УДК 004.056+658.7+65.007
DOI: 10.31733/2078-3566-2022-6-537-542

Олена ГАЛУШКО©
викладач
(*Придніпровська державна академія будівництва та архітектури, м. Дніпро, Україна)*

Тетяна СЕЛІВЬОРСТОВА©
кандидат технічних наук, доцент
(Український державний університет науки і технологій, м. Дніпро, Україна)

КІБЕРБЕЗПЕКА В УПРАВЛІННІ ЛАНЦЮГАМИ ПОСТАЧАНЬ (SCM)

Кібербезпека в управлінні ланцюгами постачань (SCM) стає все більш актуальною, оскільки сучасні компанії все більше використовують інформаційні технології та цифрові системи. А самі ланцюги постачань стають все більш розгалуженими та включають все більше учасників. З такою кількістю точок взаємодії та сторонніх постачальників і покупців важко відслідковувати, чи всі сторони дотримуються належних протоколів кібербезпеки.

Нозглянуто сутність управління ланцюгами постачань та проаналізовано роль кібербезпеки в системі управління. Зазначено, що в сучасних умовах кібербезпека стає елементом управління ланцюгами постачань. Проаналізовано основні види ризиків та кіберзагоз в ланцюгах постачань, зокрема питання безпеки сторонніх постачальників. Запропоновано заходи щодо усунення кіберризиків та підвищення кібербезпеки в управлінні ланцюгами постачань. Застосовуючи проактивний підхід і впроваджуючи потужні заходи кібербезпеки, компанії можуть зменшити ризик кібератак і забезпечити безпеку свого ланцюжка постачань.

Ключові слова: *ланцюги постачань, кібербезпека, інформаційні потоки, контрагенти, кіберзагрози.*

Постановка проблеми. Сучасні ланцюги постачань стають все більш складними і розгалуженими. Вони включають багато процесів: потоки доставки сировини, матеріалів та напівфабрикатів до місця виробництва, складську логістику в процесі виробництва, потоки розподілу готової продукції та її доставки споживачам. І якщо у XX сторіччі ризики ланцюгів постачань виникали переважно в сфері матеріальних та фінансових потоків, то у XXI сторіччі з переходом до цифрової економіки зросло значення і кількість кіберзагроз, тобто ризиків втручання в інформаційні потоки ланцюгів постачань та їх технічне забезпечення.

Під кібербезпекою (англ. Cyber Security) розуміють практику захисту комп'ютерів, серверів, мобільних пристроїв, мереж, критично важливих систем, даних і конфіденційної інформації від зловмисних цифрових атак. Тобто кібербезпека – це набір стратегій та рішень, які особа або організація використовують, щоб уникнути небезпеки та загроз у кіберпросторі. А захист від кіберзагроз (англ. Cyber Defense) є ключовим компонентом будь-якої стратегії кібербезпеки, при цьому рішення для кіберзахисту зосереджені на активних протидіях атакам.

Компанія IBM зазначає, що заходи кібербезпеки призначені для боротьби із загрозами мережевим системам і програмам, незалежно від того, чи походять ці загрози зсередини організації, чи ззовні. Вважають, що термін «кібербезпека» вперше виник у середині 1990-х років у США, коли питання захисту від кіберзагроз було розглянуто урядом [1]. Проведене у 2022 р. у Великій Британії опитування щодо кіберзагроз

© О. Галушко, 2022
ORCID iD: https://orcid.org/0000-0002-4578-5820
olena_galushko@ukr.net

© Т. Селівьорстова, 2022
ORCID iD: https://orcid.org/0000-0002-2470-6986
tatyanamikhaylovskaya@gmail.com

свідчить, що з 39 % британських компаній, які виявили кібератаку, більшість спіткалися зі спробами фішингу (83 %). З 39 % приблизно кожен п'ятий (21 %) визначив більш витончений тип атаки, такий як атака для відмови в обслуговуванні, зловмисне програмне забезпечення або програма-вимагач. Незважаючи на низьку поширеність, організації назвали програмне забезпечення-вимагач основною загрозою: 56 % компаній дотримуються політики не платити викуп [2].

