важливо мати аварійний сценарій. У ситуації, що склалася життєво важливо реагувати якомога швидше, щоб пом'якшити вплив та інші ризики і підготувати організацію до подальшого спалаху пандемії COVID-19 і її можливих сценаріїв. Управління безперервністю бізнесу охоплює інфраструктурні, кібернетичні, службові, ділові,

операційні та комунікаційні ризики з метою управління організацією, яка стикається з новими проблемами і ризиками і хоче забезпечити безперервність операцій і виробництва.

Під час повсякденної діяльності і у відповідь на аварійні події (наприклад, збої) управління безперервністю бізнесу встановлює стратегічні та операційні рамки для активного підвищення корпоративної стійкості [2]. Мета зрозуміла: запобігти зупинці операцій або послуг.

Аналіз карантинних заходів [3], які впроваджувалися в Україні у період пандемії COVID-19 в 2020-му році дав можливість виокремити методи забезпечення неперервності бізнеса у схожих умовах.

COVID - початкові заходи:

- впровадити фундаментальні надзвичайні заходи в ситуації, що склалася;
- виконати всі рекомендації ВОЗ, МОЗ України;
- орієнтир введених заходів у вашій галузі;
- обмеження на поїздки співробітників або їх повна заборона.

COVID - інфраструктурні ризики:

- перевірка готовності інфраструктури та інших сервісів (SaaS, тощо) до збільшення навантаження на співробітників, що працюють віддалено;
- перевірка, чи можливо управляти корпоративними системами віддалено без фізичної присутності IT-співробітників (операції, підтримка, тощо);
- побудова карти окремих точок відмови в інфраструктурі при віддалених операціях, розробка контрзаходів;
- визначення обов'язків постачальників відповідно до SLA в разі виникнення надзвичайних ситуацій, підготовка необхідних змін;
- налаштування достатньої IT-підтримки для віддалено працюючих співробітників;
- пріоритетність доступу до корпоративних систем (управління, пріоритет вищого керівництва, тощо);
- перевірка кількості ліцензій додатків, що забезпечують віддалений доступ.

COVID - кібер ризики:

- перевірка безпеки і моніторинг програм для віддаленого доступу;
- тестові програми для віддаленого доступу (VPN, тощо) + патчі, оновлення;
- проведення інформаційної кампанії для конкретних випадків атак соціальної інженерії.

COVID - ризики співробітників:

- аналіз ключових ролей, які потребують присутності на місці, планування резервного плану на випадок їх відсутності (наприклад, взаємозаміна співробітників);
- розробити заходи, щоб допомогти співробітникам справлятися зі стресом і стресовими ситуаціями;
- організувати метод призначення і розподілу працівників на різних рівнях оперативного скорочення;
- налаштування доступу для мобільності співробітників (зміни, транспорт, тощо).

COVID - бізнес і операційні ризики:

- створення карти окремих точок відмови в організації (процеси, співробітники, технології) і проекту контрзаходів;
- встановлення заходів з надзвичайних ситуацій і організаційні інструкцій для забезпечення безперервності операцій відповідно до рівня ризику;
- створення планів реагування (процедури, розподіл співробітників, інструменти та інші ресурси);
- підготовка до проблем в ланцюжку поставок;
- організація роботи, яка не може бути виконана віддалено;
- підготовка до необхідності закрити офіс;
- стабілізація організації на випадок значного впливу на її економіку (план з оптимізації витрат, процесів і портфелів);
- підготовка сценаріїв, планів і заходів з відновлення бізнес-операцій (планів аварійного відновлення).

COVID - комунікаційні ризики:

- встановлення механізму спілкування з співробітниками (із позитивними тестами), партнерами, постачальниками, владою і громадськістю.

Аналіз досвіду Українських та закордонних компаній [1; 2; 4; 6], досліджень у галузі забезпечення безперервності бізнесу дав можливість нам сформувати контрольний список забезпечення безперервності IT, який допоможе організаціям захистити критично важливе IT-обладнання.

