DOI: https://doi.org/10.32782/2524-0072/2022-44-21

УДК 338.245

КІБЕРБЕЗПЕКА БІЗНЕСУ ПІД ЧАС ВІЙНИ

BUSINESS CYBER SECURITY IN TIME OF WAR

Кузьменко Олена Юріївна
старший викладач,
Херсонська державна морська академія
ORCID: https://orcid.org/0000-0001-7542-7322

Маклюк Олег Володимирович
викладач,
Чернігівський інститут імені Героїв Крут
Приватного акціонерного товариства «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID: https://orcid.org/0000-0002-7429-692X

Чернишова Олена Олександрівна
магістр,
Euromonitor International
ORCID: https://orcid.org/0000-0001-9437-9100

Kuzmenko Olena
Kherson State Maritime Academy

Makliuk Oleh
Chernihiv Institute named after Heroes Krut Private Joint Stock Company
«Higher Educational Institution
«Interregional Academy of Personnel Management»

Chernyshova Olena
Euromonitor International

У статті розкриті ключові аспекти кібербезпеки бізнесу в умовах війни. Визначено, що в останні роки використання інформаційних технологій в процесі гібридної війни обумовило виникнення принципово нових кіберзагроз вищого рівня, які спрямовано на національну та міжнародну безпеку. Виявлено, що спектр сучасних кібератак є досить різнорідним. Розглянуто ключові види кіберзагроз, які поділяються на зовнішні, цільові та внутрішні кіберзагрози. Розглянуто виклики для України у сфері кібербезпеки. Встановлено, що нова ера кібербезпеки потребує цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Виявлено, що слабкою ланкою у кібербезпеці підприємства можуть бути партнери та постачальники. Визначено превентивні заходи щодо кіберзахисту бізнесу. З'ясовано, що аудит кібербезпеки приватного бізнесу має проводитись незалежними аудиторами, а звіти – надаватися галузевим регуляторам.

Ключові слова: кібербезпека, кіберзахист, кібеззагроза, кібератака, бізнес, підприємство.

The article reveals the key aspects of business cyber security in wartime. It was determined that in recent years, the use of information technologies in the process of hybrid warfare caused the emergence of fundamentally new cyber threats of a higher level, which are aimed at national and international security. It was found that the spectrum of modern cyberattacks is quite diverse. The key types of cyber threats are considered, which are divided into external, targeted and internal cyber threats. Challenges for Ukraine in the field of cyber security are considered. It was established that the new era of cyber security requires completely new approaches to the management of the enterprise and its resources, in particular information. It was found that partners and suppliers can be the weak link in the company's cyber security. It has been proven that regardless of the causes of their occurrence, cyber incidents in one way or another pose a threat to the continuous activity and sustainable development of any enterprise. It was determined that the main tool for overcoming cyber attacks is the cyber protection system based on existing organizational and technological capabilities, financial and human resources, as well as the regulatory and legal basis. The system administrator is most often responsible for building the specified system at the local level.

At large enterprises, the construction of a complex to counter cyber threats is already a management problem, for the solution of which it is necessary to involve specialized specialists. Regardless of the specific tools that are planned to be used, security management is carried out according to the following principles: localization of the human factor; understanding critical places and sources of danger; risk monitoring; the possibility of prompt response. Preventive measures for business cyber protection are defined. It was found that private business cyber security audits should be conducted by independent auditors, and reports should be provided to industry regulators. It has been proven that business cyber security is a continuous and extremely relevant process in modern Ukrainian realities. It is a process, since the enemy is constantly working on improving attacks, which means that we should work on improving defense. This task remains strategically important for both public institutions and private businesses.

Keywords: cyber security, cyber defense, cyber attack, business, enterprise.

Постановка проблеми. Український бізнес перебував під загрозою кібератак від початку незалежності країни, а з початком повномасштабного вторгнення кібератаки набули значних масштабів. У таких умовах кожен представник бізнесу мусить оцінювати вразливість своєї діяльності до інцидентів кібербезпеки й технологічних збоїв. Ці загрози можуть виникати внаслідок атак на системи та інфраструктуру, а можуть бути й наслідками воєнних дій.

Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові підприємства, мають бути у режимі підвищеної готовності, оскільки саме ці сфери діяльності, якими займаються зазначені вище представники бізнесу, часто вважаються пріоритетними цілями кібератак у період війни. Бізнес має бути готовий протидіяти цим викликам – підприємства повинні оцінити готовність до кіберінцидентів і здатність відновити діяльність. Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету повинна здійснюватись шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Аналіз останніх досліджень і публікацій. Проблематику кібербезпеки бізнесу, зокрема в умовах війни, вивчали та продовжують вивчати Ю. Білявська, В. Вишківський, А. Кириленко, О. Криворучко, А. Пампуха, Я. Шестак та інші.

