DOI 10.15276/imms.v11.no4.296
УДК [004.056.54:334]614.46

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 4, pp. 296-302

ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЙ В УМОВАХ ПАНДЕМІЇ COVID-19 ТА КАРАНТИННИХ ОБМЕЖЕНЬ

Д.Б. Мехед[1], К.М. Мехед[2]

[1]Національний університет «Чернігівська політехніка»
вул. Шевченка, 95, м. Чернігів, 14035, Україна. E-mail: d.mekhed@gmail.com
[2]Національний університет «Чернігівський колегіум» імені Т. Г. Шевченка
вул. Гетьмана Полуботка, 53, м. Чернігів, 14013, Україна. E-mail: ekaterina.mekhed@gmail.com

Метою роботи є дослідження наслідків впливу дистанційної, віддаленої роботи співробітників організацій, яка стала вимушеною у зв'язку з пандемією COVID-19 та введенням карантинних обмежень, які розпочалися на початку 2020 року і все ще продовжуються на момент написання цієї статті. Цілі дослідження зосереджені на визначенні різних шляхів реалізації посилення спроможностей організацій для протидії кіберзагрозам, забезпеченні належного рівня їх захищеності. В роботі розглянута проблема розповсюдження кіберзагроз майже у всіх сферах життя людини, окреслена важливість відповідних змін алгоритмів, стратегій та тактик до протидії ним, підкреслена значущість вміння з максимальною швидкістю виявляти вразливості та кібератаки задля влучного та ефективного реагування, обговорено важливість оцінки кожною організацією можливих ризиків з вживання відповідних заходів з метою підвищення рівня кібербезпеки до кращого захисту організацій. Робота містить збір даних про свіжі дослідження, проведені в рамках вивчення динаміки віддаленої, дистанційної роботи та ризиків кібербезпеки як в наслідок карантинних обмежень у зв'язку з Covid 19 так і не обумовлених цією причиною. Пандемія COVID-19 створила нові проблеми для організацій, оскільки вони повинні адаптуватися до операційної моделі, в якій дистанційна робота вдома стала «нормою нашого часу». Обмеження, запроваджені урядом у відповідь на пандемію, спонукали співробітників працювати з дому і навіть залишатися вдома. Як наслідок, інформаційно-комунікаційні технології стали ще важливішими як у роботі, так і в особистому житті кожного. Незважаючи на зростання потреби в технологіях, слід зауважити, що багато організацій досі не реалізували кібербезпечне середовище дистанційної роботи. У цій статті розглядається вплив COVID-19 на кібер-ризики та заходи щодо їх зниження, які можуть прийняти організації.

Ключові слова: кібербезпека, інформаційні загрози, дистанційна робота, безпека організацій, пандемія COVID-19.

Вступ

21 століття під вагомим впливом шостого технологічного укладу разом з ризиками їм обумовленим, з котрими зустрічається цивілізація сьогодення, важливого пріоритету у системі національної безпеки України набуває питання забезпечення кібербезпеки. Наразі спостерігаємо удосконалення технічного рівня реалізації кіберзагроз, впроваджуються та успішно використовуються новітні інструменти, алгоритми й механізми кібератак, розробляються нові ідеї для маніпуляції суспільної поведінки та думки. Безперечно треба врахувати вплив пандемії COVID-19 та карантинних обмежень, пов'язаних з нею, адже очевидно, що даний вплив буде довготерміновий на системи світопорядку, що в свою чергу неминуче призведе до посилення ролі інформаційних технологій та електронних комунікацій у буденному спілкуванні та спілкуванні на роботі, що обумовлює зростання вразливості процесів інформаційної обробки та обробки персональних даних. Важливого значення в досягненні окресленої нами пріоритетності забезпечення кібербезпеки набуває посилення можливостей та ефективності нацсистеми кібербезпеки для протидії

кіберзагрозам в безпековому середовищі сьогодення, забезпечення на потрібному рівні захищеності персональних даних, даних організації, інформаційних ресурсів тощо шляхом впровадження в державі та організаціях зокрема відповідних додаткових заходів.

Пандемія COVID-19 створила нові проблеми для організацій, оскільки вони повинні адаптуватися до операційної моделі, в якій дистанційна робота вдома стала «нормою нашого часу». Обмеження, запроваджені урядом у відповідь на пандемію, спонукали співробітників працювати з дому і навіть залишатися вдома. Як наслідок, інформаційно-комунікаційні технології стали ще важливішими як у роботі, так і в особистому житті кожного. Незважаючи на зростання потреби в технологіях, слід зауважити, що багато організацій досі не реалізували кібербезпечне середовище дистанційної роботи. У цій статті розглядається вплив COVID-19 на кібер-ризики та заходи щодо їх зниження, які можуть прийняти організації.

