DOI: https://doi.org/10.32782/2524-0072/2023-58-44

УДК 338.656

КОРПОРАТИВНА БЕЗПЕКА НА УКРАЇНСЬКИХ ПІДПРИЄМСТВАХ В УМОВАХ ВІЙНИ

CORPORATE SECURITY AT UKRAINIAN ENTERPRISES IN TIME OF WAR

Давиденко Євген Анатолійович
здобувач PhD кафедри,
ПВНЗ «Європейський університет»
ORCID: https://orcid.org/0009-0007-7720-3913

Davydenko Yevhen
European University

У статті розкриті ключові аспекти корпоративної безпеки на українських підприємствах в умовах війни. Сформульовано та удосконалено класифікації зовнішніх та внутрішніх загроз. Особливу увагу відведено зовнішнім загрозам комплексного характеру. Вивчено проблеми впливу кібератак на корпоративну безпеку на українських підприємствах. Кібератаки розглядаються як ключовий елемент зовнішньої загрози в умовах війни з позицій забезпечення внутрішньої фінансової та економічної стабільності, а також національної безпеки в цілому. З початку військових дій на території України інтенсивність та складність кібератак на корпоративні системи та мережі суттєво зросла. Очевидно, що несанкціоновані атаки спрямовані на викрадення конфіденційної інформації, розкрадання фінансових ресурсів або припинення функціонування підприємств. Запропоновано методи попередження кібератак з метою уникнення фінансових втрат чи блокування ресурсів. Тому проблеми, що обговорюються в даній роботі є актуальними.

Ключові слова: корпоративна безпека, кібербезпека, кіберзахист, кібеззагроза, кібератака, підприємство.

The article reveals the key aspects of corporate security at Ukrainian enterprises in the context of war. Classifications of external and internal threats are formulated and improved. Particular attention is paid to external threats of a complex nature. The problems of the impact of cyberattacks on corporate security at Ukrainian enterprises are studied. Cyberattacks are considered a key element of the external threat in the context of war from the standpoint of ensuring internal financial and economic stability, as well as national security in general. Since the beginning of hostilities in Ukraine, the intensity and complexity of cyber attacks on corporate systems and networks have increased significantly. Unauthorized attacks are aimed at stealing confidential information, embezzling financial resources, or disrupting the normal functioning of enterprises. Methods of preventing and avoiding financial losses or blocking of resources as a result of cyber attacks are proposed. Therefore, the issues discussed in this paper are relevant. In particular, the article examines the impact of cyberattacks on corporate security at Ukrainian enterprises, which are considered a key element of the external threat in the context of war from the standpoint of ensuring domestic financial and economic stability, as well as national security in general. The research has led to conclusions about the significant impact of cyberattacks on Ukrainian businesses and state-owned enterprises during the full-scale war, which were subjected to massive cyberattacks, and their number has increased significantly compared to the pre-war period. According to statistical data, along with the use of various vulnerabilities, one of the most popular methods of unauthorized penetration is phishing, which can be either a separate technology or a component of a larger-scale attack to get into a particular information and communication system. It is found that in Ukraine, not all administrators of such systems still update the software promptly and use licensed software. Several cybersecurity measures for government agencies and private businesses are proposed since this task remains strategically important. It is determined that cybersecurity is trust within the framework of interaction between the State and business, and Ukraine's cyber resilience significantly depends on the business's resilience to threats. Therefore, it is necessary to protect public authorities by protecting businesses from cyberattacks and vice versa.

Keywords: corporate security, cyber security, cyber defense, cyber threat, cyber attack, enterprise.

Постановка проблеми. Корпоративна безпека на українських підприємствах відіграє важливу роль у забезпеченні стійкості та успішності бізнесу в умовах сучасного підприємницького середовища. Вона охоплює широкий спектр заходів, спрямованих на запобігання ризикам і загрозам, які можуть виникнути як ззовні, так і зсередини компанії.