Однак, виходячи із важливості досліджень, проведених науковцями, необхідно зазначити, що не повністю проведені дослідження у напрямку розкриття особливостей кібербезпеки бізнесу в умовах воєнного стану.

Постановка завдання. Мета наукової статті полягає у розкритті ключових аспектів кібербезпеки бізнесу в умовах війни.

Виклад основного матеріалу дослідження. Кібербезпека здатна не лише реагувати на інциденти, але й запобігати атакам до початку їх виникнення. З метою покращення ефективності діяльності підприємства менеджери з кібербезпеки мають бути сфокусовані на технологіях, а також на тісній співпраці з бізнес-командами. Результатом такої взаємодії повинна бути готовність до боротьби з кіберзловмисниками на рівних, даючи відсіч і відбиваючи атаки з небаченою раніше результативністю. Керівники підприємств дедалі частіше звертаються до фахівців з інформаційної безпеки за допомогою у питаннях підвищення стійкості інформаційної системи та створення цінності захисту для бізнесу [1].

Проте в останні роки використання інформаційних технологій в процесі гібридної війни обумовило виникнення принципово нових кіберзагроз вищого рівня, які спрямовано на національну та міжнародну безпеку. Зокрема, зростає кількість та потужність кібератак, вмотивованих геополітичними інтересами окремих держав, груп та осіб. І при їхньому здійсненні вже не враховуються такі поняття як фінансова ефективність чи рентабельність кібератаки.

Проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кіберсфері, випереджаючому реагуванні на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадженню ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб

стримування військових конфліктів та загроз у кіберпросторі [2].

Кіберфахівці Служби безпеки України з початку повномасштабного вторгнення нейтралізували майже 3500 кібератак на електронні системи центральних органів влади та об'єктів критичної інфраструктури України. З них 1650 кіберзагроз виявлено в режимі «реального часу» за допомогою системи управління подіями інформаційної безпеки, що створена на базі СБУ. Встановлено, що переважна більшість російських атак мали на меті або знищити цифрові сервіси, або дестабілізувати роботу стратегічно важливих підприємств енергетичної та транспортної сфер діяльності. До організації і проведення таких диверсій причетні російські спецслужби та підконтрольні їм хакерські угруповання [3].

Спектр сучасних кібератак є досить різнорідним, тож доцільно їх класифікувати за такими базовими ознаками, як [4]: інструментальний засіб, що використовується при проведенні; специфіка реалізації; міра складності; умова ініціалізації; дистанційність; процес автоматизації; зовнішній прояв; спрямованість кінцевого результату та специфіка порушення базових характеристик системи інформаційної безпеки.

До основних видів кіберзагроз належать [5]:

1. Зовнішні загрози (Сюди включають DDoS і DoS атаки, а також експлуатація зловмисниками зовнішніх вразливостей систем підприємства. Для можливого захисту доцільно проаналізувати власну систему безпеки, виявити слабкі місця та усунути їх).

2. Цільові загрози (Основним вразливим елементом рівня захисту все ще залишається людина і цільовий вплив на неї в будь-якому куточку мережі інтернет через методи соціальної інженерії, включаючи найпоширеніші фішингові розсилки зі шкідливими файлами або посиланнями. Натискаючи на такі вкладення, можна заразити ПК. Це призводить до проникнення в мережу організації вірусів, «троянів», програм-шифрувальників / вимагачів та іншого шкідливого програмного забезпечення (ПЗ). Для захисту потрібно реалізувати як мінімум базовий набір засобів захисту – мова йде про мережевий екран, антивіруси, системи захисту WEB і MAIL, і паралельно – вести пропаганду комп'ютерної грамотності, навчати основним правилам «цифрової гігієни»).

3. Внутрішні загрози (До цієї групи слід віднести не лише системний, але і людський фактор: інсайдери, витік інформації або ігнорування правил поводження з чутливими даними. Захисту від інсайдерів та витоку інформації сприяє система моніторингу та контролю обігу даних на підприємстві та за його межами (Data Loss Prevention), спостереження за підозрілою активністю користувачів (User Activity Monitoring), а також системи класифікації даних (Data Classification) відповідно до рівня її конфіденційності та важливості для підприємства. Також важливо дотримуватись балансу між контролем і зручністю використанням ресурсів для співробітників).