Контрольний список включає в себе список завдань, які повинні бути виконані до впровадження карантинних заходів, і повинен бути налаштований у відповідності до потреб організації. Контрольний список включає в себе наступні завдання для виконання:

1. Виконайте оцінку ризиків безпеки для конкретних загроз, включаючи захист від вірусів, виявлення вторгнень, запобігання хакерських атак і мережевих аварійних подій.

Якщо це можливо, попрацюйте з інтернет-провайдером, щоб оцінити ймовірність критичних ситуацій і отримати пропозиції щодо пом'якшення наслідків і загроз.

2. Визначте обладнання для комунікацій, необхідне для підтримання зв'язку під час пандемії, включаючи корпоративні мобільні телефони та рації та працюйте з начальником управління безперервності бізнесу для затвердження покупки.

3. Переконайтесь, що вся апаратура для підтримки зв'язку з персоналом працює і знаходиться у робочому стані. Скоординуйте ці дії з спеціалістом із забезпечення безперервного бізнесу.

4. Додайте інформацію про ліцензії апаратного та програмного забезпечення до робочого листа з інвентаризацією IT обладнання та надішліть керівнику з питань безперервності бізнесу.

5. Якщо ви працюєте з зовнішніми постачальниками IT-послуг, уточнюйте, які з них будуть доступні під час карантину.

6. Обговорюйте варіанти використання робочого обладнання за межами офісу з начальником управління безперервної роботи.

7. Налаштуйте хмарне сховище для доступу до важливих даних.

8. Забезпечте доступ керівного персоналу з віддалених місць, включаючи домашнє підключення до мережі, телефон, VPN для безпеки.

9. Визначте ефективність політики та процедур резервного копіювання та відновлення даних. Виконуйте резервні копії через регулярні інтервали, щодня, щотижня або щомісяця.

Підтримка домашніх користувачів і віддалене регулярне адміністрування системи - це одна з дуже важливих задач забезпечення безперервності бізнесу у період пандемії. Проте ремонт і модернізація фізичної інфраструктури, на яку ми спираємося, і більшості випадків, просто неможливі без присутності на місці. І без цієї присутності ймовірність того, що збої в роботі серверів, мереж та пристроїв зберігання даних залишаться без нагляду, зростає [5].

Нами було виокремлено ряд ключових моментів, які повинні бути частиною плану забезпечення безперервності бізнесу на період пандемії COVID-19.

Необхідно визначити конкретного співробітника (-ів) в якості точки контакту для координації дій із забезпечення готовності до пандемії. Його обов'язки будуть включати в себе відстеження новин і оголошень, інформування/підвищення інформованості ключових зацікавлених сторін про проблеми, оновлення плану забезпечення безперервності бізнесу; стежити за тим, що заплановано, відслідковувати і перевіряти операції. Це також може включати в себе відображення залежностей в IT-інфраструктурі і бізнес-сервісах, щоб зрозуміти, де можливі збої, і оцінювати вплив на ланцюжок створення вартості.

Віддалений доступ для співробітників буде єдиною можливістю для продовження роботи компанії. Навантаження на VPN буде зростати. Деякі організації можуть збільшити потужності за рахунок розгортання VDI, щоб надати більше віртуальних робочих місць віддаленим співробітникам. Все це збільшує навантаження на групи підтримки віддалених робочих місць, якщо співробітники стикаються з проблемами, працюючи вдома. Повинен бути встановлений належний моніторинг для вирішення проблем, пов'язаних з кінцевою точкою.

Якщо більшість або всі IT-співробітники працюватимуть удома, як ми встановили раніше, IT-інфраструктура перестає контролюватися і управлятися фізично. У разі виникнення проблеми з пристроєм, що призводить до його відмови, неможливим стає своєчасний ремонт обладнання, переналаштування, перезавантаження сервера для запобігання перебоїв. Таким чином брак ресурсів вплине на ключові бізнес-сервіси. Отже, окремі точки збою повинні бути визначені в карті можливих відмов, а плани забезпечення високої доступності та відпрацювання відмови повинні плануватися заздалегідь і впроваджуватися для забезпечення безперервності бізнесу [6].