В умовах повномасштабного вторгнення для українського бізнесу значно зросли зовнішні загрози комплексного характеру, які включають різноманітні аспекти. Зокрема, від початку війни кібератаки на корпоративні мережі збільшились в рази. А зростання їх інтенсивності та складності на корпоративні системи та мережі, очевидно, спрямовані на викрадення конфіденційної інформації, розкрадання фінансових ресурсів або припинення нормального функціонування підприємств. Тому, в умовах війни підприємства різних форм власності (бізнес чи державне підприємство) повинні оцінювати вразливість своєї діяльності до таких інцидентів як шпигунство та кіберрозвідка, адже атаки можуть бути спрямовані на отримання конфіденційної інформації, яка, в свою чергу, може бути використана для стратегічного шпигунства або економічної шкоди. Щоб попередити та уникнути фінансових втрат чи блокування ресурсів загалом через кібератаки, а також блокування доступу до банківських рахунків та інших фінансових інструментів, кібербезпека, що є невід'ємною частиною корпоративної безпеки на українських підприємствах, має бути пріоритетним напрямком дослідження та розвитку з метою якнайшвидшого реагування та запобігання інцидентам з нею пов'язаних. Бізнес та держава мають бути готовими протидіяти загрозам, оскільки останній рік війни показав, що ризики впливу на критичну інфраструктуру, таку як енергетика, транспорт, комунікації, може призвести до перебоїв в наданні послуг та економічних збитків. Втручання в логістичні та ланцюги постачання несе не менші загрози. Треба відмітити, що кібератаки несуть надзвичайно високі ризики витоку конфіденційної інформації про клієнтів та порушення їх приватності, що може призвести до втрати довіри та репутаційних проблем підприємства, а в масштабах держави – ставить під загрозу національну систему безпеки держави України вцілому. Слід відмітити і соціально-психологічні впливи на стан персоналу та клієнтів підприємства під впливом кібератак, що може призвести до стресу та негативного відношення до підприємства. Фізична безпека, безпека персоналу є важливими складовими загальної безпеки підприємства в умовах війни. Вирішення цих проблем вимагає розробки та впровадження комплексних стратегій кібербезпеки, враховуючи конкретні потреби та умови кожного підприємства. Також важливо співпрацювати з відповідними урядовими та IT-організаціями для обміну інформацією та взаємодії у сфері кіберзахисту.

Аналіз останніх досліджень і публікацій. Проблеми корпоративної безпеки на підприємствах України досліджувалися багатьма науковцями [1, с. 93–96], [2, с. 165–170], [3, с. 141–146], [4, с. 161–167]. Достатньо ґрунтовно досліджені саме внутрішні загрози для підприємств [5, с. 159–169]. Проте, в умовах повномасштабного вторгнення доцільно акцентувати увагу науковців на зовнішніх загрозах, що безумовно впливають і на внутрішні проблеми корпоративної безпеки українських підприємств. Прийшов час активно використовувати теоретико-методологічну базу та втілювати на практиці раніше викладені концепції [1, с. 93–96], [2, с. 165–170], [3, с. 141–146], [4, с. 161–167], [6, с. 54–61]. З кожним днем війни стає зрозуміло, що ключовим аспектом зовнішніх загроз корпоративної безпеки підприємств в Україні є кібербезпека. Встановлено, що Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак [7]. Тому, попри проведені дослідження В. Засанського, О. Тимошенко, О. Куриліної, Ю. Білявською, В. Вишківським, А. Кириленко, О. Криворучко, А. Пампуха, Я. Шестаком в області кіберзахисту підприємств, і, зокрема, в умовах війни, дана проблема все ж потребує більш детального вивчення та встановлення закономірностей згаданих загроз з метою їх попередження та блокування, бо це питання захисту інтересів не лише на рівні підприємства, а і на рівні держави.

Формулювання цілей статті (постановка завдання). Метою даної наукової статті є встановлення ключових аспектів корпоративної безпеки на українських підприємствах в умовах війни. Формування та удосконалення класифікації зовнішніх та внутрішніх загроз з акцентом на кібербезпеку та її інструментів для захисту промислових підприємств в умовах нинішніх реалій війни.

Виклад основного матеріалу дослідження. Корпоративна безпека на українських підприємствах відіграє важливу роль у забезпеченні стійкості та успішності бізнесу в умовах сучасного підприємницького середовища. Вона охоплює широкий спектр заходів, спрямованих на запобігання ризикам і загрозам, які можуть виникнути як ззовні, так і зсередини компанії. Деякі ключові аспекти корпоративної безпеки в українських підприємствах включають наступні складові: фізична, інформаційна і кадрова безпека, бізнес-контингент, юридична та фінансова безпека, навчання та освіта, співпраця з органами влади (схема 1).