В умовах сьогодення викликами для України у сфері кібербезпеки є [6]:

1) активне використання кіберзасобів у міжнародній конкуренції;

2) конкурентний характер розвитку інструментів кібербезпеки в контексті інформаційно-комунікаційних технологій, що швидко розвивається та змінюється, особливо хмарних і квантових обчислень, мереж 5G, великих даних, Інтернету речей, штучного інтелекту тощо;

3) мілітаризація кіберпростору та розробка кіберзброї для здійснення таємних кібератак у кіберпросторі для підтримки військових дій та діяльності знищення інформації;

4) вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинило швидку зміну та організацію значної частини суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

5) впровадження нових технологій, цифрових сервісів та електронних механізмів взаємодії між громадянами та державами, які здійснюються поетапно без належної оцінки ризиків з точки зору заходів кібербезпеки.

Своєю чергою, загрозами кібербезпеці України слід відзначити [6]:

1. Гібридну агресію російського агресора проти України в кіберпросторі. Держава-загарбник постійно розширює свій арсенал агресивної кіберзброї, яка може мати незворотні та руйнівні наслідки. Кібератаки противника спрямовані в першу чергу на інформаційно-комунікаційні системи державних органів України та критичні інформаційні інфраструктури з метою їх виведення з ладу (кібердиверсії), прихованого доступу та контролю, ведення інформаційно-підривної діяльності. Кібератаки також активно використовуються в країні-агресорі як елемент спеціальних розвідувальних операцій, спрямованих на маніпулювання населенням, зрив

виборчого процесу та дискредитацію української держави.

2. Кіберзлочинців, які завдають шкоди інформаційним ресурсам, суспільним процесам та окремим громадянам, знижують довіру суспільства до інформаційних технологій і завдають значних матеріальних збитків. Кіберпростір використовується для вчинення злочинів проти основ національної безпеки України, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного поводження зі зброєю, бойовими припасами або вибуховими речовинами, незаконного обігу наркотичних засобів і психоактивних речовин.

3. Кібератаки, організовані та спонсоровані урядами інших країн у зв'язку з крадіжкою конфіденційної інформації в політичних, економічних або військових цілях (кібершпигунство) та проведенням інформаційної та підривної діяльності. Природу цих кібератак важко запобігти, виявити та нейтралізувати через їх тривалість, складність і прихований характер.

4. Використання кіберпростору терористичними організаціями для здійснення кібертерористичних актів, фінансової допомоги та іншого сприяння терористичній діяльності.

Нова ера кібербезпеки потребує цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, наскільки гнучко організовані бізнес-процеси на підприємстві, а також як імплементуються нові моделі та методи роботи. У процесі аналізу стану та тенденцій цифрових технологій як нової ери кібербезпеки сформовано ключові напрями захисту підприємства від кіберзагроз. Щодня набуває актуальності зміна стереотипів у суспільстві стосовно того, що особисті дані нікому не цікаві, тому доречно провести навчання фахівців щодо користування захищеними протоколами передачі інформації, застосування захищених інформаційних систем для роботи.

Забезпечення кіберзахисту бізнесу можливе за рахунок залучення міжнародних партнерів. Так це дозволить забезпечити:

1) захист від кіберзагроз шляхом покращення здатності державних установ, підприємств і громадян захищати себе та реагувати на кіберзагрози;

2) здатність до ефективного реагування, оперативного виявлення та розслідування недружньої поведінки в кіберпросторі, створення ефективних систем превентивних дій для запобігання такій поведінці та проведення наступальних операцій у кіберпросторі;

3) людські ресурси та розвиток інноваційних ринків кібербезпеки, які сприятимуть створенню національних розробок на рівні кращих світових практик для забезпечення спроможності реагувати на майбутні кіберзагрози.

Слабкою ланкою у кібербезпеці підприємства можуть бути партнери та постачальники. Можна скільки завгодно посилювати захист IT-систем, але через атаку хакери можуть отримати доступ до даних.

Головна загроза в тому, що підприємства налагоджують потужний кіберзахист своїх інформаційних систем, але водночас їм важко контролювати всіх своїх партнерів та підрядників, яким дають доступ до своїх даних. Ці партнери та підрядники можуть мати нижчий рівень кіберграмотності серед співробітників, слабші рішення з кібербезпеки тощо. Саме цими вразливостями хакери й користуються, атакуючи компанії-підрядники та отримуючи доступ до потрібних їм інформаційних систем.

