УДК 005.33
DOI: 10.31673/2409-7292.2022.040011

Скибун О.Ж.

СУЧАСНА ЕТИКА ЯК ПРАКТИЧНА ФІЛОСОФІЯ КІБЕРБЕЗПЕКИ

У статті розглянуто питання моралі та етики у рамках професійного та корпоративного кодексів поведінки у сфері кібербезпеки. Було відзначено, що нові засоби виробництва, цифрові технології, цифровізація інформаційних та комунікативних процесів, побудова *е-економіки* створили передумови до появи нових сфер виробництва, нових професій та спеціальностей. У таких нових реаліях зростає рівень відповідальності серед працівників, які мають доступ до автоматизованих систем управління, баз даних персональних даних та масивів інформації, коли через низьку культуру виробництва та низький рівень кібергігієни та основи кіберзахисту приводить до втручання кіберзловмисників у роботу критичної інфраструктури, виробничих процесів, а це може спричинити витік чутливої інформації, аварії на об'єктах критичної інфраструктури, системі управління країною (сферою безпеки і оборони), а також витік приватних даних. Для мінімізації наслідків кіберінцидентів необхідно піднімати рівень професійної та корпоративної етики поведінки співробітників через адаптування існуючих кодексів поведінки у контексті безпеки інформації та кібербезпеки. Також запропоновано додати до переліку базових та ключових компетентностей нові, а саме: кібергігієна та кібербезпека. При цьому необхідно передбачити включення до існуючих та розроблення нових освітніх стандартів для нових професій та спеціальностей у сфері безпеки інформації та кібербезпеки набуття нових компетентностей, пов'язаних із кібербезпекою та кіберзахистом.

Ключові слова: базовий рівень компетентностей, мораль, етика, кодекс поведінки, професійна та корпоративна етика, кіберпростір, кіберзагрози, кіберзахист, кібербезпека, сфера безпеки інформації та кібербезпеки.

Вступ

Питання етики та моралі супроводжують людство на всіх етапах його цивілізаційного розвитку. Разом із людиною змінювалися і акценти та розуміння тих чи інших морально-етичних норм, сфера їх використання, а також відбувалося становлення певного переліку загальнолюдських морально-етичних норм, чеснот, вчинків, які підтримуються суспільством на рівні цивілізованого соціуму, де в якому перебуває більшість. Так, на рівні традиційного суспільства відбувався чіткий поділ на соціуми за допомогою майнового стану та ступінь фізичної свободи індивіда, який також впливав на морально-етичне становлення особистості. Наприклад, Стародавні Греція та Рим, де поряд із високим рівнем громадянських прав і свобод, ознак демократії існував інститут рабства, работоргівлі тощо. Аналогічна ситуація споглядалася і середні віки, де існували залежні люди, кріпосні тощо. Але це стосовно особистісного рівня та/або побутового рівня.

Поштовхом для формування та розвитку професійної та корпоративної етики став розвиток ремесл. Прообразом сучасної професійної та корпоративної етики були гільдії ремісників, в яких чітко регламентувалася уся діяльність ремісників, що входили до цих гільдій. Розквіт діяльності цих гільдій прийшовся на середні віки в Європі. Наступним етапом розвитку професійної та корпоративної етики стало зародження капіталізму та побудова масових виробництв, де на заводах і фабриках почала працювати значна кількість людей, роботу яких необхідно було контролювати та управляти великими масами людей.

З часом перелік сфер діяльності людини та професій постійно збільшується, а це в свою чергу потребує формалізацію поведінки спеціаліста на рівні підприємства/корпорації та на рівні професії в цілому.

Слід звернути увагу, що при цьому окремі питання моралі та етики так і залишилися на рівні фізичного права, і регулюються лише фізичним правом. Інші знайшли відображення на рівні юридичного права. Так, дотримання норм природнього права повною мірою залежить від самої конкретної людини, її рівня сомовиховання, саморозвитку та самоконтролю. Що стосується юридичного права, то його норми чітко вписані та носять обов'язків характер до виконання. На сьогодні суттєвий акцент робиться на такі питання моралі та етики, як: особиста та суспільна свободи, рівність, людська гідність, толерантність, людинцентризм тощо.