Схема 1

Ключові аспекти корпоративної безпеки на українських підприємствах

Джерело: авторська розробка

Отже, забезпечення корпоративної безпеки вимагає комплексного підходу та взаємодії різних відділів підприємства. Також важливо постійно вдосконалювати заходи безпеки, враховуючи динамічні зміни бізнес-середовища та сучасні загрози. Для підприємств в Україні важливо ретельно аналізувати не лише внутрішні, а із особливою прискіпливістю віднестись до проблеми зовнішніх загроз, вживати відповідних заходів з кібербезпеки, ризик-менеджменту та стратегічного планування. Також важливо співпрацювати з урядовими та іншими зацікавленими сторонами для ефективного захисту інтересів та безпеки бізнесу.

Зовнішні загрози для корпоративної безпеки підприємств в Україні, які можуть впливати на дестабілізацію їх функціонування включають різноманітні аспекти. Нижче наведені найбільш значущі, на нашу думку, загрози.

1. *Кібератаки* – це спроба несанкціонованого доступу, впливу, знищення або маніпулювання комп'ютерними системами, мережами чи даними, з метою завдання шкоди або отримання несанкціонованого доступу до інформації. З цією метою кіберзлочинці можуть використовувати різні типи кібератак, що наведені в таблиці 1.

2. *Шпигунство* інтелектуальної власності полягає в тому, що зовнішні агенти можуть намагатися викрасти чи сприяти витоку конфіденційної інформації, технології чи інтелектуальної власності підприємства.

3. *Торгівля людьми* в сучасному світі, також може становити загрозу. Це може включати в себе примусову працю, яка може бути використана для незаконних цілей або для отримання конфіденційної інформації.

4. *Економічні чинники* такі як економічна нестабільність, валютні коливання та інші економічні фактори можуть також впливати на корпоративну безпеку підприємств.

5. *Політичні та геополітичні конфлікти* можуть призводити до змін у законодавстві, що, в свою чергу, може впливати на діяльність підприємства.

6. *Тероризм*. Терористичні акти можуть спричинити фізичні руйнування, а також впливати на психологічний клімат та безпеку персоналу.

7. *Порушення торговельних відносин* викликають зміни на міжнародному рівні і можуть мати вплив на експорт та імпорт товарів і послуг.

8. *Енергетична залежність* від імпортованої енергії може вносити нестабільність у функціонування підприємств у випадку геополітичних або енергетичних криз, що і спостерігається в період війни.

На нашу думку, для ефективного управління цими загрозами підприємства повинні вживати заходів з кібербезпеки, розвивати стратегії управління ризиками, встановлювати ефективні системи моніторингу та реагування, а також враховувати геополітичні та економічні фактори при розробці бізнес-планів. Тому наступним кроком нашого дослідження є деталізація такого елементу зовнішньої загрози корпоративній безпеці підприємства як кібератаки, що стало особливо

Таблиця 1

Типи кібератак

1. Створення програм, які можуть розповсюджуватися та реплікуватися самостійно.
2. Шахрайські спроби отримати конфіденційну інформацію (наприклад, паролі, номери кредитних карт) шляхом маскування як відомих або надійних джерел.
3. Зміна або видалення даних на комп'ютері чи мережі без належного дозволу.
4. DDoS атаки або намагання переповнити систему або мережу трафіком, забороняючи легітимним користувачам отримувати доступ.
5. Атаки на інтернет-протоколи та служби з метою завдання шкоди.
6. Спілкування по сторонніх каналах – захоплення системи або мережі та встановлення комунікації зі стороннім контролером для здійснення подальших атак.
7. Шпигунство – намагання несанкціонованого отримання конфіденційної інформації через інтернет.
8. Соціальна інженерія – використання елементів маніпулції людьми для отримання конфіденційної інформації.
9. Атаки на програмне забезпечення з метою використання вразливостей у програмному забезпеченні для отримання несанкціонованого доступу.
10. Спроби отримати доступ до системи шляхом підбору або зламу паролів.

Джерело: авторська розробка

актуальним в Україні з початком повномасштабного вторгнення.

Кібератаки як елемент зовнішньої загрози корпоративної безпеки підприємства

Кібератаки стали серйозним елементом зовнішньої загрози для корпоративної безпеки підприємств. Ці атаки можуть призвести до серйозних наслідків для бізнесу, включаючи втрату конфіденційної інформації, фінансових збитків, пошкодження репутації та призупинення роботи бізнес-процесів. Ось деякі ключові аспекти, які роблять кібератаки елементом зовнішньої загрози:

1. Витік інформації – кіберзлочинці можуть заволодіти конфіденційною інформацією, такою як особисті дані клієнтів, бізнес-секрети, патенти або фінансові дані.

