КИВЛЮК Ольга Петрівна,
д-р філос. наук, професор,
Київський інститут інтелектуальної власності та права
Національного університету «Одеська юридична академія»,
м. Київ
ORCID ID: 0000-0002-7900-9299

ВОРОНКОВА Валентина Григорівна,
д-р філос. наук, професор,
академік НАН ВО України,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні,
м. Запоріжжя
ORCID ID: 0000-0002-0719-1546
Україна

ФІЛОСОФСЬКА РЕФЛЕКСІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЦИФРОВОМУ СЕРЕДОВИЩІ: ПРОБЛЕМИ, РИЗИКИ, ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ

Актуальність дослідження інформаційної безпеки як складного соціального, економічного феномена у тому, що у цифровому середовищі існують десятки або, можливо, навіть сотні різних взаємопов'язаних активів, мереж і систем, на які ми щодня покладаємось для нормального функціонування суспільства. Без цих різноманітних компонентів інфраструктури суспільство не змогло б насолоджуватися перевагами життя в сучасному столітті, так як навіть невеликі збої у роботі цих компонентів призвели б до тимчасової втрати важливих можливостей. Щоб позбутися збоїв, загроз і катастроф цього або пом'якшити його наслідки слід ввести інформаційну безпеку на підприємстві і забезпечити надійну безпеку критичної інфраструктури[1]. Управління інформаційною безпекою – це спосіб захисту конфіденційних даних організації від загроз і вразливостей, що вбудовується через систему управління інформаційною безпекою (СУІБ), яка забезпечує основу для ефективного управління[2]. У центрі структури підприємств лежить управління інформаційними ризиками, які

1 Воронкова В.Г. Формування концепції стратегії кібербезпеки в умовах глобалізації: економічні засади. Scientific trends: modern challenges. Volume 2 : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2021, С.46-60

2 Воронкова В. Г. Технології інформаційного менеджменту в державному управлінні, Вісник Національного університету цивільного захисту України : зб. наук. пр. Харків : Вид-во НУЦЗУ, 2021, Вип. 2 (15). С.70-79.

можуть поставити під загрозу конфіденційність, цілісність і доступність інформації. Сучасні підприємства обробляють і зберігають величезні обсяги конфіденційних даних, які можуть знадобитися для надання послуг, покращення взаємодії з користувачем або прийняття кращих рішень щодо способу роботи. Якою б не була мета цих даних, важливо, щоб організації чи підприємства захищали їх, тому що якщо неавторизовані суб'єкти отримають інформацію у результаті кібератаки чи порушення конфіденційності, це завдасть довгострокової шкоди. **Метою даної статті** є теоретичні та практичні аспекти інформаційної безпеки. **Об'єкт дослідження** – інформаційна безпека як складний соціальний, економічний та управлінський феномен. **Предмет дослідження** - проблеми, ризики та виклики цифрового середовища, що впливають на упровадження інформаційної безпеки у сучасному суспільстві у контексті викликів та загроз.

Теоретичні та практичні аспекти спираються на цілі інформаційної безпеки, до яких відносяться наступні: 1) конфіденційність; 2) цілісність; 3) доступність. Дані та послуги, які на них покладаються, мають бути доступними авторизованим користувачам як у компанії, так і за її межами. Атака в обслуговуванні (DDoS) є прикладом загрози доступності даних і служб організації. Конфіденційність, цілісність і доступність даних організації чи підприємства можуть бути під загрозою різними способами[3].

Тому управління інформаційною безпекою передбачає виявлення потенційних ризиків для організації, оцінку їхньої ймовірності та потенційного впливу, розробку та впровадження стратегій усунення проблем для максимального зменшення ризиків за допомогою наявних ресурсів. Управляючи ризиками, організації отримують повне розуміння того, як вони можуть постраждати від витоку даних та інших руйнівних тенденцій, а також кроків, які вони можуть вжити, щоб захистити себе. З огляду на постійно зростаючу загрозу витоку даних і пов'язаних з цим регулятивних заходів важливо, щоб організації ефективно керували ризиками інформаційної безпеки. Тому слід створити таку систему, щоб запровадити стандарти, які допоможуть організації виконувати юридичні та нормативні зобов'язання[4]. Система управління інформаційною безпекою (ISMS) - це набір політик і процедур для систематичного управління конфіденційними даними організації; система засобів контролю, які систематично керують

3 Воронкова Валентина, Никитенко Виталина, Андрюкайтене Регина, Олексенко Роман, Капитаненко Наталья. Киберпреступность как новейшее явление инфрормационно-коммуникационного общества и пути ее предупреждения. Ежеквартальный немецкий научный/научно-популярный Вестник «Результаты работы ученых»; Социология, Криминология, Философия, Политология. 2021, Том 2, №7. С.58-67.