Разом з цим нові засоби виробництва, цифрові технології, цифровізація інформаційних та комунікативних процесів, побудова *е-економіки* створюють передумови до появи нових сфер виробництва, нових професій та спеціальностей.

Також ці фактори впливають на формування нової цифрової реальності, де кіберпростір, соціальні мережі та соціальні медіа, інформатизація широко входять у повсякденне життя сучасної людини. Крім того, як відначають дослідники Ю. Щавінський та І. Щавінська, «використання інформаційних технологій визначає структуру і якість військових озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил», а «інформаційна сфера нині є системоутворювальним фактором життя суспільства, вона активно впливає на стан політичної, економічної, оборонної і інших складових безпеки держави» [6, с.195]. При цьому необхідно враховувати, що цифровізація, комп'ютеризація, автоматизація багатьох процесів разом із широким використанням цифрових технологій формують новий простір – кіберпростір, тип загроз – кіберзагроз, кібератак, кіберінцидентів, кіберрозвідка, кібертероризм, кібершпигунство та злочинів – кіберзлочинів, а це в свою чергу створює необхідність кіберзахисту, кібероборони. Відповіддю на вказане є поява нових професій та спеціальностей у сфері безпеки інформації та кіберзахисту.

Аналіз останніх публікацій показав, що подальший дискурс сучасної етики як практичної філософії сфери кібербезпеки є досить популярним серед дослідників та науковців, а саме: А. Баришева, Л. Веселова, Ю. Гладка, О. Довгань, А. Каленський, Ю. Матюхіна, А. Тарасюк, Н. Троянска, Е. Фаулер, П. Френкен, Н. Шредер, Ю. Щавінський, І. Щавінська тощо.

Незважаючи на досить широкий спектр проведених досліджень, питання дискурсу щодо сучасної етики як практичної філософії сфери кібербезпеки, **виступає частиною загальної проблеми,** котрій присвячується означена стаття.

Формулювання завдань (мети) статті. Метою статті є розгляд формування сучасної етики та моралі у контексті дискурсу практичної філософії сфери кібербезпеки на рівні професійних та корпоративних правил поведінки, етики та моралі.

Методи дослідження, використані у процесі написання статті, передбачають застосування загальнонаукових та емпіричних прийомів, що ґрунтуються на системному підході. Крім цього, у процесі роботи застосовувались такі загальні методи досліджень, як узагальнення та порівняння. В результаті проведеного аналізу дискурсу сучасних питань етики та моралі у контексті практичної філософії кібербезпеки було сформовано практичні рекомендації щодо подальшого формування професійної та корпоративної етики у сфері кіберзахисту.

Виклад основного матеріалу. Сучасний етап розвитку технологій та техніки разом і широким впровадженням результатів цифрової та четвертої промислової революцій у повсякденне життя змінює не тільки навколишнє середовище, а і саму людину, її психологічний та моральний-етичний облік. При цьому «виникає висока соціальна небезпека безконтрольного застосування технологій, засобів і методів психофізичного впливу на великі соціальні групи людей через свідомість і підсвідомість людини» [6, с.193], що також впливає на питання безпеки інформації та кіберзахисту.

На сьогодні вже виросло і починає виходити на ринок праці так зване цифрове покоління, діти, які народилися в епоху цифрових технологій, коли мобільний телефон, планшет, комп'ютер опановувався ними швидше ніж будь-які традиційні іграшки та побутові предмети. Для таких дітей робота з новими гаджетами, цифровими технологіями, мережеві комп'ютерні ігри та перебування у віртуальному просторові (соціальні мережі та соціальні медіа) є природнім середовищем перебування, де вони почувають себе «як риба у воді». При цьому необхідно враховувати, що комунікації у мережевих комп'ютерних іграх та перебування у соціальних мережах відбуваються на глобальному світовому рівні, що вимагає знання основних мов міжнародного спілкування, а також потребує дотримання певних норм етики та моралі, інакше порушник буде видалений модератором цієї мережі, а також самі гравці та/або інші користувачі соціальних мереж «забанять» порушника. Окрім чітко