У групі організацій, які повідомляють про кібератаки, 31 % підприємств і 26 % благодійних організацій вважають, що вони зазнавали атак принаймні раз на тиждень. Кожен п'ятий бізнес (20 %) і благодійна організація (19 %) стверджують, що відчули негативний результат як прямий наслідок кібератаки, тоді як третина підприємств (35%) і майже чотири з десяти благодійних організацій (38%) зазнали хоча б один негативний вплив [2].

Також в результаті опитування було визначено, що малі, середні та великі підприємства використовують аутсорсинг для IT рішень та кібербезпеки їх передають зовнішнім постачальникам у 58%, 55% і 60% випадках відповідно. Мотивацією для використання аутсорсингу є більший досвід, людські і технічні ресурси, а також високі стандарти кібербезпеки профільних компаній. Таким чином, лише 13% підприємств оцінили ризики, пов'язані з їхніми безпосередніми постачальниками, а організації заявили, що кібербезпека не була важливим фактором у процесі закупівель [2]. Отже з результатів опитування можна зробити висновок, що організації приділяють недостатньо уваги питанням кібербезпеки у ланцюгах постачань.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Питанням кібербезпеки та розбудови відповідних систем кіберзахисту присвячені роботи зарубіжних та вітчизняних вчених, зокрема: Дж. Ліпмана, А. Льюїса, К. Хартмана, В. Шарпа, Р. Олдрича, І. Діордіци, М. Шмітта, Д. Крамера, Б. Шнаєра, Р. Девара, В. Бурячка, Р. Грищука, Ю. Грицюка, О. Горбаня, О. Довганя, Д. Дубова, В. Ліпкана, А. Семенченко, В. Мохора, О. Корченка, В. Цуркана, В. Фурашева, В. Шеломенцева та ін. [1, 3-5]. Також питання кібербезпеки та кіберзахисту висвітлені в національних стратегіях кібербезпеки, рекомендаціях ITU, ENISA, NATO та ін. [3-5].

Сучасний розвиток інформаційних технологій призводить до появи нових кіберзагроз та каналів їх розповсюдження, отже питання кібербезпеки в ланцюгах постачань, які включають багато контрагентів, вимагає подальшого дослідження.

Метою статті є дослідження актуальних питань кібербезпеки в управлінні ланцюгами постачань.

Виклад основного матеріалу. Ланцюг постачання охоплює всі процеси, пов'язані з доставкою продукту чи послуги від постачальника до клієнта, включаючи закупівлю, виробництво, транспортування та розподіл. Під управлінням ланцюгами постачань (SCM) розуміють сучасну управлінську концепцію та організаційну стратегію управління потоками товарів і послуг, яка базується на інтегрованому підході до планування та управління всіма інформаційними та матеріальними потоками, які притаманні логістичним і виробним процесам. Концепція SCM була запропонована у 1982 році Кейтом Олівером, а далі була реалізована з використанням програмного забезпечення [6]. Саме автоматизація дозволила вивести управління логістичними, матеріально-технічними та інформаційними потоками на принципово новий рівень. Це призвело до появи самостійних SCM-систем, що являють собою пакети прикладного програмного забезпечення та зазвичай містять 2 модулі:

1) SCP-система планування ланцюгів постачань (англ. Supply Chain Planning), яка включає функції планування та формування календарних графіків, інтерфейси для спільного проектування, прогнозування та моделювання ситуацій, аналіз виконання операцій;

2) SCE-система реалізації ланцюгів постачань (англ. Supply Chain Execution), яка дозволяє відстежувати та контролювати потоки та операції на всіх етапах ланцюга.