4 Мар'єнко В. Ю. Інформаційне забезпечення менеджменту в організаціях як складних системах в умовах цифровізації. Modern scientific strategies of development : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022, P. 62-81.

безпекою та ризиками на підприємстві і націлені на упровадження концепції інформаційної безпеки. Ці елементи управління безпекою можуть відповідати загальним стандартам безпеки або бути більш орієнтованими на ту чи іншу галузь. Метою Системи управління інформаційною безпекою є мінімізація ризиків та забезпечення безперервності бізнесу шляхом проактивного обмеження впливу порушення безпеки, що складає переваги управління інформаційною безпекою на підприємстві.

Окрім покращення безпеки даних організації, програма управління інформаційною безпекою може надати переваги: 1) створити оптимізовану безпеку даних: створити структуру та процес для оцінки ризиків безпеки даних та їх усунення; 2) прийняття такої програми може перетворити безпеку даних на більш ефективнішу та результативнішу, що дозволить організації оптимізувати архітектуру безпеки та усунути непотрібні та дублюючі рішення та сформувати покращену культуру безпеки; 3) часто Infosec належить ІТ-відділу або відділу безпеки, її важко поширити та застосувати в усій організації, тому навчання співробітників програмі управління інформаційною безпекою компанії може покращити безпеку та створити більш позитивну культуру безпеки; 3) розробити імідж бренду, так як витік даних та інші інциденти безпеки можуть зашкодити іміджу бренду організації. Продемонстрована відповідність найкращим практикам безпеки може підтримати репутацію організації та покращити відносини з клієнтами та партнерами. Основним призначенням управління інформаційною безпекою є запобігання витоку даних, яке починається з управління ризиками, під час якої організації створюють свої інформаційні активи та способи управління ризиками. Одним із основних принципів управління інформацією безпеки є розробка інтегрованої цілісної стратегії безпеки, яка ефективно усуває ризики безпеки даних організації. Найкраще це досягається за допомогою консолідованої архітектури безпеки, яка забезпечує ефективний моніторинг та керування безпекою[5].

Як свідчить аналіз, уніфікована платформа кібербезпеки Check Point була розроблена з урахуванням комплексного, консолідованого управління безпекою на основі чотирьох основних принципів[6]: 1) автоматизація процесів безпеки та їх інтеграція в конвеєри CI/CD, яка допомагає усунути помилки конфігурації та пришвидшити розгортання, водночас віддаючи

5 Voronkova, V., Nikitenko, V., Oleksenko, R., Cherep, O., Andriukaitiene, R., Briki, I. Digital paradigm of economy and management in the conditions of global human transformation. Technology Transfer: Innovative Solutions in Social Sciences and Humanities 2021. Вип. 4. P. 37–40.

6 Нікітенко В. О., Васильчук Г. М., Мержинський Є. К. Мережева економіка як чинник підвищення ефективності цифровізації у контексті розвитку цифрового суспільства від 1G до 5G. HUMANITIES STUDIES : Collection of Scientific Papers / ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 2022, Вип. 10 (87). С. 112-121

пріоритет безпеці; 2) консолідована архітектура безпеки покращує видимість і спрощує керування, підвищуючи ефективність; 3) гнучкі та динамічні рішення для управління безпекою дозволяють організації йти в ногу з кіберзагрозами, що швидко розвиваються, і скорочують час на керування безпекою; 4) високопродуктивний ефективний захист, який гарантує, що керування безпекою не є вузьким місцем і не перешкоджає цифровій трансформації[7]. Щоб дізнатися більше про те, як організації можуть покращити управління інформаційною безпекою організації, слід побудувати уніфіковану платформу кібербезпеки у дії. Управління інформаційною безпекою визначає та керує засобами контролю, які організація повинна запровадити, щоб переконатися, що вона розумно захищає конфіденційність, доступність і цілісність активів від загроз і вразливостей. Ядро системи управління безпекою включає управління інформаційними ризиками, процес, який передбачає оцінку ризиків, з якими організація повинна мати справу в управлінні та захисті активів, а також розповсюдження ризиків. Це вимагає належної ідентифікації активів та етапів оцінки, включаючи оцінку конфіденційності, цілісності, доступності та розвитку активів. У рамках управління інформаційною безпекою організація може запровадити інші передові практики, які містяться в стандартах ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035 щодо інформаційної безпеки. Система управління інформаційною безпекою включає: 1. Управління ризиками та їх зменшення. 2. Стратегії впровадження та навчання. 3. Відповідні стандарти. 4. Управління та пом›якшення ризиків. Управління інформаційною безпекою означає управління ефективними загрозами та вразливими місцями та їх пом'якшення, збалансовуючи зусилля з управління ефективними загрозами та вразливими місцями шляхом вимірювання ймовірності їх реального виникнення[8].