встановлених правил поведінки та перебування і тій чи інший віртуальній спільності, блозі існують «неписані правила поведінки», яких також необхідно дотримуватися. Якщо враховувати рівень охоплення та час проведення людини у віртуальному просторові (поза робочий час) можна з усією упевненістю надавати усі ознаки нової сфери і визначати правила поведінки, етики та моралі як професійні. Адже у багатьох заробіток та робота відбуваються безпосередньо у соціальних мережах та медіа (стрімери, блогери, ведучі окремих сторінок тощо). Вказані професії та спеціальності поки не знайшли офіційного визначення у існуючих класифікаторах, але разом з тим їх не можна не враховувати під час розгляду питань етики та моралі у сфері кібербезпеки на професійному та корпоративному рівнях.

Крім цього, робота з цифровою інформацією, а також доступ до персональних даних та значних масивів даних інформації з різних сфер суспільства створює передумови для вироблення відповідної етики поведінки з цими даними та роботи в кіберпросторі взагалі. Також цифрові технології, робототехніка та широке впровадження цифрових технологій та віддаленої роботи відбувається на рівні різних технологічних виробничих процесів, а також під час управління цими процесами на об'єктовому рівні та рівні цілої сфери (галузі виробництва). У таких нових реаліях зростає рівень відповідальності серед працівників, які мають доступ до автоматизованих систем управління, персональних даних та масивів інформації, адже втручання у роботу критичної інфраструктури, виробничих процесів може спричинити до катастрофічних наслідків від яких може постраждати значна кількість людей. Саме цьому все більшої актуальності набувають питання набуття високого рівня кіберкомпетеностей (кібергігієна та основи кіберзахисту) на всіх рівнях здобуття освіти, подальшої роботи та у повсякденному житі та побуті. Таким чином правилами кібернетичної поведінки, моралі та етики необхідно доповнювати вже існуючі професійні та корпоративні правила поведінки, етики та моралі. При цьому поява окремих спеціальностей у сфері кібербезпеки формує базу для професійних та корпоративних правил поведінки, етики та моралі.

Крім того, місце перебування значної кількості людей по всьому світові та значна частина комунікацій визначається кіберпростором, так званим віртуальним світом, рівень якого постійно зростає, коли як рівень фізичного (реального) простору зменшується. А тому є потреба у зростанні рівня цифрових та кіберкомпентностей з боку усього населення та молодих спеціалістів в першу чергу. Отже, набуття кібероснов є вкрай важливим. Так, відповідно до Державного стандарту базової середньої освіти [4] включено, серед іншого, такі ключові компетентності: інформаційно-комунікаційна компетентність та навчання впродовж життя [1]. При цьому «компетентність» визначається як здатність особи успішно соціалізуватися, навчатися, провадити професійну діяльність, яка виникає на основі динамічної комбінації знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей» (стаття 1 Закону України «Про вищу освіту»). На наш погляд вказаного вже стає недостатньо, оскільки розвиток суспільства, технологій та техніки відбувається дуже стрімко, а тому вже і цих компетентностей стає недостатньо для набуття високого професійного рівня для майбутнього спеціаліста. Так, на професійному рівні відбувається формалізація нової реальності, де питання безпеки інформації та кіберзахисту виступають провідниками формування нових професій та спеціальностей. Так, у вересні 2022 року «були внесені зміни та додано 17 нових професій у галузі безпеки інформації та кіберзахисту», серед яких виділяють такі: «розробник систем захисту інформації; аналітик загроз безпеки; фахівець криптографічного захисту інформації; фахівець реагування на інциденти кібербезпеки; фахівець підтримки інфраструктури кіберзахисту; фахівець з технічного захисту інформації; фахівець з тестування систем захисту інформації; інструктор-методист інформаційної безпеки та кібербезпеки; дізнавач сфери кібербезпеки та захисту інформації; експерт-криміналіст сфери кібербезпеки та захисту інформації; слідчий кіберзлочинів тощо» [2]. У зв'язку з чим постає питання у наявності набуті майбутніми спеціалістами нових компетентностей, а саме основ кібергігієни та кіберзахисту. Адже підготовка

зазначений вище професій та спеціальностей потребує відкриття нових спеціальностей на факультетах у закладах вищої освіти та передвищої освіти де будуть готуватися майбутні спеціалісти з нових професій у сфері безпеки інформації та кіберзахисту. Для цього виникає потреба у адаптації переліку базових компетенцій, яких набувають здобувачі освіти у закладах освіти усіх рівнів.