Безпека це ключ. Оскільки співробітники отримують доступ до корпоративних даних з віддалених місць і з особистих пристроїв, вони можуть піддаватися загрозам інформаційної безпеки. Наявність належних заходів безпеки, таких як політика VPN/брандмауера, антивірусні інструменти, встановлені на пристроях кінцевого користувача, тощо, є необхідністю. Моніторинг відхилень або відхилень шаблону в доступі до даних може допомогти виявити порушення безпеки або потенційно небезпечні події.

Сховище є важливою частиною IT-інфраструктури. Всі дані та програми зберігаються на накопичувачах і дисках, або безпосередньо підключаються до серверів, або через мережі зберігання даних (SAN). Коли IT-фахівці залишають їх без нагляду навіть на короткі проміжки часу, існує більш висока ймовірність збою обладнання або збою живлення, що безпосередньо вплине на доступ до даних і, в свою чергу, на продуктивність додатків і взаємодія з користувачем. Щоб забезпечити безперервність бізнесу і високу доступність даних - будь то під час вірусної епідемії чи ні, IT-спеціалісти повинні зосередитися на:

1. Створенні двосторонніх або тристоронніх кластерів стійкості даних для обходу окремих точок відмови.

2. Реалізації автоматичного переходу на інший ресурс у разі виникнення збоїв.

3. Створенні періодичних знімків даних для доступу до зображень на певний момент часу в разі втрати даних.

4. Визначенні балансу навантаження (IOPS) між системами зберігання, щоб уникнути перевантаження і перевантаження основного сховища, обслуговуючого важливі для бізнесу дані.

Особливо в цей період відсутності співробітників в офісах важливо заздалегідь планувати непередбачені обставини і задіяти функції автоматичного і самовідновлюваного управління даними, які забезпечать доступність даних і допоможуть зберегти цілісність даних.

Висновки. В статті виокремлено основні загрози пандемії на забезпечення безперервності бізнесу та заходи протидії їм. Авторами був створений контрольний список, який включає в себе список завдань, які повинні бути виконані до впровадження карантинних заходів, і повинен бути налаштований у відповідності до потреб організації. В період карантинних заходів значною мірою збільшується навантаження на IT спеціалістів компанії. В статті визначено ряд ключових моментів які повинні бути частиною плану забезпечення безперервності бізнесу на період пандемії для IT-фахівців. Доцільність повного або часткового впровадження всіх запропонованих заходів має визначатися кожною компанією окремо, зважаючи на фінансові та інші види витрат та втрат під час пандемії.

ЛІТЕРАТУРА

[1]. О. Онуфрієнко, "Як власнику убезпечити свій бізнес після пандемії", *Економічна правда*, 2020. [Електронний ресурс]. Режим доступу: https://www.epravda.com.ua/columns/2020/04/28/659883/.

[2]. *Рекомендації для компаній, на роботу яких вплинула пандемія COVID-19*, 2020. [Електронний ресурс]. Режим доступу: https: // support. google. com / business/ answer/9773423?hl=uk.

[3]. *Карантин vs бізнес: як діяти в епоху обмежень*, 2020. [Електронний ресурс]. Режим доступу: https://mind.ua/publications/20208709-karantin-vs-biznes-yak-diyati-v-epohu-obmezhen.

[4]. *Public Health Agency of Canada,* 2020. [Електронний ресурс]. Режим доступу: https://www.canada.ca/en/public-health.html.

[5]. *Key Steps Help Ensure Business Continuity During COVID-19 Pandemic,* 2020. [Електронний ресурс]. Режим доступу до ресурсу: https://www.facilitiesnet.com/emergencypreparedness/ contributed/ Key - Steps-Help- Ensure- Business- Continuity-During-COVID-19-Pandemic--45982.

[6]. *Business continuity in a COVID-19 world,* 2020. [Електронний ресурс]. Режим доступу до ресурсу: https://home.kpmg/xx/en/home/insights/2020/03/business-continuity-in-a-covid-19-world.html.

ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА В ПЕРИОД ПАНДЕМИИ

Экономика всего мира сегодня испытывает существенные убытки из-за пандемии, и ищет адекватные решения как реагировать на угрозу COVID-19. 11 марта правительство Украины вышло на тропу войны с COVID-19 и опубликовал программу по предотвращению распространения коронавируса в стране. Запретили посещение учебных заведений; проведение всех массовых мероприятий, в которых принимает участие более 200 человек. Было ограниченное количество пунктов пропуска через государственную границу. Компании должны были защищать здоровье своих сотрудников и минимизировать влияние на свой бизнес с помощью надежного планирования непрерывности бизнеса. Существуют различные события, в том числе текущая пандемия коронавируса, которые могут вызвать значительные сбои в работе бизнеса. Эти сбои могут привести к временной или постоянной потери критически важных данных, включая жизненно важные записи, ИТ-инфраструктуру и персонал, необходимый для выполнения бизнес-операций. Чтобы справиться с волновым эффектом COVID-19 ИТ-специалисты должны оценить свои уязвимости и, если его еще нет, составить план действий в чрезвычайных ситуациях в случае серьезных сбоев оборудования. Сложность в том, что здесь ИТ-специалисты должны делать все возможное,

пока они работают дома или удаленно. Недостаточно исследованым остаётся вопрос выявления новых угроз, вызванных пандемией COVID-19 для обеспечения непрерывности бизнеса и выделение мер противодействия им. Важным является определение ряда ключевых моментов, которые должны быть частью плана обеспечения непрерывности бизнеса на период пандемии для ИТ-специалистов. Целью проведенного исследования является привлечение внимания ученых, специалистов и работников к решению вопросов обеспечения непрерывности бизнеса в период пандемии.
Ключевые слова: обеспечение непрерывности бизнеса, ИТ-специалист, риски. пандемия, карантин.

ENSURING BUSINESS CONTINUITY DURING A PANDEMIC

Business continuity is a priority for participants in the financial sector and financial authorities. Business continuity management, an important component of operational risk management, is an approach that covers all aspects of the business and includes policies, standards and procedures to ensure or timely resumption of certain business operations in case of disruption in business continuity. The goal of the management is to minimize the consequences of violation – operational, financial, legal, material consequences, as well as damage to reputation, etc. Effectively manage business continuity, in which special attention is paid to the nature of the impact, and not to the source of the violation. This allows participants in the financial sector and financial authorities to have more room to maneuver in the event of various violations. At the same time, organizations cannot ignore the nature of the risks they face. Effective business continuity management usually includes analyzing the impact of various events on business continuity, choosing a recovery strategy and drawing up a business continuity plan, as well as providing audit programs, staff training and information programs, as well as information exchange and crisis management programs. It is impossible to predict the next crisis, but you can prepare for it. Failures of established business processes can affect an organization of any scale, regardless of country. Natural disasters, interruptions in the supply of electricity, political instability and even an epidemic of the virus - each organization should have a plan "B", which will ensure the continuity of its work in any unforeseen situation. We are amidst a global pandemic. The coronavirus COVID-19 has been spreading like wildfire across geographies affecting people's health and well-being. To contain its spread, many organizations in both the private and public sector have encouraged – and in some parts of the world enforced – their employees to work from home. This includes IT staff that vigilantly care for our datacenters.
Keywords: ensuring business continuity, IT specialist, risks, pandemic, quarantine.

Мехед Дмитро Борисович, к.п.н., доцент кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: d.mekhed@gmail.com.
Orcid ID: 0000-0003-3905-3620.
Мехед Дмитрий Борисович, к.п.н., доцент кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Mekhed Dmytro, PhD, associate professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology.

Мехед Катерина Миколаївна, аспірант кафедри математики та економіки Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка.
E-mail: ekaterina.mekhed@gmail.com.
Orcid ID: 0000-0003-4599-4099.
Мехед Екатерина Николаевна, аспирант кафедры математики и экономики Национального университета «Черниговский колегиум» имени Т. Г. Шевченка.
Mekhed Kateryna, PhD Student of mathematics and economics department, T.H. Shevchenko National University «Chernihiv Colehium».

Шелест Михайло Євгенович, д.т.н., професор кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: mishel3141@gmail.com.
Orcid ID: 0000-0002-8565-0525.
Шелест Михаил Евгеньевич, д.т.н., профессор кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Shelest Mykhailo, Doctor of Technical Sciences, Professor of the Department of Cybersecurity and Mathematical Modeling, Chernihiv National Technological University.