Безпека критичної інфраструктури включає визначення пріоритетів, надання планів захисту як фізичної, так і електронної інфраструктури, що сприяє належному функціонуванню суспільства. Аналізуючи фізичну безпеку та кібербезпеку, керівники гарантують продовжувати функціонування підприємства безперешкодно або з мінімальними збоями внаслідок навмисної атаки чи стихійного лиха. Різні сектори інфраструктури, які підпадають під безпеку критичної інфраструктури, бувають різноманітними.

7 Нікітенко В. О., Васильчук Г. М., Мержинський Є. К. Мережева економіка як чинник підвищення ефективності цифровізації у контексті розвитку цифрового суспільства від 1G до 5G. HUMANITIES STUDIES : Collection of Scientific Papers / ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 2022. Вип. 10 (87), С. 112-121.

8 Череп А. В., Воронкова В. Г., Череп О. Г. Систематизація дослідження цифрової трансформації нових бізнес-моделей. Економіко-правові та соціально-технічні напрями еволюції цифрового суспільства: матеріали міжнародної науково-практичної конференції: у 2 т. Том 2. Дніпро: Університет митної справи та фінансів, 2022, С. 331-332.

Однак, якщо розглядати разом, ці сектори складають більшу частину спроможності будь-якого суспільства функціонувати – і порушення навіть одного з цих секторів інфраструктури може мати катастрофічні наслідки для підприємства чи суспільства. Зазвичай вони включають оборону та національну безпеку, банківську справу та фінанси, розумні установи смарт-міста та смарт-суспільства[9].

Проаналізуємо вразливості, що загрожують суспільству та особистості. Терористичні атаки: будь-яка терористична атака, незалежно від того, ким вона здійснена, має лише одну мету - зруйнувати суспільство, на яке спрямовано напад. Руйнування Всесвітнього торгового центру у 2001 році є яскравим прикладом, оскільки воно порушило роботу інфраструктури центру Манхеттена[10]. **Геополітичні дії:** конфлікти на геополітичній арені є одним із найпоширеніших джерел руйнування інфраструктури. Сили вторгнення намагаються дестабілізувати своїх опонентів, пошкоджуючи комунальні послуги, обмежуючи доступ до транспортних мереж, відключаючи телекомунікації опонента[11]. **Пандемії охорони здоров'я:** Всесвітня пандемія або навіть пандемія, обмежена меншою територією, наприклад країною чи континентом, руйнує сучасне суспільство кількома способами. Хвороба знижує здатність людей виконувати повсякденні завдання, такі як робота. Пандемія COVID-19 є яскравим прикладом потужності пандемії здоров'я[12]. **Стихійні лиха:** більшість стихійних лих є локальними. Сейсмічна подія, наприклад, має достатньо руйнівної сили, щоб зруйнувати міста. Околиці міста можуть бути зруйновані торнадо або затоплені повінню. Проте є деякі природні катаклізми, які представляють більш серйозну небезпеку, наприклад, електромагнітний імпульс, спричинений сильним сонячним спалахом або викидом корональної маси. Виявлення та класифікація будь-яких загроз, з якими стикається суспільство, коли справа доходить до безперервної роботи його критичної інфраструктури, є лише першим кроком у забезпеченні безпеки інфраструктури. Також необхідно розробити стратегії стримування цих загроз. Багато з цих методів стримування та запобігання вже широко використовуються. Міністерству внутрішньої безпеки США чітко доручено запобігати терористичним атакам на території США.

9 Voronkova, V & Kyvliuk, O. Philosophical reflection smart-society as a new model of the information society and its impact on the education of the 21st century. Future human image 2017. P. 154-162.

10 Tovarnichenko, V. Pseudoscience and information security in smart-society. Humanities Studies 2019. Вип. 1 (78), P. 15-26.

11 Воронкова В. Г., Пунченко О. П. Флософія геополітичного переформатування світу у контексті сучасних викликів глобалізації.Humanities studies: Collection of Scientific Papers. Zaporizhzhia: Zaporizhzhia National University, 2021, Вип. 8 (85). С. 8-19.

12 Пунченко Олег, Воронкова Валентина, Водопьянов Павел. Здравоохранение как глобальная проблема человечества.International scientific-practical conference "Management. business. technologies - innovation. trends and challenges «. 20 – 21 May 2021, Marijampole, 2021. P.204-212.