Що стосується виробничої сфери та корпоративної діяльності в сфері безпеки інформації та кіберзахисту, то виникає потреба у створенні нових кодексів етики і моралі до нових професій. Так, словник іншомовних слів (https://www.jnsm.com.ua) дає нам такі тлумачення слова «кодекс», як: «сукупність етичних норм, правил поведінки, що склалися в даному суспільстві (наприклад, моральний Кодекс)», «збірник правил, інструкцій, що регулюють певну галузь діяльності, спортивних змагань», а також пропонується тотожний термін «статут», який визначається як «зведення правил, що визначають завдання, структуру, функції та порядок діяльності якої-небудь установи, організації і т. ін.; збірка правил; устав, кодекс» [5]. В свою чергу А. Каленський, досліджуючи питання «розвитку професійно-педагогічної етики у майбутніх викладачів спеціальних дисциплін» у загальному вигляді визначає «кодекс етики» як зведення норм правильної, належної поведінки, що вважаються доречним для людини тієї професії, до якої даний кодекс має відношення» [3, с.99]. На наш погляд доцільно до питань етики додавати і питання моралі, щоб у цілому це був морально-етичний кодекс поведінки в сфері безпеки інформації та кіберзахисту.

Вказане у повній мірі необхідно відносити не тільки до нових професій у сфері безпеки інформації та кібербезпеки, а і до традиційних професій, адже на сьогодні комп'ютеризація, IT-технології, ІКТ робота з базами даних широко впроваджуються в інші сфери, де відбується поєднання професій із такими спеціальностями як: користувач ПЕОМ, обчислення (комп'ютеризація), обчислювальні системи, розробники комп'ютерних програм, електроніка та телекомунікації тощо.

До певного базису моралі і етики у сфері кібербезпеки слід віднести наявність певного рівня компетентності в частині кібергігієни та кіберзахисту, адже якщо навіть у майбутньому людина не буде працювати у сфері безпеки інформації та кіберзахисту, набуті знання, навички, уміння стануть у нагоді, адже на побутовому рівні поступово зростає рівень кіберпростору та цифрових комунікацій у віртуальному кіберпросторі. Найпростішим прикладом може слугувати налагодження для своєї дитини робочого місця для онлайн навчання у школі, здійснення комунальних платежів через онлайн платформи, замовлення та оплата товарів та послуг через Інтернет, доступ до засобів масової інформації та засобів масових комунікацій, банківські операції, розваги (мережеві комп'ютерні ігри, SMART TV тощо), перебування у соціальних мережах, навчання, отримання адміністративних послуг через Інтернет, телемедицина тощо. Усе це потребує роботи з власними персональними даними, які разом із приватною інформацією, коштами можуть стати легкою здобиччю кібершахраїв та кіберзлочинців. Вказані вище аспекти стосуються так би мовити приватного рівня. Інший рівень – робочий: під час виконання свої посадових обов'язків, коли низький рівень кібергігієни та основ кіберзахисту може спричинити до втрати даних на робочому місці або навіть призвести до катастрофічних наслідків для екології, навколишнього середовища, життя людей тощо.

На сьогодні багато міжнародних корпорацій значну увагу приділяють питанням корпоративної поведінки, моралі та етики співробітників, особливо компанії, які обслуговують об'єкти критичної інфраструктури, а також, які забезпечують функціонування відкритих соціальних мереж, соціальних медіа, веб-сервісів, онлайн-сервісів та пошукових систем, де є доступ до значної бази даних персональних даних, телеметричних даних та управління виробничими процесами. Як показує практика, значна частка кіберінцидентів відбувається через людський фактор: низький рівень кібергігієни та основ кіберзахисту, неуважність та халатне ставлення до інструкцій та застережень.