Слід зауважити, що підприємства, які є ціллю для хакерів, атакують переважно через підрядників у випадках [7]:

1) де цільове підприємство надійно захищене від зовнішніх атак і втручання напряму реалізувати неможливо;

2) коли підрядне підприємство має нижчий рівень розвитку кібербезпеки, ніж цільове підприємство;

3) коли цільове підприємство має підрядників із легітимними доступами до своїх систем.

Наразі кожному представнику бізнесу в Україні важливо об'єктивно та критично оцінювати власний ступінь захищеності і бути готовим до запобігання існуючим та потенційним загрозам кібербезпеки.

Тут слід відзначити такі превентивні заходи щодо кіберзахисту бізнесу як [8]:

1) оцінювання ризику та вразливості:

аналізування потенційних ризиків кібербезпеки для кращого розуміння потенційних бізнес-загроз;

– аналізування мережевої інфраструктури підприємства та надання методів для виявлення та запобігання кіберінцидентам (наприклад, впровадження систем контролю доступу, зберігання даних/систем у захищеній «хмарі», використання лише поточних облікових записів, оновлення звичайного програмного забезпечення, створення резервних копій конфіденційної інформації компанії тощо);

2) розроблення та впровадження плану реагування на кібератаки:

– створення або оновлення планів реагування для своєчасного відновлення підприємства, бізнес-процесів, IT-систем і даних у разі кібератаки;

– створення групи експертів, відповідальних за реалізацію плану реагування та ліквідацію наслідків можливих кібератак;

3) сприяння безпечній співпраці:

– регулярна перевірка всіх доступів до ресурсів підприємства, наданих партнерам і постачальникам;

– необхідна професійна попередня спільна перевірка партнерів і постачальників щодо кібербезпеки, включаючи перевірку наявності планів реагування на кібератаки та планів безпечності бізнесу;

4) обізнаність співробітників:

– слід переконатися, що співробітники служби кібербезпеки розвивають необхідні знання, навички та компетенцію для своєчасного виявлення ознак атак, інформування та запобігання потенційним кіберзагрозам;

– проведення обов'язкового регулярного навчання для співробітників щодо того, як реагувати на несподівані або кризові ситуації, пов'язані з кібербезпекою;

5) постійне аналізування і систематичні діяння щодо мінливості середовища:

– моніторинг поточних тенденцій у світі кібербезпеки, щоб передбачити конкретні сценарії та зменшити негативний вплив кіберінцидентів, якщо вони виникнуть;

– регулярна діагностика загрози та вразливості кібербезпеки та постійно вдосконалення підходу до забезпечення конфіденційності, цілісності та доступності інформації.

Незалежно від причин виникнення, кіберінциденти так чи інакше становлять загрозу для безперервної діяльності і сталого розвитку будь-якого підприємства.

Основним інструментом при цьому виступає система кіберзахисту на основі наявних організаційних та технологічних можливостей, фінансових та людських ресурсів, а також нормативно-правового базису. Відповідальним за побудову вказаної системи на локальному рівні найчастіше виступає системний адміністратор. На великих підприємствах побудова комплексу протидії кіберзагрозам є вже управлінською проблемою, для вирішення якої потрібно залучати профільних фахівців. Незалежно від конкретних інструментів, які планується використовувати, менеджмент безпеки здійснюється згідно з наступними принципами: локалізація людського фактору; розуміння критичних місць та джерел небезпеки; моніторинг ризиків; можливість оперативного реагування.

Якщо підприємство все ж таки зазнало кібератаки, то ключовими кроками є [8]:

1) своєчасно повідомити всі потенційно постраждалі сторони;

2) не зволікати та не замовчувати інцидент, який відбувся, а за першої можливості повідомити всі сторони, які потенційно могли постраждати – співробітників, клієнтів, постачальників та інших учасників бізнесу;

3) провести ґрунтовний аналіз кіберінциденту, який має включати причини та сценарії виникнення, а також канали/шляхи здійснення, вивчення даних;

4) оцінити наслідки і втрати;

5) після отримання результатів аналізу, оцінити потенційний масштаб інциденту та визначити загальні збитки (вже понесені і потенційно очікувані);

6) відновити пошкоджені IT-системи та скомпрометовані дані;

7) впровадити додаткові превентивні заходи;

8) після ліквідації наслідків кіберінциденту переглянути існуючі системи контролю, з метою виявлення потенційних прогалин та пошуку можливостей для покращення поточного плану реагування на подібні інциденти, а також подальшого посилення інформаційної безпеки підприємства.

Аудит кібербезпеки приватного бізнесу має проводитись незалежними аудиторами (або самими власниками критичних об'єктів), а звіти – надаватися галузевим регуляторам.