Для запобіганню цих лих, необхідно, **по-перше**, зробити перелік усіх уразливостей: відомості про недоліки, які можна використовувати для пошкодження або компрометації конфіденційної інформації. До них слід віднести; 1) загрози - дії, за допомогою яких виникли вразливості, як, наприклад, кіберзлочинець використовує дефекти програмного забезпечення; 2) вплив - збиток, який спостерігається під час використання загрози, що включає затримку, втрату бізнесу, фінансові наслідки, репутаційну шкоду; 3) організація повинна аналізувати різні способи зламу інформації. Це можна розглядати через три принципи інформаційної безпеки. **По-перше,** це конфіденційність, яка приймає те, чи інформація доступна чи розкрита неавторизованим особам. **По-друге,** це щільність, яка вимагає повноти та точності конфіденційної інформації. Нарешті, існує доступність конфіденційної інформації, яка застосовується до того, що може авторизованим користувачам отримати доступ до інформації за вимогою[13]. **По-третє,** слід зробити перелік усіх загроз: небажані події, які можуть спричинити навмисну або випадкову втрату, пошкодження або нецільове використання інформаційних активів: 1) уразливості - кількість інформаційних активів та пов'язаних засобів керування вразливими до використання одного чи ключа загрозами; 2) вплив та ймовірність - розмір наявної шкоди інформаційним активам від загроз і вразливостей, які становлять серйозний ризик вони становлять для активів; аналіз витрат і вигод також може бути частиною оцінки впливу або окремо від неї; 3) пом›якшення - метод(и) для мінімізації впливу та ймовірності наявних загроз і вразливостей. Після того, як загрозу та/або вразливість буде ідентифіковано та оцінено як такі, що мають достатній вплив/ймовірність впливу на інформаційні активи, можна ввести в план дії пом'якшення. Вибір методу пом'якшення значною мірою залежить від того, в якому із доменів інформаційних технологій міститься загроза та/або вразливість. Загроза байдужості користувача до політики безпеки (домен користувача) вимагає значного іншого плану пом'якшення, ніж той, який використовується для обмеження загрози несанкціонованого зондування та сканування мережі.

Система управління інформаційною безпекою. Система управління інформаційною безпекою (СУІБ) являє собою зіставлення всіх взаємопов'язаних/взаємодіючих елементів інформаційної безпеки організації, щоб гарантувати, що політика, процедури та цілі можуть бути створені, реалізовані, передані та оцінені, щоб краще гарантувати загальну інформацію

13 Бугайчук О. В.,Воронкова В. Г. Інновації та інноваційні стратегії як фактор сталого цифрового розвитку економіки: зарубіжний досвід. Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах: матеріали Міжнародної науково-практичної інтернет-конференції. Дніпро : Університет митної справи та фінансів, 2021. С.55-58.

організації[14]. На цю систему впливають потреби, цілі, вимоги безпеки, розмір і процеси організації. Система управління інформаційною безпекою включає в себе ефективне управління ризиками та стратегії пом'якшення. Крім того, прийняття організацією Система управління інформаційною безпекою значною мірою вказує на те, що вона систематично виявляє, оцінює та керує ризиками інформаційної безпеки та «буде здатна успішно відповідати вимогам щодо конфіденційності, цілісності та доступності інформації. Однак пов'язані з цим людські фактори з розробкою, впровадженням і практикою Системи управління інформаційною безпекою (домен користувача також слід враховувати, щоб найкраще забезпечити кінцевий успіх.

Компоненти стратегії впровадження та навчання. Впровадження ефективного управління інформаційною безпекою (включаючи управління ризиками та пом'якшення) вимагає стратегії управління, яка враховує наступне: Керівництво вищого рівня повинно рішуче підтримувати ініціативи з інформаційної безпеки, надаючи офіцерам з інформаційної безпеки можливість «отримати ресурси, необхідні для повнофункціональної та ефективної освітньої програми» і, відповідно, систему управління інформаційною безпекою. Стратегія інформаційної безпеки та навчання повинні бути інтегровані в стратегії відділу та передаватися через них, щоб забезпечити позитивний вплив плану інформаційної безпеки організації на весь персонал. Навчання конфіденційності та «оцінка ризиків» може допомогти організації виявити критичні прогалини в знаннях зацікавлених сторін і ставленні до безпеки[15]. Належні методи оцінювання для «вимірювання загальної ефективності програми навчання та підвищення обізнаності» гарантують, що політики, процедури та навчальні матеріали залишаються актуальними. Політики та процедури, які належним чином розроблені, реалізовані, повідомлені та впроваджені, зменшують ризик і забезпечують не лише зменшення ризику, але й постійне дотримання чинних законів, нормативних актів, стандартів і політик. Основні етапи та часові рамки для всіх аспектів управління інформаційною безпекою допомагають забезпечити майбутній успіх. Без достатніх бюджетних міркувань для всього вищесказаного - на додаток до грошей, виділених на стандартне регулювання, IT, конфіденційність і безпеку - план/система управління інформаційною безпекою не може досягти повного успіху. Система управління інформаційною безпекою стосується поведінки та