Аналіз останніх досліджень та публікацій

Проблема дистанційної роботи через COVID-19 і карантинних обмежень докладно розглянута у працях зарубіжних науковців E. Ingusci, A. Khanna, A. Manuti, M. Molino, питанню кібербезпеки та кіберзагрозам в епоху COVID 19 присвячені праці науковців G. Anderson, S. Blumenfeld, S. Brohi, S. Chakraborty, G. Crossland, E. DeFilippis, Y. Hernandez, V. Hooper, S. Impink, N. Khan, J. Polzer, R. Sadun, M. Singell, N. Zaman. На сьогодні вітчизняними науковцями недостатньо уваги приділяється методам протидіїї кіберзагрозам для захисту організацій у період пандемії та карантину.

Мета роботи

Дослідити наслідки впливу дистанційної, віддаленої роботи співробітників організацій, яка стала вимушеною у зв’язку з пандемією COVID-19 та введенням карантинних обмежень, які розпочалися на початку 2020 року і все ще продовжуються на момент написання цієї статті. Цілі дослідження зосереджені на визначенні різних шляхів реалізації посилення спроможностей організацій для протидії кіберзагрозам, забезпеченні належного рівня їх захищеності.

Виклад основного матеріалу

Наразі ми спостерігаємо істотні зміни майже у всіх сферах нашого життя під впливом четвертої промислової революції – суспільство функціонує по-іншому, інформаційно - комунікаційні технології мають всюдипроникливий вплив і разом з великими можливостями відкривають поле і для динамічного розвитку злочинів у цій сфері. З кожним роком кіберзлочини стають дедалі масовішими й небезпечнішими. Згідно Стратегії Кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021 «Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі» [1].

У 2020 році на рівень кіберзлочинності вплинув не тільки стрімкий розвиток інформаційних технологій, а й відомі карантинні обмеження у зв’язку з пандемією через вірус COVID-19: перехід співробітників організацій на віддалену роботу, які в свою чергу все більше покладаються на технології для обміну тієї чи іншої інформації, емоційна нестабільність особистості через страхи та накладені обмеження, зростання кількості онлайн розрахунків тощо. В [1] зазначено, що «Пандемія COVID-19 матиме

довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних. Це вимагає забезпечення належного рівня їх захищеності та змушує державу і бізнес впроваджувати додаткові механізми і заходи щодо належного функціонування і захисту всіх необхідних для життєдіяльності інформаційних ресурсів і систем.»

Згідно з звітом [2] ми спостерігаємо, що кількість кібератак у світі за 2020 рік у 2,2 рази перевищила кількість витоків даних організацій, що виникла через помилку. У 2020 році кількість зламаних записів збільшилась у 1,5 рази ніж у 2019 році. За даними фахівців, за минулий рік було скомпрометовано понад 20 мільярдів записів персональних даних та платіжної інформації [3] і завдано збитків за даними американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) на трильйон доларів США, що становить понад один відсоток світового ВВП.

За даними звіту Голови Національної поліції України про результати відомства у 2020 році в Україні наразі зафіксовано всі ключові «класичні» кіберзлочини і їх кількість зросла у порівнянні з попередніми роками. У даному звіті зазначено про наявність крадіжок грошей з банківських рахунків, різних видів шахрайств з платіжними картами, поширення комп'ютерних вірусів, викрадення різних типів даних, онлайн-торгівля наркотиками та зброєю, формування у дітей суїцидальної поведінки. За даними кіберполіції у 2020 році зареєстровано понад 5 тисяч кіберзлочинів із завданими матеріальними збитками на суму 241 млн. гривень, з яких 180 млн. гривень було відшкодовано. Враховуючи актуальність даної проблеми кіберполіцією була відкрита пряма лінія сервісної служби з надання громадянам консультацій з питань кібербезпеки, яка за 9 місяців своєї роботи прийняла більш ніж 100 000 дзвінків та понад 40 000 електронних звернень. У світлі викладеного саме протидія кіберзлочинам відмічена як пріоритет у діяльності Національної поліції. [4]. Але як підкреслює голова департаменту кіберполіції О. Гринчак, на жаль за чотири перші місяці 2021 року кількість кіберзлочинів продовжує зростати і знову ж таки збільшилась на 25% у порівняні з попереднім роком [5].

