***Процик Л. С.**, кандидат психологічних наук,*
старший науковий співробітник,
Державний науково-дослідний інститут МВС України

ПСИХОЛОГІЧНІ ТА ПРАВОВІ ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Нині, у процесі загострення глобалізаційних викликів, реалізується впровадження сучасних інформаційних технологій, що призводить до формування нового спектра ризиків і загроз в усіх сферах суспільного життя – економіці, культурі, освіті та практиці. Кібернетичні загрози охоплюють усі базові сфери громадської діяльності (політичну, безпекову, правову, інфраструктурну тощо), впливаючи на складові сектору безпеки і оборони України та на органи державної влади України. Як правило, сучасні заходи кібербезпеки в цифровому середовищі обумовлюються технологічними особливостями та можливостями сучасного кіберпростору, охоплюють як технічні питання захисту інформаційних ресурсів (продуктів/активів), так і майнових прав фізичних та юридичних осіб. Однак, людина вважається найбільш вразливим об'єктом у системі забезпечення безпеки, і ступінь вразливості залежить від багатьох факторів, насамперед, рівня усвідомлення можливих загроз та їх наслідків, обізнаності щодо методів захисту, її характерологічних особливостей і світоглядних позицій, морально-етичних цінностей, сімейних обставин та інших складових. Відповідно, на сучасному етапі розвитку новітніх інформаційних технологій та цифрового середовища актуального значення набуває проблема психологічних та правових особливостей кібербезпеки.

Дослідження особливостей кібербезпеки у цифровому середовищі носять міждисциплінарний характер, які у своїх працях описували такі зарубіжні й вітчизняні вчені: Л. Арсенович, В. Бурячок, Р. Валліс, Д. Вербицький, Н. Громова, І. Діордіца, М. Костікова, О. Литвиненко, С. Мельник, Л. Найдьонова, Р. Покровська, Я. Чаплак, Г. Чуйко, С. Шейбе та інші. Як свідчать останні публікації, потребують подальшого вивчення питання психологічних та правових особливостей кібербезки, які нині є малодослідженими.

Цифрові технології відіграють все важливу в професійному та приватному житті громадян України, а цифрові компетентності стають все більш важливими як для кожної особистості окремо, так і для країни в цілому. *Правову основу кібербезпеки України становлять*: Конституція України, закони України «Про основи Національної безпеки», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші закони, Конвенція Ради Європи про

кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Необхідно зауважити на те, що дія зазначеного Закону не поширюється на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), а також не стосується інформаційно-телекомунікаційних систем, в яких циркулює інформація, яка складає державну таємницю.

Відповідно до «Концепції розвитку цифрових компетентностей в суспільстві України» та плану заходів щодо її реалізації, яку 3 березня 2021 року своїм розпорядженням схвалив Кабінет Міністрів України *цифрове середовище* – це середовище, що охоплює інформаційно-комунікаційні технології, включаючи Інтернет, мобільні та пов'язані з ними технології та пристрої, а також цифрові мережі, бази даних, контент та послуги, та яке використовується для взаємодії з іншими користувачами та доступу та публікації створеного контенту. Однак цифрове середовище надає нам не тільки ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти.

Варто відзначити, що розвиток законодавства в сфері кібербезпеки в Україні безпосередньо пов'язаний з євроінтеграційними прагненнями України та розвитком правового регулювання електронної комерції в межах СОТ. Одним з ключових чинників, що сприяє попередженню кібератак є ефективна система захисту та жорстка система покарань кіберзлочинців, наприклад, така як існує у США. Національна система кібербезпеки представляє собою комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами та Національним банком України.

Забезпечення безпеки в кіберпросторі не вичерпується заходами державного регулювання і контролю, а в багатьох випадках залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема, суб'єктів господарювання. Через низьку медіаграмотність та відсутність цифрової культури постійно збільшується частка населення, яка не вміє протистояти пропаганді, маніпуляціям та шахрайству в цифровому середовищі, не бачить загроз та не вміє захистити власні інтереси.

В одному з досліджень Cyber Security Intelligence Index компанії IBM йдеться про те, що особистісний чинник є причиною практично 60% усіх кібератак у сфері бізнесу. За даними дослідження Positive Technologies у 57% випадків основним засобом реалізації кібератак на компанії (57%) є *соціальна інженерія* – отримання доступу до конфіденційної інформації, паролів, банківських даних та інших захищених систем, базуючись на психологічних особливостях людей. Якщо говорити про напади, спрямовані на фізичних осіб, то частка соціальної інженерії сягає 90%. Більшість випадків кібератак орієнтовані на непідготовленого користувача, який не знайомий з *базовими правилами кібербезпеки*. Ці правила *включають в себе*: розпізнавання фішингових листів, заборону на перехід за незнайомими посиланнями, самостійне встановлення програмного забезпечення з неперевірених джерел, завантаження невідомих файлів та добровільну передачу особистих даних в Інтернеті тощо. Саме такі, на перший погляд, прості дії можуть захистити від великомасштабних атак та блокування доступу до систем [1].