14 Нікітенко В. О., Васильчук Г. М. Модель цифрового міста як чинник креативного розвитку. Humanities studies: збірник наукових праць / Гол. ред. В. Г. Воронкова. Запоріжжя : Видавничий дім «Гельветика». 2022, Вип.11 (88). С. 48-58.

15 Воронкова В. Г., Нікітенко В. О. Філософія цифрової людини і цифрового суспільства: теорія і практика: монографія. Львів-Торунь : Liha-Pres, 2022. 460 с.

процесів працівників, а також даних і технологій, націлений на певний тип даних, як-от дані клієнтів.

Чому управління інформаційною безпекою є важливим? Запровадження Загального регламенту захисту даних (GDPR) та його еквівалента у країнах ЄС підкреслило важливість ефективної інформаційної безпеки, надаючи наглядовим органам повноваження накладати значні штрафи. Створюючи Загальний регламент захисту даних, організації знижують ризик злому та демонструють регуляторам, що вони серйозно ставляться до інформаційної безпеки. Це допоможе на етапі розслідування та призведе до більшого м'якого покарання – або, відповідно, його взагалі не буде. Переваги управління інформаційною безпекою у тому, що, крім зниження ризику витоку даних і наступних штрафів, управління інформаційною безпекою забезпечує низку інших переваг. Наприклад, організації, які впроваджують Загальний регламент захисту даних завдяки підходу СУІБ до оцінки та аналізу ризиків організації можна скоротити витрати, витрачені на невибіркове додавання рівнів захисних технологій, які можуть не працювати; поліпшити культуру компанії. Цілісний підхід до використання стандарту охоплює всю організацію, а не лише ІТ, охоплює людей, процеси та технології. Це дає користувачам можливість легко розуміти ризики та використовувати засоби контролю безпеки як частину своєї повсюдної роботи. Для цієї організації необхідно розділити ризик на його складові компоненти[16].

Стандарти управління інформаційною безпекою та відповідністю

Відповідність стандартам управління інформаційною безпекою може залежати від багатьох факторів. Програма може бути навіяна внутрішньою політикою або детермінуватися зовнішніми силами. Обидва ці потенційні драйвери мають відповідні стандарти та відповідність. Назвемо стандарти управління інформаційною безпекою та відповідністю: 1) Загальний регламент захисту даних: захищає особисту інформацію громадян ЄС суворими вимогами щодо конфіденційності та безпеки даних. 2) Закон про перенесення та доступність медичного страхування: Постанова США для галузіохорониздоров'я,якавимагаєконтролюбезпекидлязахищеноїмедичної інформації. 3) Стандарт безпеки даних платіжних карток: нормативний акт, розроблений фінансовим сектором для запобігання шахрайству шляхом захисту особистих даних власників платіжних карток. Ці та інші закони про конфіденційність даних можуть прямо чи неявно вимагати впровадження

16 Марєнко В. Ю. Системна парадигма інформаційного забезпечення менеджменту на підприємстві в умовах цифровізації. Системний аналіз в управлінні: міжгалузеві дослідження: матеріали IV Всеукраїнської науково-практичної конференції за міжнародної участі 26-27 травня 2022 року / Національний педагогічний університет імені М. П. Драгоманова. Київ : Ореол-Сервіс, 2022. С.45-48.

програми керування безпекою інформації. Навіть якщо така програма не потрібна, дотримання нормативних вимог щодо безпеки даних масштабовано та стабільно робить необхідним впровадження ефективних процесів і процедур керування безпекою. Метою Системи управління інформаційною безпекою є максимізація інформаційної безпеки, досягнення бажаного для організації рівня інформаційної безпеки. Залежно від конкретних потреб галузі ці рівні контролю можуть змінюватися. Наприклад, оскільки охорона здоров'я є строго регульованою сферою, організація охорони здоров'я може розробити систему для забезпечення повного захисту конфіденційних даних пацієнтів[17]. Система управління інформаційною безпекою забезпечує цілісний підхід до управління інформаційними системами в організації.