Тож з огляду на вищезазначене гостро постає проблема необхідності підвищення рівня кібербезпеки, вживання відповідних заходів до кращого захисту організацій. Наряду з такими завжди актуальними азами, як правила створення та використання надійних паролей, правила безпечного користування соціальними мережами, безпечний онлайн-шопінг, особливо актуальні наразі рекомендації націлені на зниження рівня кіберзлочинності, враховуючи загрози, які або посилились, або виникли чи адаптувались в наслідок умов пандемії.

Кожній організації треба враховувати те, що практика кібербезпеки вдома відрізняється від такої в офісі, тому співробітників необхідно інформувати та навчати новим зразкам поведінки та методам, які їм за необхідності треба буде використовувати. У дослідженні [6] у ході опитування понад півтисячі віддалених та штатних співробітників виявили ряд факторів, які сприяли дотриманню політики інформаційної безпеки та відмінностей в поведінці та діях віддалених та штатних співробітників. Результати дослідження виявили, що співробітники, які працюють дистанційно відрізняються від офісних співробітників передбачуваним рівнем поінформованості про політику безпеки та конфіденційності, самоефективністю та намірами дотримуватися нормативних вимог. Ці результати свідчать, що відсутність підтримки (чи то усної, демонстративної чи матеріальної) знижує здатність дистанційних співробітників усвідомлювати політику безпеки та конфіденційності у своїй організації та відповідно здатність її дотримуватися. Ці висновки підтверджуються попередньою роботою [7] цих науковців, яка демонструє, як «статус дистанційного працівника» може призвести до зниження поінформованості про інформаційну безпеку. Зарубіжні дослідники стверджували, що робота вдома збільшує

ризик (зазвичай ненавмисних) внутрішніх загроз. Так, згідно з дослідженням [7], третина організацій, які приймали участь в опитуванні, зазнала кібератаки внаслідок того, що співробітник працював за межами периметра безпеки підприємства. P. Chapman у [8] стверджує, що робота з дому може викликати ті ж проблеми, що й така політика організації як BYOD («bring your own device» або «принеси свій власний пристрій»). Якщо працівники працюють на особистих пристроях, вони мають бути захищені на рівні, санкціонованому компанією. Треба враховувати, що зловмисники в кіберпросторі використовують пандемію та націлені на домашніх працівників, намагаючись вкрасти інформацію [9]. K. Okereafor та O. Adebola дають наступні рекомендації у світлі досліджуваної проблеми: тестувати комерційні веб-сайти перед здійсненням платежів, проявляти пильність щодо фішингових листів та інших методів соціальної інженерії, встановлювати антивірусне програмне забезпечення, уникати кліків на підозрілі веб-адреси та URL-адреси, перевіряти джерела інформації про коронавірус та створювати резервні копії даних [10]. Що стосується паролей, то поради щодо їх надійності залишаються актуальними як і раніше[11]. Хоча експерти з кібербезпеки в найближчі 10 років сподіваються, що цей напрямок буде розвиватися і ми матимемо більше можливостей аутентифікації без паролей. Найближчим десятиліттям прогнозується більше біометрії та перехід на додаткові методи аутентифікації за допомогою мобільних пристроїв, які уже завжди з нами.

Спеціалістами з кібербезпеки запропоновані різні моделі для подолання проблем поінформованості про інформаційну безпеку при дистанційній роботі. Частина з них ґрунтується на припущенні, що співробітників можливо змусити знайомитися з ризиками, пов’язаними з виходом у кіберпростір, примушуючи розміщувати модулі інформаційної безпеки в мережі. Однак ця модель не гарантує, що користувачі з більшою ймовірністю дотримуватимуться політики організації, оскільки поінформованість не завжди призводить до зміни поведінки. Крім того, є ймовірність виникнення негативної реакції персоналу на примусове навчання, що може призвести до зниження довіри до роботодавця. Інша модель основана на припущенні, що знання та поінформованість про інформаційну безпеку, які отримані одного разу на робочому місці, переносяться в домашнє середовище. Автори цієї моделі роблять припущення, що така модель навчання дає можливість відійти від програм підвищення обізнаності організації та перейти до стратегій підвищення обізнаності, що в свою чергу сприятимуть розвитку всебічної індивідуальної культури безпеки для користувачів незалежно від того, чи працюють вони в офісі чи дистанційно [12].

