системі або зараження вашого пристрою шкідливим програмного забезпечення через неправильне посилання під час перегляду веб-сторінок або електронної пошти.

Прогрес цифрової трансформації неминуче спричинив нові загрози кібербезпеці. Існує критична потреба в забезпеченні надійної інформаційної безпеки в країні. В той час як в контексті ескалації конфлікту в Україні потреба в забезпечення воєнноінформаційної безпеки стала найбільш актуальною за всі останні роки.

1. Про інформацію: Закон України від 02.10.1992 р. Відомості Верховної Ради України. 1992. № 48. С. 650.

2. Конституція України: Закон України від 08.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

3. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки». 2021. № 685/2021.

4. Гребенюк А. М. Кіберзлочинність в Україні. Економічна та інформаційна безпека: актуальні питання та інновації: матер. Міжнар. наук.-практ. конф. (м. Дніпро, 4 листопада 2021 р.). Дніпро : ДДУВС, 2021. С. 85-88.

УДК 004
DOI: 10.31733/17-03-2023-530-532

Наталія КОМИХ
доцент кафедри гуманітарних дисциплін
та психології поліцейської діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат соціологічних наук

АКТУАЛЬНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В УКРАЇНІ ПІД ЧАС ВІЙНИ

Сучасний розвиток глобального суспільства визначається стрімким прогресом цифрових технологій. Інтернетизація, цифровізація, штучний інтелект є невід'ємною складовою сучасних реалій та буденного життя людини. Зазначені процеси набули інтенсивності за часів пандемії COVID-19. Фактично соціальна реальність в якій існує сучасний індивід розділилась на дві: об'єктивну та віртуальну, доповнену. Ці реальності тісно переплетені і потужно впливають на характер соціальних процесів, форми соціальної взаємодії.

В публічному та, подекуди, в науковому дискурсі віртуальну реальність, віртуальний простір часто синонімічно називають кіберпростором. Підтвердження думки знаходимо в Законі України «Про основні засади забезпечення кібербезпеки України», згідно якого, кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [3].

В кіберпросторі на сьогодні поширенні численні загрози: кібератаки на державні та недержавні структури та установи, підприємства, маніпуляції, дезінформація, пропаганда фізичного чи сексуального насильства, екстремістської діяльності, поширення заборонених чи обмежених до продажу товарів, кіберпереслідування, кіберзлочинність, кібершахрайство, надмірне використання екранного часу, пропаганда суїцидів чи доведення до самогубства. А існування чорного ринку – darknet, вже визнано правоохоронцями, та посилило продаж наркотиків, зброї та інших нелегальних товарів та послуг. Фахівці з інформаційних технологій всього світу погодились з тим, що кіберзлочинність – це загроза, яка набуває стрімкого зростання.

Найрозповсюдженими на сьогодні формами кіберзлочинності в світі, на думку швейцарської дослідниці Кавелті Маріам є:

– кібервандалізм – знищення змісту сайту, відключення або перезавантаження серверу;

– інтернет-злочини (діяльність переважно з метою отримання прямого фінансового зиску від такої діяльності), може включати як злочини з комп'ютерної техніки,

так і суто комп'ютерні злочини);

– кібершпигунство – жертвою стає корпоративний сектор, урядові мережі;

– кібертероризм – незаконні напади з боку недержавних суб'єктів стосовно комп'ютерів, мереж та інформації, що міститься в них, які здійснюються для залякування уряду (чи населення) чи з метою досягнення певної поведінки суб'єкта, який залякується;

– кібервійна [4].

Зараз в України відбувається кібервійна. Для українського суспільства кіберпростір став місцем розгортання гібридної війни. Кібератаки на державні установ, організації, фінансові структури відбуваються щоденно.

За даними Державної служби спеціального зв'язку та захисту інформації України зафіксовано 1123 кібератаки за шість місяців повномасштабного вторгнення. Вони спрямовані

на всі сектори економіки України, включно з ІТ та телекомунікаціями. Серед основних секторів, що були атаковані агресором є: уряд і місцеві органи влади, сектор безпеки і оборони, комерційні організації, фінансовий сектор. Найпоширенішими методами кібератак були і є: збір інформації зловмисником, шкідливий програмний код, втручання, відома вразливість. І це підтверджує факт, що кібератаки є повноцінною реальністю війни [1]. На жаль, саме війна є каталізатором та простором можливостей, умовою для посилення кіберзлочинності завдяки випробуванням та застосуванням інноваційних технологій, штучного інтелекту.

За таких умов потужного значення набуває проблема кібербезпеки вирішення якої відбувається на національному, державному рівні в формі діяльності потужних інституційних організацій, які здатні забезпечити захист та контроль кіберпростору. Маємо дієву структуру Державну службу спеціального зв'язку та захисту інформації України, яка тісно співпрацює з Міжнародними структурами кіберзахисту. У липні минулого року було підписано Меморандум про взаєморозуміння між Держспецзв'язком та Урядовим офісом Республіки Словенії інформаційної безпеки у сфері зайнятості та з Агентством кібербезпеки інфраструктури Департаменту національної безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки. Тісне співробітництво у сфері кібербезпеки відбувається з Республікою Польща [1].