Це забезпечує численні переваги. Система управління інформаційною безпекою: 1) Захищає конфіденційні дані. ISMS захищає всі типи інформаційних активів, незалежно від того, зберігаються в цифровому вигляді чи знаходяться в хмарі. Ці активи можуть включати персональні дані, інтелектуальну власність, фінансові дані, дані клієнтів і дані, довірені компаніям через треті сторони. 2) Відповідає нормативним вимогам, допомагає організаціям виконувати всі нормативні та договірні вимоги, забезпечує краще розуміння законності навколо інформаційних систем. Оскільки порушення законодавчих норм супроводжується значними штрафами, наявність СУІБ може бути особливо корисною для регульованих галузей із критично важливою інфраструктурою, як-от фінанси чи охорона здоров'я. 3) Забезпечує безперервність бізнесу: коли організації інвестують у СУІБ, вони автоматично підвищують свій рівень захисту від загроз. Це зменшує кількість інцидентів безпеки, таких як кібератаки, що призводять до меншої кількості збоїв і простою, що є важливим фактором для підтримки безперервності бізнесу. 4) Зменшує витрати. СУІБ пропонує ретельну оцінку ризиків усіх активів. Це дає змогу організаціям визначити пріоритетність активів із найвищим ризиком, щоб запобігти невибірковим витратам на непотрібні засоби захисту та забезпечити цілеспрямований підхід до їх захисту. 5) Підвищує культуру компанії. СУІБ забезпечує всеохоплюючий підхід до безпеки та управління активами в організації, не обмежуючись ІТ-безпекою. Це заохочує всіх співробітників розуміти ризики, пов'язані з інформаційними активами, застосовувати найкращі методи безпеки як частину своєї щоденної роботи. 6) Адаптується до нових загроз, так як загрози безпеці постійно розвиваються. СУІБ допомагає

17 Oksana Buhaychuk, Vitalina Nikitenko, Valentyna Voronkova, Regina Andriukaitiene, & Myroslava Malysh. Interaction of the digital person and society in the context of the philosophy of politics. Interacción persona digital y sociedad en el contexto de la filosofía política. CUESTIONES POLÍTICAS. Vol. 40, Nº 72. P. 558-572.

організаціям підготуватися та адаптуватися до нових загроз і постійно мінливих вимог середовища[18].

Коли йдеться про захист інформації та активів кібербезпеки, одностороннього підходу недостатньо. Слід дізнатися про різні типи елементів керування кібербезпекою та про те, як їх розмістити. Кожен технологічний бізнес-процес наражається на загрози безпеці та конфіденційності. Складні технології здатні протистояти атакам на кібербезпеку, але цього недостатньо: організації повинні переконатися, що бізнес-процеси, політики та поведінка персоналу мінімізують або пом'якшують ці ризики. Оскільки цей шлях не є ані легким, ані зрозумілим, компанії приймають рамки, які допомагають керувати найкращими методами інформаційної безпеки. Ось тут і вступають у гру системи управління інформаційною безпекою. Наприклад, ISO 27001 - це набір специфікацій, що детально описує, як створювати, керувати та впроваджувати політики та засоби контролю СУІБ. ISO не вимагає конкретних дій; натомість він надає вказівки щодо розробки відповідних стратегій системи управління інформаційною безпекою[19]. Для забезпечення оперативної інформаційної безпеки та системи управління подіями компанії необхідно: 1) виявляти загрози ІТ-безпеці швидко та на ранній стадії; 2) своєчасно вживати відповідних заходів проти ІТ-ризиків; 3) надійно відповідати внутрішнім вимогам компанії та міжнародним нормам; 4) звільнити ІТ-персонал від щоденного навантаження, автоматично визначаючи вразливі місця; 5) надати повні докази інцидентів комп'ютерної безпеки пізніше[20].

Правове забезпечення інформаційної безпеки

Нині поширення та використання ІКТ зачіпає інтереси всього міжнародного співтовариства. Ці технології потенційно можуть бути використані для цілей, які несумісні з цілями міжнародної стабільності та безпеки, і можуть мати негативний вплив на цілісність інфраструктури держав, порушуючи їх безпеку в цивільній і військовій сферах. Для забезпечення міжнародної інформаційної безпеки недостатньо зусиль окремих держав. Перш за все, заборона на використання державами інформаційної зброї повинна бути закріплена у міжнародному праві. До

18 Voronkova Valentina, Nikitenko Vitalina, Metelenko Natalya. AGILE-economy as a factor in improving the digital society. Baltic Journal of Economic Studies, Riga, Latvia : "Baltija Publishing", 2022, Vol.8, No 2. P. 51-58.

19 Крупа А. Г. Цифрова трансформація промисловості у країнах ЄС як чинник удосконалення суспільства INDUSTRY 4.0. XV Міжнародна науково-практична конференція «INTERNATIONAL SCIENTIFIC INNOVATIONS IN HUMAN LIFE».2022. С. 313-322.