Якщо спочатку SCM-системи отримали розвиток як самостійні рішення автоматизованої системи управління, то згодом вони почали інтегруватися в повноцінні ERP-системи (англ. Enterprise Resource Planning). ERP-системи – це автоматизовані системи планування та управління ресурсами підприємства. Вони базуються на організаційній стратегії інтеграції всіх інформаційних, матеріально-технічних, фінансових потоків підприємства в єдину систему, метою якої є безперервний моніторинг, балансування та оптимізація всіх видів ресурсів підприємства за допомогою загальної моделі даних та процесів для всіх сфер діяльності підприємства,

реалізованої у пакеті прикладного програмного забезпечення.

З управлінської точки зору, такі рішення є доцільними, оскільки вони дозволяють ефективно управляти ресурсами підприємства, а також вимірювати сукупний економічний ефект (зниження витрат, задоволення попиту на кінцеву продукцію). Цей ефект особливо відчутний в сучасних умовах, коли компанії зазвичай мають багато контрагентів в різних регіонах, а ланцюги постачань стали складними і розгалуженими. Автоматизація управління ланцюгами постачань та інтеграція SCM-систем в ERP-системи призвели до створення потужних інформаційних систем, які містять всю інформацію про діяльність підприємства. До того ж, зв'язки зі сторонніми контрагентами також здійснюються через цифрові канали. Тобто в сучасних ланцюгах постачань всі учасники мають економічний ефект від використання сучасних інформаційних технологій, але в той же час стають вразливішими через ризики витоку інформації та додаткові кіберзагрози.

Рисунок 1 відображає, що складові елементи управління компанією, такі як: виробничі процеси, фінанси, маркетинг, технології та інновації, персонал, потребують відповідних системи захисту даних. Але в ланцюгах постачань інформація розповсюджується не тільки у мікросередовищі компанії, до якого входять безпосередні контрагенти, а і у всьому ринковому середовищі. Отже постає питання захисту мереж та кінцевих споживачів.

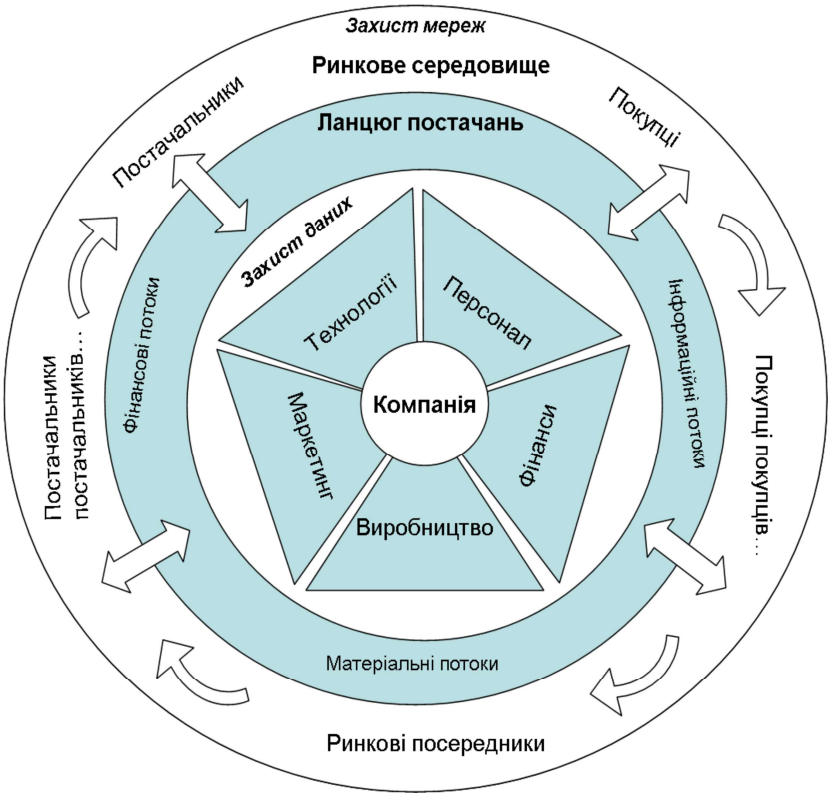

Рис. 1. Кіберзахист в ланцюгу постачань (розроблено авторами)

