ШІ, а й створення ціннісних рамок для його використання, що захищатимуть і підсилюватимуть людські цінності. Це дозволить забезпечити відповідальний розвиток технологій, що підтримуватимуть суспільство, а не загрожуватимуть йому.

Література

1. Тегмарк М. Життя 3.0. Доба штучного інтелекту / Пер. з англ. – К.: КМ-Букс, 2018. – 480 с.

2. Бостром Н. Штучний інтелект: Етапи. Загрози. Стратегії / Пер. з англ. – К.: Наш Формат, 2018. – 432 с.

3. Харарі Ю. Н. 21 урок для XXI століття / Пер. з англ. – К.: BookChef, 2019. – 384 с.

4. Флоріді Л. Етика інформації / Пер. з англ. – К.: КМ-Букс, 2021. – 320 с.

5. Каплан Дж. Штучний інтелект: що потрібно знати людству / Пер. з англ. –Х.: Фоліо, 2020. – 336 с.

Філософія кібербезпеки

Олександр СЕМЕНЕЦЬ здобувач ІІІ освітньо-наукового ступеня (PhD)
Науковий керівник тез - Ольга ПРОЦЕНКО, доктор. філос. наук, професор
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут»

У сучасному світі, де цифрові технології стали невід'ємною частиною життя, кібербезпека набуває все більшого значення. Водночас із технічними рішеннями, які захищають інформацію, постає низка філософських питань: як визначити межу між приватністю та контролем? Чи може держава втручатися в цифрове життя своїх громадян? Які етичні принципи мають лежати в основі розробки систем безпеки? Базуючись на цих тезах, я хотів би розкрити надважливі теми сучасного світу.

Філософія, як наука, що займається пошуком сенсу, етики та істини, допомагає аналізувати ці виклики на глибшому рівні. Вона ставить питання про відповідальність, свободу і людську природу у світі, де інформація може бути водночас ресурсом і зброєю. Концепції етики, онтології, політики та соціальної справедливості знаходять нове застосування в аналізі цифрового простору та його безпеки.

У цьому контексті, філософія кібербезпеки досліджує не лише технічні аспекти захисту даних, а й морально-етичні дилеми, соціальні наслідки глобального контролю та питання про те, як кіберпростір змінює наше розуміння реальності. Саме на перетині технічного прогресу та філософських ідей відкривається простір для дискусій про нові виклики, які стоять перед людством у цифрову епоху.

Для розуміння цих питань важливо не лише аналізувати сучасні технології, але й звертатися до філософських концепцій, які дозволяють осмислити фундаментальні аспекти кіберпростору та його вплив на наше життя.

Однією з ключових проблем є довіра до технологій і алгоритмів. Люди дедалі частіше передають свої особисті дані цифровим платформам, використовуючи мобільні додатки, соціальні мережі та сервіси електронної

комерції. У своїй праці «Принцип відповідальності» (2001) Йонас наголошував, що технологічний прогрес несе не тільки користь, але й ризики, які можуть загрожувати самому існуванню людства. Він підкреслював важливість відповідальності не лише перед сучасними поколіннями, а й перед майбутніми. У контексті кібербезпеки ця філософія закликає до усвідомлення довготривалих наслідків використання технологій, які впливають на довіру між людьми, державами та корпораціями [1]. Його підхід закликає як розробників, так і користувачів думати не лише про сьогодення, але й про те, як наші дії вплинуть на майбутнє цифрового суспільства.

Важливо підкреслити ще одну проблематику у сучасному світі - проблему приватності. Приватність завжди була однією з ключових цінностей людини, адже вона дозволяє кожному зберігати незалежність, свободу і контроль над своїм життям. Однак у цифрову епоху це поняття набуло нового значення, адже більша частина нашого життя тепер відбувається в інтернеті, де залишаються сліди наших дій, думок і зв'язків.

Іммануїл Кант пропонує філософський підхід, який наголошує на важливості поваги до людської гідності, автономії та права кожного вирішувати, як використовувати свої дані. У цифрову епоху, коли приватність перебуває під загрозою через технології, його ідеї мають ключове значення. Вони допомагають створювати системи, що базуються на принципах моралі, відповідальності та прозорості, які дозволять зберегти фундаментальні права людини в умовах швидкого технологічного розвитку. Автономія є основною умовою моральної дії, і кожна людина має бути здатною діяти відповідно до своїх моральних переконань, а не під зовнішнім тиском [2]. У контексті цифрової епохи це означає, що людина повинна мати контроль над тим, які її дані збираються, як вони використовуються і ким.

Філософські дебати щодо балансу між свободою і безпекою сягають своїм корінням у роздуми про природу держави, суспільства і прав людини. У контексті кібербезпеки ці питання набувають нового виміру, оскільки технології дозволяють досягти безпрецедентного рівня моніторингу і контролю. Ключова моральна дилема тут полягає у питанні: чи виправдане обмеження приватності та свобод заради забезпечення абсолютної кібербезпеки? Хочу розглянути це з позицій різних філософів і їхніх концепцій.

