Список використаних джерел:

1. Про правовий режим воєнного стану : Закон України від 12 травня 2015 року № 389-VIII (із змінами станом на 29.09.2022). URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 21.11.2022).

2. Про вищу освіту : Закон України від 1 липня 2014 року № 1556-VII. Дата оновлення: 18.03.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-18.

3. Енциклопедія освіти / Акад. пед. наук України, головний ред. В.Г. Кремень. К. : Юрінком Інтер, 2008. 1040 с.

4. Вайда Т.С. Деякі проблемні питання розвитку дистанційного навчання в закладах вищої освіти МВС України // *Матеріали Міжнародної науково-практичної конференції «Реформування правоохоронних органів України у світлі змін євроінтеграційних процесів»* (20 березня 2020 року, ХФ ОДУВС). Херсон : Олді-плюс, 2020. С. 12-19.

5. Вайда Т.С. Педагогічні можливості деяких сучасних інформаційних технологій як засобів дистанційного навчання здобувачів вищої освіти у закладах МВС України. *Юридичний бюлетень* : наук. журнал. Одеса: ОДУВС, 2020. Випуск 12 (12). С. 202-212.

УДК 004.77

ГОРЕЛОВ ЮРІЙ ПЕТРОВИЧ,

кандидат технічних наук, доцент, доцент кафедри кібербезпеки та DATA-технологій Харківського національного університету внутрішніх справ

https://orcid.org/0000-0002-0330-5008

КОБЗЕВ ІГОР ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформатики та комп'ютерної техніки

Харківського національного економічного університету ім. С. Кузнеця

https://orcid.org/0000-0002-7182-5814

ЄВСТРАТ ДМИТРО ІВАНОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформаційних систем

Харківського національного економічного університету ім. С. Кузнеця

https://orcid.org/0000-0001-8393-6063

ХМАРНІ СЕРВІСИ, ЯК ЗАСІБ ЗАХИСТУ ВІД АТАК ПІД ЧАС ВІЙНИ

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни.

Найбільш серйозним та руйнівним видом загроз для державних структур є DDoS-атака. DDoS-атака — це метод атаки, при якому хакери націлюються на сервери і перевантажують їх користувальницьким трафіком. Коли сервер не справляється з вхідними запитами, сайт, програма або додаток, розташовані на ньому, відключаються або працюють з низькою продуктивністю.

Наприклад, після початку повномасштабного вторгнення Росії в Україну Мінцифри створило добровільну кіберармію, яка здійснює DDoS-атаки на ресурси країни-окупанта. За короткий період IT ARMY of Ukraine поклала сайти російських пропагандистів, органів влади, компаній із держсектора, енергетики, банків, рітейлу, сервіси грошових переказів, бухгалтерської звітності та багато іншого [1].

Сьогодні в умовах війни з'явився різкий зростання запитів на хмарні технології. Організація резервних майданчиків для зберігання даних, резервного копіювання та кібербезпеки стали основними викликами для держави та бізнесу після вторгнення РФ на територію України.

Постановою Кабінету міністрів України від 12 березня 2022 року в умовах воєнного стану державні установи отримали дозвіл на розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України. Це

розширило можливості використання хмар. Тепер державні організації можуть використовувати всі їхні переваги, щоб без перешкод працювати у складний воєнний період [2].

Державні установи всіх рівнів потребують перехід на хмарні інфраструктури. Це необхідно для швидкого надання населенню якісних послуг, гнучку, масштабну та економічну технологічну базу. Автоматизація процесів та їхнє перенесення у хмарне середовище дають можливість максимально прискорити процедуру надання послуг, а також забезпечити громадянам мінімальні витрати часу на отримання тієї чи іншої інформації. Першочергова загроза використання хмарних технологій у держсекторі – безпека зберігання даних. За кордоном із цією проблемою вирішили боротися шляхом використання приватних хмар, коли обладнання установи знаходиться безпосередньо всередині мережі держструктури. Традиційною проблемою використання публічних хмарних платформ державними структурами є специфічні вимоги до безпеки. Враховуючи, що держсектор є одним із найбільших ІТ-замовників у нашій країні, найлогічніше припустити, що він піде шляхом побудови «громадської хмари» — хмарної платформи, яка використовуватиметься іншими держструктурами зі схожими вимогами до безпеки.

Через масштабні бойові дії в Україні робота дата центрів під загрозою, оскільки територія країни знаходиться під постійними обстрілами армією РФ, тому навіть власники серверних не можуть дати гарантії, що дата центрів не постраждають.

Воєнний стан в Україні викликає занепокоєння також через нові виклики у забезпеченні безперебійної роботи критичних сервісів та систем, які можуть бути пошкоджені або виведені з ладу внаслідок бойових дій. Перенесення ІТ-інфраструктури в хмару або створення сайтів аварійного відновлення у глобальних хмарних ЦОД дозволить гарантувати необхідний рівень доступності.

Для цього потрібно обрати провайдера хмарних сервісів, враховуючи наявні компетенції ІТ-спеціалістів, визначити черговість та критичність перенесення тих чи інших елементів ІТ-архітектури в хмару; організувати

збереження резервних копій інформації в хмарі, організувати сайти аварійного відновлення в публічній хмарі в Європі або США. Наприклад компанія Microsoft вже надала безоплатні хмарні сервіси до кінця 2022 року і продовжила термін до 2023 року. Сьогодні значна частина критично важливої інформації перетворюється на цифровий вигляд за межі контрольованої зони. У зв'язку з цим ЦОД, які надають хмарні послуги, повинні взяти на себе цю роль і забезпечувати захист інформації шляхом запровадження внутрішніх сервісів, що обмежують доступ до інформації неавторизованим особам. Головний висновок із всього вищезазначеного — необхідно забезпечити свої корпоративні дані від наслідків війни можна, перемістивши їх на постійне або тимчасове зберігання у хмарне сховище

Список використаних джерел:

1. Що таке кібербезпека і як бізнесу захиститися від DDoS-атак. GigaCloud //URL: https://gigacloud.ua/blog/navchannja/scho-take-kiberbezpeka-i-jak-biznesu-zahistitisja-vid-ddos-atak

2. Підгайна Є. Тримаємо стрій: добірка корисних хмарних сервісів для відновлення роботи бізнесу в умовах війни / Євгенія Підгайна // Інтерфакс-Україна – URL: https://mind.ua/publications/20238662-trimaemo-strij-dobirka-korisnih-hmarnih-servisiv-dlya-vidnovlennya-roboti-biznesu-v-umovah-vijni.

УДК 004.8

ГУДІЛІН ВЛАДИСЛАВ ВЛАДИСЛАВОВИЧ

слухач магістратури факультету №5