З початку війни Служба не тільки активно співпрацює з органами влади та представниками критичної інфраструктури, а і з простими громадянами – через соціальні мережі надає інструкції з розпізнання та запобігання кібератакам. Суб'єктами національної системи кібербезпеки є також Міністерство оборони України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Координує діяльність цих структур Рада національної безпеки і оборони України.

Не менш важливим для держави є підготовка та прийняття потужного законодавчого супроводу для забезпечення прав та можливостей індивіда у віртуальному просторі та врегулювання відносин всіх учасників взаємодії. Правове підгрунтя інформаційної безпеки в Україні створюють Конституція України, закони України «Про засади забезпечення кібербезпеки України», «Про інформацію», «Про національну безпеку України». Згідно зазначених законодавчих документів чітко зазначається, що кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства і держави під час використання кіберпростору. Водночас, кіберзахист – це сукупність правових, організаційних, інженерно-технічних заходів, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків. А кіберзлочин – це винне, небезпечне діяння в кіберпросторі, передбачає кримінальну відповідальність згідно Закону України про кримінальну відповідальність [3].

Не менш важливим аспектом кіберзахисту є дотримання громадянами власної інформаційної безпеки. Особливо це стосується працівників державних установ, підприємств критичної інфраструктури. Кожен повинен дбати про власну кібербезпеку і розуміти, що може стати точкою входу для подальшої кібератаки. Сприйняття формуванню культури взаємодії в кіберпросторі, що передбачає знання та компетенції з інформаційної гігієни, фактчекінгу має бути першочерговим завданням для закладів освіти всіх рівнів. Сучасний індивід має знати основні правила: користуватися ліцензійним програмним забезпеченням; не повідомляти стороннім особам персональні дані, дані та паролі доступу до банківських карток і систем; не завантажувати та не відкривати підозрілі комп'ютерні файли; не довіряти повідомленням у месенджерах або sms про виграші та акції сумнівного походження; користуватися антивірусом.

Так, наприклад, з початком повномасштабного вторгнення росії, Держспецзв'язком було створено телеграмканал Кібер Армія України [2]. Метою каналу є надання громадянам інформацію про те, як захиститися від кібератак рашистів. Було надано адреси чатботів, наприклад Кіберполіції та інших служб, куди можна повідомити про загрози, а також про важливі застосунки, які можна використовувати для унебезпечення особи. Так, було повідомлено, що за підтримки Служби безпеки України було створено додаток (YouControl: «Ти хто?») для перевірки підозрілих осіб, щоб не потрапити до диверсанта чи на підозрілу людину. Завдяки додатку можна перевірити дійсність фото з паспорта, перебування людини у державному розшуку та іншу інформацію [2].

Отже, проблеми кібербезпеки та кіберзахисту не зводяться до вирішення винятково технічних аспектів функціонування кіберпростору. Необхідно звертати на такі види захисту як правові, технічні, психологічні, інформаційні та організаційні. Особливо відкритим для громадян є питання самозахисту від кіберзлочинів. А отже, є нагальною потреба у формуванні культури кібербезпеки. Зокрема, закладам освіти, перш за все, потрібно переорієнтуватися на обов'язкове формування культури поведінки у кіберпросторі. Адже, соціалізація сучасного індивіда ускладнюється тим, що потрібно засвоювати певні соціальні норми та правила поведінки, цінності віртуального середовища, формування та набуття сталості яких відбувається тут і зараз.

1. Війна в Україні. Пульс кіберзахисту, серпень 2022. URL: https://www.ppl.org.ua/wp-content/uploads/2022/09/1662392024242416.pdf.

2. Кібер Армія України. URL: https://t.me/CyberArmUA.

3. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради. 2017. № 45. Ст. 403. URL: https://ips.ligazakon.net/document/TM059780.

4. Cavelty M. D. Cyberwar: concept, status quo, and limitations. URL: https://www.academia.edu/1058235/Cyberwar_Concept_Status_Quo_and_Limitations.

УДК 004
DOI: 10.31733/17-03-2023-532-534

Олександр КОСИЧЕНКО
доцент кафедри інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПРОБЛЕМИ БЕЗПЕКИ, ПОВ'ЯЗАНІ З МЕТАДАНИМИ ДОКУМЕНТІВ

Метадані – це дані про дані, інформація про інформацію. Іншими словами – це інформаційно-технічна інформація, що міститься в документах різних форматів, яку не видно при звичайному використанні. Метадані нерідко поміщаються у документ програмним чи апаратним засобом, з якого документ було створено. Так як цей процес автоматизований, користувач може залишатися необізнаним про наявність таких даних, і не вживати заходів для захисту цієї інформації, що нерідко має особливе значення.

Серед типів документів, що містять метадані – документи MS Office, Adobe PDF, Corel Word Perfect, зображення, створені Corel DRAW, Adobe Photoshop, створені або оброблені різними редакторами растрової графіки GIF і JPEG, аудіофайли MP3, відео файли, веб-сторінки, електронні листи.

Це найбільш поширені формати, які використовуються на різних офісних платформах
у повсякденній діяльності.

Метадані можуть включати ім'я автора документа, організацію, мітку програмного або апаратного засобу, історію модифікацій документа і так далі. В особливо складних випадках (MS Word) це може бути навіть текст, який колись входив у документ, але пізніше віддалений, але зберігається у файлі документа у вигляді метаданих. Метадані можуть також бути присутніми і у вихідному коді прикладних програм у вигляді коментарів