З 2020 року кількість хакерських атак на ланцюги постачань зросла у декілька разів. Наприклад, у березні 2020 р. при атаці на компанію FireEye, зловмисники встановили оновлення зі шкідливим кодом у продукт для управління мережею під назвою Orion від SolarWinds до того, як код був наданий FireEye, отже споживачі отримали пошкоджений кінцевий продукт. Таким чином хакери отримати доступ до сотень федеральних державних установ та освітніх організацій США, а також до 80 % компаній зі списку Fortune 500. При цьому близько 18000 комерційних та державних організацій встановили шкідливе оновлення через механізм Orion, близько 100 з них стали жертвами наступних кібератак [7]. Хакери залишалися непоміченими тривалий час і займатися крадіжкою інформації.

Отже, безпека сторонніх постачальників є одним з найбільших ризиків в SCM,

оскільки якщо отримати доступ до інформаційної системи постачальника, це може не тільки скомпрометувати весь ланцюжок поставок і поставити під загрозу конфіденційну інформацію, а і призвести до значних фінансових втрат. Іншим ризиком у SCM є атаки на самі ланцюги поставок, як в наведеному вище прикладі, де хакери отримали доступ до системи постачальника та використовували цей доступ для проникнення в мережи великих компаній та значної кількості компаній. Зазвичай великі компанії вживають достатньо заходів для захисту власних систем і даних, але і вони не можуть відстежувати загрози, які йдуть через мережу їх постачальників. Отже цей тип атаки може бути важко виявити та запобігти, оскільки в ній часто беруть участь декілька сторін і систем.

В результаті кібератак на ланцюги постачань страждають переважно кінцеві споживачі. Як зазначають аналітики, «саме тому атаки на ланцюг постачання несуть величезні збитки, оскільки зламавши тільки одного постачальника, зловмисники можуть в кінцевому підсумку отримати безперешкодний доступ до великих клієнтських баз, який складно виявити» [7].

Наразі впроваджено навіть термін SCA (англ. Supply Chain Attack) – атака на ланцюжок постачань. Основна ідея SCA – отримання доступу до даних компанії та/або контролю над її інформаційною системою через її контрагентів. Атака може бути спрямована як на покупців, так і на постачальників компанії. І серед постачальників слід особливо виділити вендорів програмного забезпечення, оскільки через них хакери можуть отримати доступ до контролю версії коду програми, а отже шкідливе програмне забезпечення може розповсюджуватися у вигляді легітимної програми і від таких загроз немає 100 % способу захисту.

Є різні види атак на ланцюги постачань, але їх можна згрупувати у два принципово різних підходи:

1) Програмні, тобто атаки, спрямовані на вихідний код програмного забезпечення постачальника. При цьому хакери вносять шкідливий код у додатки та оновлення легітимного програмного забезпечення;

2) Апаратні, тобто атаки, спрямовані на пристрої, зокрема на маршрутизатори, веб-камери, клавіатури з метою обходу стандартних процедур автентифікації та несанкціонованого віддаленого доступу до комп'ютерів.

Одним з поширених видів атак на ланцюги постачань є бекдор (англ. back door – чорний хід), тобто отримання віддаленого доступу до пристроїв та даних, залишаючись непоміченим. Бекдор може набувати форми встановленої програми (наприклад, так звані трояни) або може проникнути у систему через руткіти (програми для приховування слідів несанкціонованого стороннього доступу або шкідливої програми в системі) [8].