2. Фінансові атаки – кіберзлочинці можуть викрадати гроші, використовуючи різні шахрайські схеми, включаючи фішинг, обманні платежі та інші види атак.

3. Загроза для бізнес-процесів – кібератаки можуть вплинути на нормальний хід бізнес-процесів, призводячи до призупинення роботи систем, обмеження доступу до важливих ресурсів або руйнування IT-інфраструктури.

4. Репутаційні ризики виникають у разі витоку конфіденційної інформації або успішного використання атак на корпоративні системи, внаслідок чого репутація компанії може значно постраждати, що може призвести до втрати довіри клієнтів і партнерів.

5. Використання атак для шпигунства - кіберзлочинці можуть використовувати атаки для шпигунства, зокрема для вивчення ділових планів, стратегій, інновацій та інших ключових аспектів діяльності підприємства.

6. Використання розподілених атак – атаки можуть бути розподілені та виконуватися з різних частин світу, зробивши їх важкими для виявлення та ліквідації.

7. Атаки на постачальників – кіберзлочинці можуть використовувати слабкі місця в IT-інфраструктурі постачальників для доступу до систем корпорації, що становить додатковий ризик.

Для захисту від кібератак підприємства повинні впроваджувати комплексні заходи безпеки, такі як регулярне оновлення програмного забезпечення, впровадження мережевих та системних заходів захисту, навчання персоналу щодо кібербезпеки та впровадження стратегій реагування на інциденти. Комплексні заходи включають в себе різноманітні технічні, організаційні та людські аспекти. Ми пропонуємо звернути увагу на деякі важливі, на нашу думку, і ключові елементи захисту від кібератак:

1. Антивірусне програмне забезпечення – встановлення та регулярне оновлення антивірусних програм для виявлення та усунення шкідливого програмного забезпечення.

2. Фаєрволи – встановлення фаєрволів для контролю трафіку мережі та блокування неправомірних підключень.

3. Оновлення програм та операційних систем, програм та інших програмних засобів для усунення вразливих місць.

4. Системи виявлення та запобігання вторгненням (IDS/IPS) – встановлення систем, які моніторять мережевий трафік та виявляють неправомірні або підозрілі активності.

5. Шифрування даних – використання шифрування для захисту конфіденційної інформації під час передачі та зберігання.

6. Резервне копіювання даних. Регулярне створення резервних копій важливої інформації та її зберігання в безпечному місці.

7. Ефективна політика паролів – застосування строгих правил стосовно паролів, включаючи їхню складність та регулярність зміни.

8. Співробітництво зі сторонніми постачальниками безпеки – використання послуг сторонніх фахівців для аудиту та оцінки рівня безпеки системи.

9. Освіта та навчання персоналу щодо безпечних практик роботи в мережі та виявлення підозрілої активності.

10. Моніторинг та інцидент-менеджмент – впровадження систем моніторингу для раннього виявлення можливих кібератак та розробка планів інцидент-менеджменту.

11. Фізична безпека – забезпечення фізичної безпеки обладнання та інфраструктури для запобігання неправомірному доступу.

12. Створення планів відновлення після інциденту – розробка та впровадження планів відновлення роботи після кібератаки для швидкого відновлення функціонування підприємства.

Ці заходи повинні взаємодіяти між собою для створення ефективної системи захисту від кіберзагроз. Регулярне оновлення та адаптація цих заходів є ключовими елементами для ефективного контролю над кібербезпекою підприємства. Комплексні заходи захисту від кібератак підприємств – це має бути *must have* захист від кібератак, що надважливо для забезпечення безпеки інформації та нормального функціонування підприємства.