Мілль вважав, що свобода людини повинна обмежуватися лише тоді, коли її дії шкодять іншим. У контексті кібербезпеки це створює кілька важливих дилем: масове стеження, спрямоване на виявлення потенційних загроз, порушує приватність усіх, а не лише тих, хто становить небезпеку. Це означає, що тотальний захист може виходити за межі принципу мінімального втручання; Мілль би закликав до чіткого визначення меж і умов контролю, щоб уникнути ситуації, коли безпека виправдовує необмежене втручання у приватне життя. Міллевий підхід також ставить питання про пропорційність: чи дійсно тотальний захист приносить стільки користі, щоб виправдати масштабні порушення приватності [3]? Ханс Йонас у своїй «Принципі відповідальності» стверджував, що сучасні технології створюють нові ризики, які вимагають

обережного і передбачливого підходу. У контексті кібербезпеки це означає, що: впровадження тотального захисту повинно враховувати не лише короткострокову безпеку, а й довгострокові наслідки для свободи і суспільства; технології масового моніторингу повинні розроблятися з врахуванням моральної відповідальності перед майбутніми поколіннями. Йонас наголосив би на необхідності обмеження технологічного втручання, щоб уникнути дегуманізації суспільства [1]. Кантівська етика заснована на принципі автономії людини і її невідчужуваній гідності. У цьому контексті тотальний захист у кіберпросторі стикається з кількома фундаментальними протиріччями: людина як мета, а не засіб - системи тотального контролю, як-от масове стеження чи аналіз поведінки користувачів, перетворюють людину на об'єкт для досягнення мети - безпеки. Це суперечить категоричному імперативу Канта, за яким до кожної особистості слід ставитися як до самоцінної мети, а не інструменту; порушення автономії - Кант вважав, що моральні рішення мають ухвалюватися вільними і раціональними істотами. Якщо держава чи технології постійно стежать за людиною, це обмежує її автономію і свободу самовираження. Тотальний захист є морально проблематичним, оскільки ставить колективну безпеку вище за індивідуальну свободу і гідність [2].

Тотальний захист у кібербезпеці - це не лише технічне, але й моральне питання. Філософи, від Канта і Мілля до Йонаса, наголошують на необхідності захисту базових прав і свобод людини навіть у контексті глобальних загроз. Моральна дилема полягає у пошуку балансу між безпекою і свободою, між колективним благом і повагою до індивідуальності. Лише етичний, прозорий і відповідальний підхід може забезпечити цей баланс у цифровому світі.

У сфері кібербезпеки найчастіше обговорюють технічні аспекти: системи шифрування, антивірусні програми, алгоритми штучного інтелекту тощо. Проте людський фактор залишається найслабшою ланкою у забезпеченні цифрового захисту. Люди - користувачі, співробітники компаній, навіть фахівці з безпеки - часто допускають помилки, через які зловмисники можуть отримати доступ до конфіденційних даних або систем. Що таке людський фактор у кібербезпеці? Людський фактор - це сукупність дій, рішень, поведінкових моделей і слабкостей, які можуть впливати на ефективність кібербезпеки. Це включає: необережність - наприклад, недбале ставлення до паролів, відкриття сумнівних файлів або посилань; незнання - брак базових знань про кіберзагрози, таких як фішинг чи соціальна інженерія; емоційний тиск - люди можуть піддаватися маніпуляціям, наприклад, діючи в паніці через термінові запити шахраїв.

Кожен користувач має відповідати за свої дії у цифровому просторі, усвідомлюючи, що навіть одна помилка може завдати шкоди багатьом [1]. Компанії повинні забезпечувати належну освіту та умови для дотримання правил, а користувачі мають виконувати свої обов'язки [4]. Свобода людини не повинна шкодити іншим. У контексті кібербезпеки недбалість чи свідома безвідповідальність можуть ставати загрозою для інших людей або організацій [3].

Людський фактор залишається найвразливішою складовою кібербезпеки, навіть за наявності найсучасніших технологій. Подолання цієї проблеми потребує інтеграції технічних рішень, освітніх програм та етичного підходу, який підвищує рівень відповідальності кожної людини за її дії у цифровому світі. Тільки поєднання технологій і свідомої поведінки дозволить досягти високого рівня захисту в умовах зростаючих кіберзагроз.

Тема кібербезпеки набуває особливого значення для нашої краї, оскільки вона перебуває в умовах гібридної війни, де кіберпростір став ключовим елементом сучасного протистояння. Україна вже кілька років є об'єктом кібератак, які використовуються як засіб політичного, економічного та військового тиску. Це робить вивчення та розвиток кіберзахисту життєво важливим для національної безпеки. У цифрових війнах основними засобами боротьби є кібератаки, злам систем, маніпуляція інформацією та використання штучного інтелекту, а головними питаннями стають захист суверенітету, приватності, цивільного населення та відповідальність за наслідки.

