2. Зорій, О.М., Коваленко Т.В. Особливості застосування аутсорсингу. *Економічний аналіз* : зб. наук. праць / Тернопільський національний економічний університет Тернопіль : Видавничо-поліграфічний центр Тернопільського національного економічного університету "Економічна думка", 2013. - Том 14. № 3. С. 18-28.

3. Гейко О.Л. Аутсорсинг у сільському господарстві провідних країн світу - досвід для України. *Агросвіт*. 2021. №3. С. 75-80

4. Дідух О.В. Основні види аутсорсингу в господарській діяльності підприємств. *Вісник Хмельницького національного університету*. 2012. №2 т.1. С. 29-33.

УДК 351.865(477)

Кулакова С.Ю., к.е.н, доцент; Богдан Б.В., магістрант
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

КІБЕРРИЗИКИ: НОВІ ВИКЛИКИ ДЛЯ БІЗНЕСУ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Сьогодні актуальність проблеми захисту від кіберризиків не викликає ніяких сумнівів. Щодня кожен з нас стикається з необхідністю використання інформаційних технологій: від соціальних мереж, розміщення інформації про свої персональні дані в інтернеті, до користування банкоматами, банківськими рахунками тощо.

У сучасних умовах агресії російської федерації проти України кібертероризм лише зростає. Так, протягом січня 2022 року українські державні органи та банки зазнали двох помітних атак. У ніч з 13 на 14 січня хакери зламали понад 70 державних сайтів. Кілька годин не працювали веб-ресурси Міноборони, МЗС, ДСНС, «Дії». Проте за даними Держспецзв'язку ні зміст сайтів, ні дані користувачів не постраждали. Через місяць, 15 лютого, DDoS-атаки зазнали сайти та додатки банків, сайти Міноборони та інших відомств. Користувачі ПриватБанку, Ощадбанку, Монобанку, А-Банку та Альфа-Банку скаржилися на труднощі з доступом до програм протягом кількох годин. Атака тривала близько доби, і за оцінками фахівців міністерства цифрової трансформації України її вартість складала мільйони доларів. «Витоку даних, спотворення чи руйнування елементів інфраструктури немає», – цитує «Економічна правда» заступника голови Держспецзв'язку Віктора Жору [1].

У традиційній війні зазвичай є чіткий початок і кінець: агресія, перехід військами кордону та укладення мирного договору. Віртуальна війна триває весь час, і атака починається задовго до того, як буде завдано реальної шкоди. Все це змушує задуматися про важливість передчасної підготовки бізнесу до кіберзагроз, адже вони можуть за кілька днів знищити накопичені роками досягнення компаній. Щоб убезпечити свій бізнес від цих кібератак варто взагалі знати, що це таке, які вони бувають і як від них можна боронитися.

Кібератака – навмисна спроба зламати ваші комп'ютерні системи чи мережі, використовуючи шкідливі програмні забезпечення для порушення цих систем.

В Україні вже з початку року відбулися наймасштабніші атаки кіберзлочинців як на державні структури, так і на бізнес: 13-14 січня, 15-16 лютого, в ніч з 23 лютого та протягом березня-квітня 2022 року. Держспецзв'язок підтверджує, що протягом лютого-березня на українські підприємства та організації було спрямовано близько 2800 кібератак, а також рекордну 271 DDoS-атаку на добу та 362 хакерські атаки за перші 1,5 місяці війни. Лише за місяць воєнного стану було майже втричі більше хакерських атак на українські державні установи та бізнес, ніж у 2021 році за аналогічний період. Як повідомляє Держспецзв'язок, більшість з них були невдалими і не зачепили важливу інформаційну інфраструктуру.

Найпопулярнішими сферами атаки є державна та місцева влада, сектор безпеки та оборони, комерційні організації різних сфер діяльності, фінансовий сектор, телекомунікаційна інфраструктура та розробники програмного забезпечення, ЗМІ та ресурси,

які збирають інформацію про російські військові злочини в Україні. Вони атакують за допомогою фішингових розсилок, розповсюдження шкідливих програм і DDoS-атак. Більше половини всіх атак за перші 1,5 місяці війни було здійснено з метою збору інформації або поширення шкідливого коду.

Нова реальність активної інформаційної війни 2021-2022 років змушує всі підприємства та організації, незалежно від масштабу та сфери діяльності, комерційної чи державної форми власності, вивчати можливості захисту, інвестувати в новітні технології «кіберзброї» та залучати кращих спеціалістів «кіберфронту» [2].

Зараз в найбільшому ступені атака загрожує державним установам, критично важливій інфраструктурі, великим підприємствам, а також середнім підприємствам, які надають послуги уряду та приватним компаніям. Як ні дивно, але зазвичай кібератаки починаються з людського фактора, коли працівники бізнесу недбало ставляться до безпеки своїх пристроїв. Росія та її проксі-хакерські групи знаходять вразливість, використовують її та створюють каскадний ефект. Він завдає шкоди низці бізнесів – від фінансового та банківського секторів, логістики та власників серверів до цілих індустрій і критичної інфраструктури в енергетичному секторі.

Враховуючи підвищену стурбованість кіберзагрозами, є сенс переглянути ключові набори контролів кібербезпеки, які можуть допомогти знизити імовірність успішності атак – зокрема тих, які допомагають захиститися від загроз від держави-агресора або організованих угруповань, які активізували свою діяльність під час війни.

Для цьому достатніми є інвестиції у найпростіші способи захисту. Найпопулярнішими методами кібератак російських військових хакерів є: фішингові розсилання, внаслідок яких вони можуть отримати облікові дані для доступу до інформаційних систем; розсилання шкідливого програмного забезпечення, яке спрямоване на викрадення даних або знищення інфраструктури; використання відомих вразливостей.