Ось чому така значна увага приділяється сьогодні до питань безпеки інформації та кіберзахисту, адже кіберзагрози починають домінувати над усіма іншими, адже на сьогодні

питання управління виробничими процесами, окремими об'єктами та цілими секторами економіки відбувається з використання ІКТ, віддаленого доступу, програмного забезпечення і навіть з використанням елементів штучного інтелекту та Інтернету речей. Крім того, уся критична інфраструктура стає залежною від організації безпеки інформації та кіберзахисту як на об'єктовому рівні, так і на рівні цілих галузей і сфер (телекомунікацій, енергетична, транспортна, банківська, сфера послуг, надання адміністративних послуг, медицина, освіта, управління у сфері безпеки і оборони тощо).

Висновки

Підсумовуючи розгляд сучасного дискурсу стосовно моралі та етики як практичної філософії кібербезпеки можна відзначити таке. Подальший розвиток сфери безпеки інформації та кібербезпеки обумовлюється появою нових професій та спеціальностей, які в свою чергу потребують підготовку відповідних фахівців та спеціалістів, які матимуть достатній рівень знань, навичок та компетентностей їх обіймати. Разом з тим, окрім вузькопрофесійної направленості підготовки кадрів існує необхідність забезпечення відповідної психологічної підготовки спеціалістів до роботи в цій сфері, а також є потреба у забезпеченні необхідного рівня стосовно морально-етичної готовності для роботи. Отже, на професійному та корпоративному рівнях необхідно адаптувати існуючи кодекси поведінки з урахуванням питань моралі та етики в частині безпеки інформації та кібербезпеки. Додати до переліку базових та ключових компетентностей, які повинні набути здобувачі освіти під час навчання такі: кібергігієна та кібербезпека та забезпечити їх широке запровадження в освітні процеси для підняття загального рівня кіберосвіти серед населення в умовах цифрового суспільства. Передбачити включення до існуючих та розроблення нових освітніх стандартів, набуття компетентностей для нових професій та спеціальностей у сфері безпеки інформації та кібербезпеки.

Перелік посилань

1. Державний стандарт базової середньої освіти. [Електронний ресурс] – Режим доступу: https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/nova-ukrayinska-shkola/derzhavnij-standart-bazovoyi-serednoyi-osviti (дата звернення 28.10.2022) – Назва з екрана.
2. ДССЗЗІ розширила кількість професій сфери безпеки інформації та кіберзахисту. [Електронний ресурс] – Режим доступу: https://mil.in.ua/uk/news/dsszzi-rozshyryla-kilkist-profesij-sfery-bezpeky-informatsiyi-ta-kiberzahystu/. (дата звернення 19.10.2022) – Назва з екрана.
3. Каленський А.А. Розвиток професійно-педагогічної етики у майбутніх викладачів спеціальних дисциплін : монографія / Андрій Анатолійович Каленський. 2- ге вид., випр. і доп. Київ: ЦП «Компринт», 2016. 424 с.
4. Про деякі питання державних стандартів повної загальної середньої освіти : постанова Кабінету Міністрів України від 30 вересня 2020 р. № 898. [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/npas/pro-deyaki-pitannya-derzhavnih-standartiv-povnoyi-zagalnoyi-serednoyi-osviti-i300920-898 (дата звернення 29.10.2022) – Назва з екрана.
5. Словник іншомовних слів. [Електронний ресурс] – Режим доступу: https://www.jnsm.com.ua/cgi-bin/u/book/sis.pl?Qry=%CA%EE%E4%E5%EA%F1(дата звернення 29.10.2022) – Назва з екрана.
6. Щавінський Ю.В., Щавінська І.Ю. Вплив розвитку інформаційних технологій на інформаційну безпеку держави: психологічний аспект. НАУКОВИЙ ВІСНИК 2 (1)′2012 Львівського державного університету внутрішніх справ. Львів, 2012, С.193-202.

Надійшла: 02.12.2022 Рецензент: д.т.н., доцент Ахрамович В.М.