Вважаємо за доцільне, щоб кожна організація оцінила які ризики викликають найбільше занепокоєння. Оцінка безпеки моделей дистанційної роботи повинна включати запитання: Як перехід у режим дистанційної роботи змінює нашу позицію у сфері кібербезпеки? Які кібер-гігієнічні методи ми використовуємо, а які потрібно додати для дистанційної роботи? Якими ще ризиками – операційними, нормативними та нормативно-правовими – ми повинні керувати?

В довгостроковій перспективі треба виділити наступні стандарти безпеки та рішень організації безпечної дистанційної роботи:

Підключення та пристрої:

- Інфраструктура на запит з використанням хмарних технологій (scale up та scale out).
- Хмарна безпека та безпека мережі.
- Безпека кінцевих точок.

Операції і доступ:

- Віртуальні операційні центри безпеки (SOC), які дозволяють віддалено працювати аналітикам, підвищуючи продуктивність та доступність.
- MSSP як економічне рішення.

- Платформа ідентифікації, що забезпечує безперебійний, легкий та простий цифровий досвід для клієнтів та співробітників.
- Оновлені алгоритми та аналітичні рішення для виявлення аномальної поведінки та встановлення цілісної ідентичності.

Координація:

- У межах міжфункціональних команд, неперервна оцінка, визначення пріоритетів та плани реагування для пом'якшення потенційних ризиків, пов'язаних із третіми сторонами.
- Надійний аналіз ризиків і планування стратегій для врахування можливих збоїв.

Актуальними на ринку кібербезпеки є нижчезазначені професійні послуги, які направлені на підвищення рівня захисту організацій: виявленні кібератак, протидії кібератак, відбитті та нейтралізації наслідків кібератак та кіберінцидентів. А саме:

- внутрішнє і зовнішнє тестування на проникнення в мережу;
- тести на проникнення (послуги етичних хакерів);
- аналіз захищеності вихідного коду;
- аналіз захищеності веб-додатків;
- аналіз захищеності інтерфейсу взаємодії з додатками (API);
- аналіз захищеності мобільних додатків.

Консалтинг з кібербезпеки пропонує:

- CISO as Service або віртуальну команду з кібербезпеки;
- управління кібер-ризиками;
- відновлення після кіберінцидентів;
- оцінка відповідності GDPR та ISO27001;
- аудит кібербезпеки;
- вибір постачальників і підрядників;
- безпека аутсорсингу;

управління обізнаністю співробітників;

- консультаційна підтримка;
- розслідування кіберінцидентів.

Наразі 42% директорів організацій, які брали участь у опитуванні PwC, підкреслили, що робоча сила/зниження продуктивності входять в трійку їх головних побоювань пов'язаних з COVID-19. Організаціям потрібно прискорити свою цифрову трансформацію, і сьогодні кібербезпека є вкрай нагальною потребою. Якщо не враховувати ризики кібербезпеки, це може мати серйозні наслідки для репутації, експлуатації, законодавства та дотримання нормативних вимог.

Висновки

В роботі розглянута проблема розповсюдження кіберзагроз майже у всіх сферах життя людини, окреслена важливість відповідних змін алгоритмів, стратегій та тактик до протидії ним, підкреслена значущість вміння з максимальною швидкістю виявляти вразливості та кібератаки задля влучного та ефективного реагування, обговорено важливість оцінки кожною організацією можливих ризиків з вживання відповідних заходів з метою підвищення рівня кібербезпеки до кращого захисту організацій.

Робота містить збір даних про свіжі дослідження, проведені в рамках вивчення динаміки віддаленої, дистанційної роботи та ризиків кібербезпеки як в наслідок карантинних обмежень у зв'язку з COVID-19 так і не обумовлених цією причиною.

Цифровий простір у зв'язку з стрімкими змінами вимагає більшої спроможності системи кібербезпеки як організацій так і держави в цілому, її ефективності та збалансованості, яка може видозмінюватися залежно від змін безпекового середовища, забезпечуючи їх безпечне функціонування.

Подальша робота має на меті вивчення стратегій, що використовуються лідерами кібербезпеки, зібрання передового досвіду протидії кібератакам задля розуміння як різні

організації адаптувалися до нових форм роботи зберігаючи/зменшуючи свою вразливість до кібер-ризиків, а також досвіду який використовується для підтримки довіри співробітників, розвитку командної роботи, захисту психічного здоров'я членів команди, зниження інсайдерського ризику та людського фактору.