Жодна компанія не може гарантовано захистити себе від атак, спрямованих на ланцюги постачань. Тому головною метою кіберзахисту в управлінні ланцюгами постачань є визначення атак на ранній стадії, перш ніж зловмисники зможуть закріпитися в системі та завдати шкоди. Такі превентивні заходи включають:

– налаштування моніторингу мережі в режимі реального часу для виявлення підозрілих активностей;

– регулярне оновлення засобів захисту пристроїв та мереж;

– резервне копіювання даних;

– протоколи безпеки, що дозволяють запуск лише авторизованих програм;

– регулярне тестування на проникнення та аналіз захищеності;

– використання блокчейн;

Реалізація заходів кібербезпеки в управлінні ланцюгами постачань ускладнюється тим, що кіберзагрози можуть виникати не в самої компанії, а в її контрагентів, тобто потрібна узгодженість в заходах кібербезпеки з іншими компаніями. Блокчейн може забезпечити більшу прозорість і безпеку в ланцюгу постачань шляхом створення незмінного запису всіх транзакцій. Це дозволяє переконатися, що всі учасники ланцюга постачань дотримуються належних протоколів безпеки.

Висновки. В сучасних умовах безпека ланцюга постачання – це частина управління ланцюгом постачання, яка фокусується на аналізі та превентивних заходах щодо зменшення ризиків зовнішніх постачальників, продавців, логістики та транспорту. Якщо йдеться про кібербезпеку ланцюга постачань, то це аналіз і мінімізація кіберзагроз, пов'язаних з усіма учасниками ланцюгу. Слід зауважити, що надійність будь-якого ланцюга не більше, ніж надійність його найслабшої ланки. Тому заходи

кібербезпеки спрямовані саме на пошук слабких ланок в ланцюгу та подолання виникаючих там кіберзагроз. Отже, кібербезпеку можна вважати сучасним важливим елементом концепції SCM.

Загалом кібербезпека в SCM має вирішальне значення для бізнесу, щоб захистити свою конфіденційну інформацію та зберегти довіру своїх клієнтів. Щоб ефективно запобігати ризикам, компаніям необхідно перейти до проактивного підходу до кібербезпеки в SCM. Це включає проведення регулярних оцінок ризиків, впровадження надійних протоколів кібербезпеки для всіх сторін, залучених у ланцюги постачань, а також впровадження систем моніторингу будь-якої підозрілої діяльності. Компанії також повинні мати чіткий план дій на випадок порушення кібербезпеки, зокрема і план відновлення системи після атаки.

Список використаних джерел

1. Баранов О. А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*, 2014. № 2 (42). С. 54-62.

2. Cyber Security Breaches Survey. 2022. URL : https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

3. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право,* 2012. № 2. С. 162-169.

4. Дубов Д. В., Ожеван М. А. Кібербезпека : світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.

5. Потій О. В., Семенченко А. І., Дубов Д. В., Бакалинський О. О., Мялковський Д. В. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації,* 2021. Vol. 23, № 1. С. 47-60.

6. Mentzer J. T., DeWitt W., Keebler J. S., Min S., Nix N. W., Smith C. D., Zacharia, Z. G. Defining supply chain management. *Journal of Business logistics*, 2001. № 22 (2). P. 1-25.

7. Кількість атак на ланцюг постачання зростає: хто під прицілом та як протистояти. *ESET.* 2021. URL : https://eset.ua/ua/blog/view/111/kolichestvo-atak-na-tsep-postavok-rastet-kto-pod-pritselom-i-kak-protivostoyat.

8. Cyber Security Threats. URL : https://www.imperva.com/learn/application-security/cyber-security-threats/.

Надійшла до редакції 08.12.2022

References

1. Baranov, O. A. (2014). Pro tlumachennya ta vyznachennya ponyattya “kiberbezpeka” [On the interpretation and definition of the concept of "cyber security"]. *Pravova Infarmatyka*. № 2 (42), pp. 54-62. [in Ukr.].

2. Cyber Security Breaches Survey (2022). URL : https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

3. Furashev, V. M. (2012). Kiberprostir ta informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist’, vyznachennya, vidminnosti [Cyberspace and information space, cyber security and information security: essence, definition, differences]. *Informatyka i pravo*. No. 2. P. 162-169. URL : http://ippi.org.ua/sites/default/files/12fvmsvv.pdf. [in Ukr.].