20 Нікітенко В. О., Воронкова В. Г. Філософський дискурс про квантові комп'ютери як вираження прогресу цифрової цивілізації. III Міжнародна науково-практична конференція «Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності» 11-12 травня 2022 року. Запоріжжя: Національний університет «Запорізька політехніка», 2022. С.33-37.

спеціальних принципів міжнародного інформаційного права відноситься принцип конфіденційності та безпеки використання ІКТ. Зміцнення структури довіри, включаючи безпеку інформації та мережеву безпеку, конфіденційність і захист споживачів є необхідною умовою для розвитку інформаційного суспільства та зміцнення довіри серед користувачів ІКТ. Глобальну культуру кібербезпеки необхідно розвивати та впроваджувати у співпраці з усіма зацікавленими сторонами та міжнародними експертними органами. Ці зусилля мають бути підкріплені розширенням міжнародного співробітництва. З метою вирішення проблем міжнародної безпеки, що виникли з розвитком ІКТ, Генеральна Асамблея ООН прийняла Резолюцію № 58/199 від 23 грудня 2003 року про створення глобальної культури кібербезпеки та захисту критичних інформаційних структур, яка визначає елементи захисту критичної інформаційної інфраструктури, а саме: 1) мати мережі екстреного попередження про кібер-вразливості, загрози та інциденти; 2) підвищення обізнаності для полегшення розуміння зацікавленими сторонами характеру та масштабів критично важливої інформаційної інфраструктури та ролі, яку кожна з них має відігравати в їх захисті; 3) дослідження інфраструктури та виявлення взаємозалежностей між ними, посилюючи захист таких інфраструктур; 4) сприяння партнерству між зацікавленими сторонами, як державними, так і приватними для обміну та аналізу критичної інформації про інфраструктуру з метою запобігання, розслідування та реагування на пошкодження інфраструктури[21].

Концепція розвитку всеосяжної системи міжнародної безпеки має системний характер. Вона не обмежується питаннями військової безпеки, охоплює економічну, політичну, гуманітарну та інформаційну безпеку. Оскільки мова йде про розвиток цілісної системи міжнародної безпеки, вона повинна охоплювати всю систему міжнародних відносин. Комплексна система міжнародної безпеки означає такий стан, коли міждержавна система захищена від небезпек, які існують у сучасному світі. Це передбачає стабільне функціонування системи міжнародних відносин. Відносини між суб›єктами міждержавної системи включають також інформаційні відносини. Компанії чи підприємства повинні заохочувати інформаційну безпеку та впевненість у своїй здатності не лише безперервно надавати товари та/або послуги, але й швидко відновлюватися після катастроф ІТ з мінімальними збоями роботи комп'ютера.

21 Воронкова В. Г. Технології інформаційного менеджменту в державному управлінні. Вісник Національного університету цивільного захисту України : зб. наук. пр. Харків : Вид-во НУЦЗУ, 2021, Вип. 2 (15). С.70-79.

Слід назвати ключові федеральні закони, що впливають на конфіденційність в Інтернеті: 2. Закон про конфіденційність електронних комунікацій (1986) – захищає певні дротові, усні та електронні комунікації від несанкціонованого перехоплення, доступу, використання та розголошення. 2. Закон про комп'ютерне шахрайство та зловживання (1986) – забороняє певну діяльність, пов'язану з комп'ютером, пов'язану з неавторизованим доступом до комп'ютера з метою отримання певної інформації, шахрайства чи отримання будь-якої цінності, передачі шкідливих елементів або передачі комп'ютерних паролів. 3. Закон про захист конфіденційності дітей в Інтернеті (1998) – вимагає від певних веб-сайтів і постачальників онлайн-послуг отримувати підтверджену згоду батьків перед збором, використанням або розголошенням особистої інформації неповнолітніх віком до 13 років. 4. Закон про контроль над розповсюдженням небажаної порнографії та маркетингу (2003) – регулює надсилання небажаної комерційної електронної пошти та забороняє оманливу інформацію. 5. Закон про модернізацію фінансових послуг (1999) регулює збір, використання та розкриття особистої інформації, яку зберігають фінансові установи, і вимагає сповіщень клієнтів і письмової програми безпеки інформації. 6. Закон про справедливі та точні кредитні операції (2003) – вимагає від фінансових установ і кредиторів підтримувати письмові програми запобігання крадіжці особистих даних[22]. Майже щодня надходять повідомлення про масштабні кібератаки, використання програм-вимагачів і витік наборів даних. Правові акти мають на меті озброїти країни ЄС проти численних загроз, які створює кіберзлочинність. 1. Директива про мережеві та інформаційні системи, яка спрямована на створення єдиної правової бази для кібербезпеки[23], має бути переглянута та адаптована до нових викликів. 2. Регламент вільного потоку даних прийнятий у листопаді 2018 року має на меті полегшити вільний потік неперсональних даних у межах ЄС з метою просування європейської індустрії даних і розвитку транскордонних технологій. 3. Закон про кібербезпеку має посилити її роль і отримати постійний мандат. Окрім інституцій ЄС, він покликаний підтримувати країни-члени у покращенні кібербезпеки[24]. Крім того,