Філософи різних напрямків пропонують свої погляди на те, як сформувати етичні принципи для цього нового типу конфліктів. Жан-Жак Руссо, хоча і жив у XVIII столітті, може бути залучений до обговорення етики кіберконфліктів через його ідеї про суспільний договір, природу людини і влади. З погляду Руссо, цифрові війни та кіберконфлікти можуть бути інтерпретовані як прояви порушення суспільного договору та руйнування гармонії між державою, суспільством і особистістю. Суспільний договір забезпечує рівність і свободу громадян в обмін на їхню згоду підкорятися загальній волі. У контексті кіберконфліктів: атаки на критичну інфраструктуру, системи управління чи інформаційний простір підривають засади суспільного договору, оскільки ставлять під загрозу безпеку громадян. Держава, за Руссо, є гарантом загального блага. Її нездатність захистити громадян від кібератак або участь у них є прямим порушенням цього договору. Ідеї філософа допомагають переосмислити цифрові війни з позицій моральної відповідальності, рівності та свободи. Він би наголосив на необхідності формування нового «кіберсуспільного договору», який би регулював поведінку держав, корпорацій і окремих осіб у цифровому просторі. Такий підхід спрямований на уникнення хаосу та забезпечення того, щоб технології служили загальному благу, а не перетворювалися на засіб руйнації [4]. Гайдеггер у своїх дослідженнях техніки зазначав, що технології є не просто засобом, а формою впливу на буття. У кіберконфліктах ця ідея наголошує на небезпеці: дегуманізації війни: застосування кіберзброї робить конфлікти абстрактними, віддаляє агресорів від наслідків їхніх дій, що може сприяти безвідповідальності; контроль техніки: кібервійни демонструють, як техніка може стати інструментом домінування, якщо вона не підпорядкована етичним принципам [5]. Згідно з Кантом, кожна людина повинна розглядатися як цінність сама по собі, а не як засіб досягнення цілей. Ця ідея знаходить застосування у сфері кіберконфліктів: захист цивільного населення: атаки на кіберінфраструктуру, які порушують права людей на приватність чи ставлять під загрозу їхнє життя, є порушенням

принципу автономії; заборона маніпуляції: використання фейкової інформації чи пропаганди для впливу на громадську думку суперечить етичним принципам поваги до людської гідності [2].

Різні філософи пропонують багатовимірний аналіз етики кіберконфліктів, акцентуючи увагу на відповідальності, прозорості, справедливості, захисті цивільного населення та обмеженні шкоди. У сучасному світі їхні ідеї спрямовують розробників і держави до створення таких норм і принципів, які допоможуть уникнути катастрофічних наслідків цифрових воєн і зберегти гуманістичні цінності навіть у новітніх конфліктах.

Якщо підсумувати всі наведені тези, то можна зробити висновок, що філософія пропонує не лише аналіз викликів, але й перспективу для створення справедливих норм поведінки в кіберпросторі. Вона нагадує, що кібербезпека - це не лише про технічні рішення, а й про цінності, які визначають, яким має бути суспільство в умовах цифрової трансформації. Спрямовуючи технології на благо людства, ми можемо забезпечити не лише безпеку, але й етичний розвиток майбутніх поколінь.

Література

1. Ханс Йонас. Принцип відповідальності: Етика для технологічної цивілізації / Дух і Літера. Київ, 2001.

2. Іммануїл Кант. Основи метафізики моральності / Київ: Основи, 2002.

3. Мілль Дж.С. Про свободу / Київ: Основи, 2009.

4. Руссо Ж.-Ж. Суспільний договір / Львів: Апріорі, 2010.

5. Гайдеггер Мартін. Питання про техніку / Львів: Афіша, 1997.

Ability to ask questions as the most important in Aircraft

Vitalii KASHTANOV, student
Mentor – Iryna USHNO, Candidate of Philosophical Sciences, Associate Professor
National Aerospace University «Kharkiv Aviation Institute»

The answer to the questions
that philosophy leaves unanswered
is that they need to be posed
differently.
– Georg Hegel, German philosopher
of the 18th and 19th centuries.

In everyday life, we often encounter misunderstandings. We ask questions that, to us, have one meaning, yet for someone else, the same words carry a different interpretation. Throughout human history, such issues have repeatedly arisen, hindering and continuing to hinder the development of technology, art, business, human relationships, law, and more.

Any invention begins with a question. This question usually serves as the initial idea for a new discovery in the universe of science and technology. A question is an idea or a thought about how to change a particular problem in society or in the specific lives of a group of people. This applies to the development of technology, manufacturing, and so forth. Take cars as an example: if a particular model from an