Висновки з проведеного дослідження. Таким чином, кібербезпека бізнесу є безперервним і вкрай актуальним процесом в сучасних українських реаліях. Проведені дослідження засвідчили, що український бізнес за час повномасштабної війни стикнувся зі значними кібератаками, число яких суттєво зросло у порівнянні із довоєнний періодом. Визначено, що для кібербезпеки бізнесу доцільно впроваджувати відповідні заходи, особливе значення серед яких належить налагодженню потужного кіберзахисту інформаційних систем. Варто також взяти до уваги позицію, що ворог постійно працює над удосконаленням кібератак, з огляду на те українському бізнесу слід працювати на удосконаленням кіберзахисту. Це завдання залишається стратегічно важливим як для державних установ, так і для приватного бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки.* 2022. № 3. С. 47–59.

2. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально-наукового інститут захисту інформації. Київ, 2022. С. 31–33.

3. Майже половину кібератак СБУ виявляє у режимі «реального часу». URL: https://www.ukrinform.ua/rubric-technology/3584942-majze-polovinu-kiberatak-sbu-viavlae-u-rezimi-realnogo-casu.html.

4. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

5. Кібербезпека: як українському бізнесу захиститися від атак російських хакерів під час війни. Поради від IT-фахівців. URL: https://uaspectr.com/2022/07/27/yak-ukrayinskomu-biznesu-zahystytysya-vid-atak-hakeriv.

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.

7. Кібератаки можуть прийти через постачальників. Як захиститися? URL: https://delo.ua/telecom/kiberataki-mozut-priiti-cerez-postacalnikiv-yak-zaxistitisya-404662.

8. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.

REFERENCES:

1. Biljavsjka, Ju., Shestak, Ja. (2022). Kiberbezpeka ta kiberghighijena: nova era cyfrovykh tekhnologhij [Cyber security and cyber hygiene: a new era of digital technologies]. *Tovary i rynky – Goods and markets*, 3, 47–59. (in Ukrainian)

2. Vyshnivsjkyj, V. V., Pampukha, A. I. (2002). Kiberbezpeka v Ukrajini [Cybersecurity in Ukraine]. Cyfrova transformacija kiberbezpeky: naukovo-praktychna internet-konferencija – Digital transformation of cyber security: scientific and practical internet conference, 20 kvitnja 2022, Derzhavnyj universytet telekomunikacij Navchaljno-naukovogho instytut zakhystu informaciji, m. Kyjiv, 31–33. (in Ukrainian)

3. Majzhe polovynu kiberatak SBU vyjavljaje u rezhymi «realjnogho chasu» [Almost half of cyberattacks are detected by the SBU in "real time" mode]. Available at: https://www.ukrinform.ua/rubric-technology/3584942-majze-polovinu-kiberatak-sbu-viavlae-u-rezimi-realnogo-casu.html. (in Ukrainian)

4. Eskalacija kiberzaghroz nacionaljnym interesam Ukrajiny ta pravovi aspekty kiberzakhystu: monoghrafija [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection: monograph] / O. D. Dovghanj, I. M. Doronin; NAPrN Ukrajiny, NDIIP. Kyiv: Vydavnychyj dim «ArtEk». 2017. 107 p. (in Ukrainian)

5. Kiberbezpeka: jak ukrajinsjkomu biznesu zakhystytysja vid atak rosijsjkykh khakeriv pid chas vijny. Porady vid IT-fakhivciv [Cyber security: how Ukrainian businesses can protect themselves from attacks by Russian hackers during the war. Advice from IT experts]. Available at: https://uaspectr.com/2022/07/27/yak-ukrayinskomu-biznesu-zahystytysya-vid-atak-hakeriv. (in Ukrainian)

6. Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 14 travnja 2021 roku «Pro Strateghiju kiberbezpeky Ukrajiny»: Ukaz Prezydenta Ukrajiny; Strateghija vid 26.08.2021 № 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine; Strategy dated August 26, 2021 № 447/2021]. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#n12. (in Ukrainian)

7. Kiberataky mozhutj pryjty cherez postachaljnykiv. Jak zakhystytysja? [Cyberattacks can come through suppliers. How to protect yourself?]. Available at: https://delo.ua/telecom/kiberataki-mozut-priiti-cerez-postacalnikiv-yak-zaxistitisya-404662. (in Ukrainian)

8. Kiberbezpeka biznesu v umovakh nestabiljnosti [Cybersecurity of business in conditions of instability]. Available at: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html. (in Ukrainian)