22 Бугайчук О. В. Ієрархія корпоративних показників цифрової трансформації на промислових підприємствах. Humanity Studies. 2021, Вип. 9 (86). С.138-146.

23 Мар'єнко В. Ю. Концепція інформаційного забезпечення менеджменту на підприємстві в умовах цифровізації. Формування сучасних концепцій менеджменту організацій та адміністрування в умовах цифровізації : матеріали міжнародної науково-практичної конференції, присвяченої 25-річчю створення кафедри менеджменту організацій та управління проектами 23–24 вересня 2021 року / ред.-упорядник д.філософ.н., проф. В. Г. Воронкова. Запоріжжя: Видавничий дім «Гельветика», 2021. С.108-114.

24 Крупа А. Г. Машинне навчання і штучний інтелект як чинники удосконалення інформаційно-комп'ютерних технологій. Актуальні проблеми сучасної філософії та науки: виклики сьогодення: зб. наук. праць / редкол. М. А. Козловець, Л. В. Горохова, О. В. Чаплінська [та ін.]. Житомир: Видавничий центр ЖДУ імені Івана Франка, 2022. С.99-102.

Закон про кібербезпеку запроваджує європейську систему сертифікації кібербезпеки, яка класифікує ІТ-продукти, послуги та процеси на визначені «низький», «середній» і «високий» рівні безпеки. 4. Директива про відкриті дані та публічну інформацію спрямована на покращення доступності даних державного сектору та запровадження загальноєвропейських правил повторного використання цих даних. 5. Директива про цифровий контент культивує покращення доступу споживачів до цифрового контенту та послуг по всій Європі. Це спрямовано на досягнення «єдиного цифрового ринку», забезпечуючи при цьому високий рівень захисту споживачів. 7. Закон про цифрові послуги знаходиться на стадії обговорення і має на меті створити надійні умови для надання інноваційних послуг на єдиному ринку та сприяти безпеці в Інтернеті. Цей законодавчий акт націлений насамперед на постачальників посередницьких послуг (особливо на онлайн-платформи, такі як соціальні медіа та торгові майданчики). 8. Закон про цифрові ринки є одним із багатьох законодавчих законопроектів, що відіграє велику роль у створенні вищого рівня конкуренції на цифрових ринках, сприяє запобіганню зловживанню ринковою владою великими компаніями та полегшенні виходу на ринок для нових компаній[25]. 9. Закон про штучний інтелект класифікукується за класами ризику: чим вищий ризик, тим більші зобов'язання мають бути покладені на відповідну компанію. 10. Закон про дані все ще перебуває на стадії консультацій і затвердження, спрямований на полегшення доступу до даних та їх використання, які мають бути краще захищені законом. 11. Закон про кіберстійкість, метою якого є встановлення єдиних стандартів кібербезпеки для мережевих пристроїв. Таким чином, політика інформаційної безпеки допомагає створити безпечне та захищене ІТ-середовище, що відповідає вимогам клієнтів компанії та забезпечує стабільність і безперервність ІТ-активів бізнесу, щоб допомогти організаціям відповідно до вимог політики та операцій безпеки інформаційних технологій компанії[26].

DOI: 10.51587/9798-9866-95907-2022-009-160-172

25 Мар'єнко В. Ю. Системна парадигма інформаційного забезпечення менеджменту на підприємстві в умовах цифровізації. Системний аналіз в управлінні: міжгалузеві дослідження: матеріали IV Всеукраїнської науково-практичної конференції за міжнародної участі 26-27 травня 2022 року / Національний педагогічний університет імені М. П. Драгоманова. К. : Ореол-Сервіс, 2022. С.45-48.

26 Бугайчук О. В. Зарубіжний досвід використання цифрової стратегії в умовах Четвертої промислової революції. Актуальні проблеми сучасної філософії та науки: виклики сьогодення: зб. наук. праць / редкол. М. А. Козловець, Л. В. Горохова, О. В. Чаплінська [та ін.]. Житомир: Видавничий центр ЖДУ імені Івана Франка, 2022. С.84-87.