Список літератури

1. Стратегія кібербезпеки України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
2. Cyber Security solutions and Products. 2020 cyber security statistics. URL: https://www.itgovernance.co.uk/
3. Статистика з кібербезпеки за 2020 рік. URL: https://10guards.com/ua/articles/2020-cybersecurity-statistics/
4. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf
5. Кіберполіція. Національна поліція України. URL: https://www.cyberpolice.gov.ua
6. Johnston A. C., Wech B., Jack E., Beavers M. Reigning in the Remote Employee: *Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes*. AMCIS. 2010 P. 493.
7. Johnston A. C., Wech B., Jack E. Engaging remote employees: The moderating role of "remote" status in determining employee information security policy awareness. *Journal of Organizational and End User Computing (JOEUC).* 2000. V. 25(1). P.1-23.
8. Cybsafe. Remote working poses significant security risk to UK's SME businesses, new research reveals. *Cybsafe*. 2018. URL: https://www.cybsafe.com/press-releases/remote-working-poses-significant-security-risk-to-uks-sme-businesses-new-research-reveals
9. Chapman P. Are your IT staff ready for the pandemic-driven insider threat? *Network Security*, 2020. No.4, P.8-11.
10. Okereafor K., Adebola O. Tackling the Cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Journal Homepage*. 2020. No. 8 (2). URL: http://ijmr. net
11. Правила створення та використання надійних паролів – рекомендації кіберполіції. URL: https://www.cyberpolice.gov.ua/article/pravyla-stvorennya-ta-vykorystannya-nadijnyx-paroliv--rekomendacziyi-kiberpolicziyi-3711/
12. Talib S., Clarke N.L., Furnell S. M. Establishing a personalized information security culture. *Int. J. of Mobile Communications*. 2011. Vol. 3 No. 1. P. 67-79.

BASIC PRINCIPLES OF PROVIDING CYBERSECURITY OF ORGANIZATIONS IN THE COVID-19 PANDEMIC CONDITIONS AND QUARANTINE RESTRAINTS

D. Mekhed, K. Mekhed

[1]National Chernihiv Polytechnic University
Shevchenko, 95, Chernihiv, 14035, Ukraine. E-mail: d.mekhed@gmail.com
[2] T.G. Shevchenko National University «Chernihiv Collegium»
Hetman Polubotok, 53, Chernihiv, 14013, Ukraine. E-mail: ekaterina.mekhed@gmail.com

In the 21st century, cyber security is becoming an important issue for the national security of Ukraine. This is due to the active formation of the sixth technological order and the risks that society faces today. Currently, there is an improvement in the technical level of the implementation of cyber threats, the latest tools, algorithms and mechanisms of cyber-attacks are being introduced and successfully used, and new ideas are being developed to manipulate public behavior and opinion. The impact of the COVID-19 pandemic and the quarantine restrictions associated with it must be taken into account. The impact on the systems of the world order of these restrictions will be long-term, which will lead to an increased role of information technology and electronic communications in everyday communication and at work. This causes an increase in the vulnerability of information and personal data processing processes. It is of great importance to strengthen the capabilities and effectiveness of the national cybersecurity system to counter cyber threats in the modern security environment, to ensure a high level of protection of personal data, organization data and information resources by introducing appropriate additional measures in the state and organizations. The paper considers the problem of the spread of cyber threats in almost all areas of human life, describes the importance of appropriate changes in algorithms, strategies and tactics to counter them, emphasizes the importance of the ability to identify vulnerabilities and cyber-attacks as quickly as possible for accurate and effective response, taking appropriate measures in order to increase the level of cyber security to better protect organizations. Due to rapid changes, the digital space requires a greater ability of the cybersecurity system of both organizations and the state as a whole, its effectiveness and balance, which can change depending on changes in the security environment, ensuring their safe functioning. The purpose of further research is to study the strategies used by cybersecurity leaders, to collect best practices in countering cyberattacks to understand how various organizations have adapted to new forms of work, maintaining / reducing their vulnerability to cyber risks, as well as the experience used to maintain employee confidence, team development. Work, protecting the mental health of team members, reducing insider risk and the human factor. The article contains a collection of data on recent research conducted as part of the study of the dynamics of telecommuting, remote work and cybersecurity risks both due to quarantine restrictions due to COVID-19 and not due to this reason.

Keywords: cybersecurity, information threats, remote work, organization security, COVID-19 pandemic