4. Dubov, D. V., Ozhevan, M. A. (2011). Kiberbezpeka : svitovi tendentsiyi ta vyklyky dlya Ukrayiny [Cyber security: global trends and challenges for Ukraine]. Kyiv : NISD. 30 p. [in Ukr.].

5. Potii, O. V. et al. (2021). Kontseptual’ni zasady vprovadzhennya orhanizatsiyno-tekhnichnoyi modeli kiberzakhystu Ukrayiny [Conceptual principles of the implementation of the organizational and technical model of cyber protection of Ukraine]. *Zakhyst informatsiyi*. № 23 (1), pp. 47-60. [in Ukr.].

6. Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D. & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*. No 22 (2), pp. 1-25.

7. Kil’kist’ atak na lantsyuh postachannya zrostaye: khto pid prytsilom ta yak protystoyaty [Supply chain attacks are on the rise : who’s being targeted and how to fight back]. *ESET.* 2021. URL : https://eset.ua/ua/blog/view/111/kolichestvo-atak-na-tsep-postavok-rastet-kto-pod-pritselom-i-kak-protivostoyat. [in Ukr.].

8. Cyber Security Threats. URL : https://www.imperva.com/learn/application-security/cyber-security-threats/.

ABSTRACT

Olena Galushko, Tetyana Selivyorstova. Cyber security in supply chain management (SCM). Cyber security in supply chain management (SCM) is becoming increasingly relevant as today’s companies increasingly use information technology and digital systems. And the supply chains themselves are becoming more and more complex and include more and more participants. With so many

points of interaction and third-party suppliers and buyers, it can be difficult to monitor whether all parties are following proper cybersecurity protocols. Therefore, in today's business environment, cyber security is becoming an integral part of supply chain management. This involves a thorough analysis of potential risks created by external suppliers, buyers and other market participants, logistics and transportation, with further preventive measures to reduce them. Any supply chain is only as strong as its weakest link. Therefore, cyber security measures are mainly aimed at identifying vulnerabilities and eliminating cyber threats in the weakest links of the supply chain.

The article deals with the essence of supply chain management and analyzes the role of cyber security in the management system. It is noted, that in modern conditions, cyber security is becoming an element of supply chain management. The main types of risks and cyber threats in supply chains are analyzed, in particular the issue of security of third-party suppliers. Measures to eliminate cyber risks and to increase cyber security in supply chain management are proposed. By taking a proactive approach and implementing strong cybersecurity measures, companies can reduce the risk of cyberattacks and ensure the security of their supply chain.

Keywords: *supply chains, cyber security, information flows, counterparties, cyber threats.*

УДК 342
DOI: 10.31733/2078-3566-2022-6-542-547

Влада ЛІТОШКО©
викладач

Каріне МКРТЧЯН©
викладач

ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ОСНОВ СПІВПРАЦІ ДЕРЖАВ З ПРОТИДІЇ ПРАВОПОРУШЕННЯМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

Правопорушення у сфері інформаційних технологій становлять реальну загрозу суспільним відносинам на внутрішньодержавному рівні та міжнародному правопорядку. Проблема протидії правопорушенням у сфері інформаційних технологій неодноразово розглядалася в документах регіональних міжнародних організацій. Оскільки кожен регіональний правовий режим є унікальним і має свої особливості, у статті розглядаються можливі наслідки такої регіоналізації. На основі проведеного дослідження зроблено висновок, що регіоналізація міжнародно-правової взаємодії у боротьбі забезпечення кібербезпеки має свої позитивні і негативні сторони та призвела до ситуації, яка частково може бути пояснена транснаціональним характером правопорушень у цій сфері.

***Ключові слова*:** *протидія правопорушенням, міжнародна співпраця, правопорушення у сфері інформаційних технологій, інформаційна безпека, кібербезпека*.

© В. Літошко, 2022
ORCID iD: https://orcid.org/0000-0001-5712-6841
Vlada_lit@ukr.net

© К. Мкртчян, 2022
ORCID iD: https://orcid.org/0000-0002-6554-3917
karina19_7777@ukr.net