Убезпечитись або мінімізувати ризики цих кібератак можна завдяки дотриманню правил кібергігієни, відповідальному ставленню до політики використання паролів, вчасному оновленню програмного забезпечення. Слід вивчати слабкі місця кіберзахисту компанії та укріплювати їх. Хакери постійно здійснюють розвідувальні операції в Україні, знаходять найслабші місця у захисті компаній та атакують через них. Не існує на 100% захищених систем. Проте що менше коштуватиме хакерам злом корпоративної системи, то вищою буде їхня мотивація.

Загарбники здійснюють кібератаки не лише на урядові структури - жертвами зламів і викрадення даних стають і пересічні громадяни. Забезпечте безпеку для кожного працівника Хакери можуть атакувати компанію чи установу і через співробітників, викравши їхні дані. В особливій небезпеці — військові та державні діячі. Фізична безпека користувачів критичної інформаційної інфраструктури така ж важлива, як і захист їхніх облікових записів. Російські хакери можуть використовувати облікові дані користувачів, які перебувають на тимчасово окупованих територіях. Компанії мають усвідомлювати, що фізична безпека їхніх працівників – це також інвестиція в їхній кіберзахист [3].

Отже, кіберризики сьогодні виходять далеко за межі крадіжки і шахрайства. Складність кіберризиків в Україні, на жаль, у подальшому буде тільки зростати. Більше підключених пристроїв, більше джерел даних, більше автоматизації процесів, сторонні стосунки створюють нові можливості для кібератак та інцидентів. Бізнесові організацій сьогодні повинні вкладати кошти в обґрунтовані заходи контролю безпеки для захисту своїх найважливіших активів від кібер-ризиків, що також дуже важливо з точки зору економічної складової нашої Перемоги.

Список використаних джерел

1. Кібератаки на Україні. Чи можливо в 2022 році залишити країну без світла, інтернету і зв’язку. – URL : https://forbes.ua/innovations/sim-rokiv-tomu-vpershe-v-sviti-khakeri-

znestrumili-tsiliy-region-tse-bulo-v-ukraini-chi-mozhlivo-v-2022-rotsi-zalishiti-krainu-bez-svitla-internetu-i-zvyazku-17022022-3714

2. Кіберзахист компанії в умовах війни: перемагають сучасні технології. – URL : https://hub.kyivstar.ua/news/kiberzahyst-kompaniyi-v-umovah-vijny-peremagayut-suchasni-tehnologiyi/

3. Як приватним компаніям посилити кіберзахист від рф. – URL : https://yur-gazeta.com/golovna/yak-privatnim-kompaniyam-posiliti-kiberzahist-vid-rf.html

4. Як приватним компаніям посилити кіберзахист від рф – URL : https://www.golovbukh.ua/news/29895-yak-privatnim-kompanyam-posiliti-kberzahist-vd-rf

УДК 334.722:355.271(477)

Кулакова С.Ю., к.е.н., доцент; Миколаєнко М. Ф., магістрант
Національний університет «Полтавська Політехніка Імені Юрія Кондратюка»
(м. Полтава, Україна)

ЗНАЧЕННЯ СОЦІАЛЬНОГО ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

На сьогоднішній день українське суспільство перебуває на шляху випробувань воєнного часу, наслідком якого стають суттєві критичні зміни в економічному, соціальному та політичному напрямках. При цьому важливі питання, що вимагають необхідних рішень та ресурсів зростають лише в геометричній прогресії у порівнянні з обмеженим потенціалом їх вирішення. Одним із найпроблемніших стає соціальний сектор, який лише збільшується за рахунок безробіття та вразливих груп населення.

Нинішня криза стала масштабним потрясінням, українське суспільство зіткнулося із безпрецедентною ситуацією. Турбулентність зовнішнього середовища, що спричинена пандемією COVID-19, ще більше підвищилась через введення воєнного стану та бойові дії на значній території України. Ці події викликали стрімке зростання безробіття, збільшення чисельності вразливих категорій населення та послаблення їх соціального захисту.

Так, за даними досліджень соціологічної групи «Рейтинг», станом на початок квітня 2022 року близько половини (53%) українців, що втратили роботу через війну, 22% продовжують працювати у звичному режимі, 21% – частково або віддалено і лише 2% – змогли знайти собі нову роботу. Найбільша кількість людей, що втратили роботу – це звісно мешканці східних областей Україні [1]. Найбільше складнощів відчувають ті, хто вимушено змінили місце проживання, особливо мешканці східних областей. Отже, можливість якнайшвидше відновити роботу, запустити підприємства залишається вкрай важливим для відносної нормалізації життя українців під час війни [2].

Одним із дієвих інструментів вирішення проблем цього напрямку може бути діяльність соціальних підприємств. На відміну від традиційного, соціальне підприємництво створюється у тому числі для вирішення суспільних проблем. При всьому бажанні в сучасних умовах, обтяжених воєнним станом, держава не може вирішити всі соціальні проблеми. Так само традиційне підприємництво нечасто зацікавлене в їх подоланні. Проте сьогодні необхідна допомога більшості із тих українців, які наразі цього потребують, перебуваючи в складному як соціальному, так і економічному становищі.

Тому соціальне підприємництво в Україні має зайняти вільну нішу в економіці і суспільстві. Воно хоча б частково вирішує проблеми малих груп. Зокрема, допомагає у подоланні соціальної ізольованості, працевлаштовуючи людей з обмеженими фізичними і психічними можливостями, безробітних, представників груп ризику і знаходить шляхи для реформування державних соціальних послуг, знижує навантаження на місцеві бюджети у вирішенні суспільних проблем.