Відповідно актуальним є формування *цифрової компетентності*, яка включає в себе впевнене, критичне та відповідальне використання і взаємодію з цифровими технологіями для навчання, роботи та участі у суспільному житті. Охоплює такі поняття як інформаційна грамотність та медіаграмотність, комунікація та співпраця, створення цифрового контенту (включаючи програмування), безпека (включаючи захист персональних даних у цифровому середовищі та кібербезпеку), а також розв'язання різнопланових проблем і навчання протягом життя. Найважливішим вмінням в цифровій компетентності є критичне мислення або можливість уникати хибних суджень про те, що ми знаходимо в Інтернеті. *Психологічні засоби,* які сприятимуть формуванню культури кібербезпеки у цифровому середовищі, можна згрупувати в залежності від масштабу реалізації, починаючи з національних, суспільних, групових та переходячи до індивідуальних звичок і когнітивних навичок.

Складові культури кібербербезпеки визначені у Резолюції Генеральної Асамблеї ООН, у якості найбільш вагомих із психологічної аспекту виділимо:

- *обізнаність* – учасники повинні бути інформовані про ризики та необхідність забезпечення кібербезпеки, а також про свої можливості у підвищенні стану захищеності;

- *відповідальність* – учасники відповідають за безпеку інформаційних систем та мереж згідно зі своєю роллю в системі кібербезпеки;
- *реагування* – учасники повинні вживати своєчасні і спільні заходи щодо попередження інцидентів, які стосуються кібербезпеки, їх виявленню і реагування на них;
- *переоцінку* – учасники повинні піддавати оцінюванню стан забезпечення кібербезпеки та вносити належні зміни в політику, практику, заходи і процедури забезпечення кібербезпеки, враховуючи при цьому появу нових і зміну колишніх загроз і чинників уразливості;
- *етику* – учасники повинні враховувати законні інтереси інших і визнавати, що їхні дії або бездіяльність можуть зашкодити іншим [2].

У свою чергу, цифрове середовище стає сьогодні реальною сферою життєдіяльності особистості, в певних випадках, кардинально змінюючи багато чого в ній самій – коло інтересів, спілкування, стиль, звички, образ життя в цілому тощо. Тобто, медіанасичене інформаційне середовище сьогодні відіграє неабияке значення у формуванні особистості. Саме ж Інтернет-середовище є невід'ємним структурним елементом сучасних інформаційних технологій в цілому та здобуває з кожним роком все більшу популярність серед різних верств населення. Технологічний прогрес кіберпростору зумовив зміни в інформаційно-комунікативних засобах і до утворень в різновидах розумової діяльності людини. Еволюційний період зміни свідомості людини сьогодні в самому розпалі, але особистість ще не дійшла до відповідного рівня розвитку, щоб в результаті хаотизації інформаційних потоків на достатньому (безпечному) рівні вміти трансформувати свій когнітивно-стратегічний потенціал і встигати займатися ефективною обробкою інформації за досить короткий проміжок часу, що, в свою чергу, надає можливість застосовувати маніпулятивні технології впливу на індивідуальну та соціальну свідомість з метою створення чи поглиблення суспільних криз [3].

Таким чином, безпека особистості в цифровому середовищі – це вже новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. Кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист особистості в IT-полі. Адже розвиток інформаційних технологій, особливо цифровізація суспільного життя, ставить гостро на порядок денний питання захисту інформаційних прав та забезпечення безпеки людини. Відповідно для безпеки особистості в цифровому середовищі необхідно сприяти підвищенню рівня обізнаності населення щодо необхідності особистої кібербезпеки, розвивати інформаційну грамотність, критичне мислення та уміння працювати з даними. Також конструктивне вирішення проблеми безпеки особистості в цифровому середовищі ґрунтується

на удосконаленні нормативно-правового регулювання діяльності в кіберпросторі, встановленні відповідальності за злочини, скоєні в цифровому середовищі.

Перспективами подальших досліджень є визначення психологічних й організаційних основ побудови системи кібербезпеки суб'єктів наукової та науково-технічної діяльності.

Список використаних джерел:

1. Кібербезпека: міфи та реальність. Metinvest Digital. URL: https://metinvest.digital/ua/page/k-berbezpeka-m-fi-ta-realn-st

2. Довгань О. Д., Тарасюк А. В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності. «Інформація і право». № 2(25)/2018. С. 51-61. DOI: https://doi.org/10.37750/2616-6798.2018.2(25).270716

3. Чаплак Я.В. Кліпова хаотичність як засіб абсурдизації та маніпулятивна технологія. Психологічний часопис : збірник наукових праць / за ред. С.Д. Максименка. № 4. Том 14. К.: Інститут психології імені Г.С. Костюка Національної академії педагогічних наук України, 2018. С.19-36. URL: https://doi.org/10.31108/2018vol14iss4pp19-36