Висновки. Розглянуто ключові аспекти корпоративної безпеки на українських під-

приємствах в умовах війни. Особливу увагу відведено зовнішнім загрозам. Зокрема, вивчено проблеми впливу кібератак на корпоративну безпеку на українських підприємствах, що розглядаються як ключовий елемент зовнішньої загрози в умовах війни з позицій забезпечення внутрішньої фінансової та економічної стабільності, а також національної безпеки в цілому. Проведені дослідження дали змогу зробити висновки про значний вплив кібератак на український бізнес та державні підприємства за час повномасштабної війни, які піддалися масованим кібератакам, а їх число суттєво зросло у порівнянні із довоєнним періодом. Встановлено, згідно зі статистичними даними, паралельно з використанням різних вразливостей одним із найпопулярніших способів несанкціонованого проникнення є фішинг, який може бути як окремою технологією, так і складовою більш масштабної атаки з метою потрапити до тієї чи іншої інформаційно-комунікаційної системи. Виявлено, що в Україні досі не всі адміністратори таких систем вчасно оновлюють програмне забезпечення і використовують ліцензійне програмне забезпечення. Запропоновано низку заходів кіберзахисту для державних установ та приватного бізнесу, оскільки це завдання залишається стратегічно важливим. Визначено, що кібербезпека – це довіра в межах взаємодії держави та бізнесу, а кіберстійкість України істотно залежить від стійкості бізнесу до загроз. Тому, потрібно захистити органи державної влади шляхом захисту бізнесу від кібератак і навпаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шира Т. Б. Корпоративна безпека підприємств в Україні: визначення ключових загроз. *Вчені записки Таврійського національного університету імені ВІ Вернадського. Серія: Економіка і управління.* 2018. Том 29 (68). № 6. С. 93–96.

2. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. *Науковий вісник Волинського держ. ун-ту ім. Лесі Українки.* 2005. № 1. С. 165–170.

3. Рудковський О. В. Формування функцій управління корпоративної безпеки. *Соціально-економічний розвиток регіонів в контексті міжнародної інтеграції*. 2013. № 12. 1. С. 141–146.

4. Франчук В.І. Теоретичні засади корпоративної безпеки. *Актуальні проблеми економіки*. 2009. № 7. С. 161–167.

5. Линник О. І., Артеменко Н. В. Стратегія економічної безпеки підприємства як фактор зменшення впливу зовнішніх та внутрішніх загроз. *Вісник Національного технічного університету ХПІ. Сер.: Технічний прогрес та ефективність виробництва.* 2013. № 67. С. 159–169.

6. Засанський, В. В., Куриліна О. В. Корупція як основа розповсюдження тіньової діяльності. *Науковий вісник Львівського державного університету внутрішніх справ (серія економічна)*. 2018. № 2. С. 54–61. URL: https://interfax.com.ua/news/interview/911979.html (дата звернення: 25.01.2024).

REFERENCES:

1. Shyra, T. B. (2018). Korporatyvna bezpeka pidpryyemstv v Ukrayini: vyznachennya klyuchovykh zahroz [Corporate Security of Enterprises in Ukraine: Identification of Key Threats]. *Vcheni zapysky Tavriys'koho natsional'noho universytetu imeni VI Vernads'koho. Seriya: Ekonomika i upravlinnya*, (29 (68), № 6), 93–96.

2. Kravchuk, P. Ya. (2005). Sutnist' ta peredumovy vynyknennya ponyattya korporatyvnoyi bezpeky pidpryyemstva [The Essence and Prerequisites of the Concept of Corporate Security of an Enterprise]. *Naukovyy visnyk Volyns'koho derzh. un-tu im. Lesi Ukrayinky*, (1), 165–170.

3. Rudkovs'kyy, O. V. (2013). Formuvannya funktsiy upravlinnya korporatyvnoyi bezpeky [Formation of corporate security management functions]. *Sotsial'no-ekonomichnyy rozvytok rehioniv v konteksti mizhnarodnoyi intehratsiyi,* (12), 1, 141–146.

4. Franchuk, V. I. (2009). Teoretychni zasady korporatyvnoyi bezpeky [Theoretical foundations of corporate security]. *Aktual'ni problemy ekonomiky,* (7), 161–167.

5. Lynnyk, O. I., & Artemenko, N. V. (2013). Stratehiya ekonomichnoyi bezpeky pidpryyemstva yak faktor zmenshennya vplyvu zovnishnikh ta vnutrishnikh zahroz [Enterprise economic security strategy as a factor in reducing the impact of external and internal threats]*. Visnyk Natsional'noho tekhnichnoho universytetu KHPI. Ser.: Tekhnichnyy prohres ta efektyvnist' vyrobnytstva*, (67), 159–169.

6. Zasans'kyy, V. V., & Kurylina, O. V. (2018). Koruptsiya yak osnova rozpovsyudzhennya tin'ovoyi diyal'nosti [Corruption as the basis of the spread of shadow activities]. Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav (seriya ekonomichna), (2), 54–61. URL: https://interfax.com.ua/news/interview/911979.html (accessed January 25, 2024).