УДК 004
DOI: 10.31733/17-03-2023-529-530

Андрій ГРЕБЕНЮК
завідувач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук

БЕЗПЕКОВІ ІНФОРМАЦІЙНІ ЗАГРОЗИ В УМОВАХ ВОЄННОГО СТАНУ

Вторгнення росії в Україну супроводжувється кібератаками, спрямованими на інфраструктуру країни, включаючи DDoS-атаки та руйнівні кампанії зі зловмисного програмного забезпечення. Також країна агресор почала використовувати інформацію як зброю, охопивши до цього недоступні засоби для завдання значної шкоди нашій країні. Так, використовуючи інформаційний вплив, маніпуляцію, пропаганду та інші інформаційні компанії.

Стаття 17 Конституції України 10 свідчить: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу…. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом» [2].

Отже для цивільної особи, яка здійснюють власні спроби зламу, атак на підприємства та іншу інфраструктуру ворожої країни можуть мати несподівані наслідки. І ці наслідки залежать від того як країни відносяться до хакерів та яке в них законодавство. Тому залучання цивільних навіть задля захисту держави потрібно зі зміною законодавства, щоб люди розуміли що вони потрібні державі, а вони зі свого боку робитимуть все для захисту держави на кіберфронті.

В Законі України «Про інформацію» «встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації» [1].

Звичайно що, закон не стоїть на місці, а постійно адаптується під нові обставини, умови та, безумовно, технології, які охоплюють усі сфери зокрема безпекові. Так, відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [3-4].

З введенням в нашій державі військового стану в зв'язку з агресією сусідньої держави та переміщенням значної кількості населення, яке залишило оргтехніку в квартирах офісах не в змозі забрати інформацію якою потім використали спецслужби окупантів.

Ось чому нас шокує той факт, наскільки напрочуд легко кіберзлочинцям отримати доступ до особистих даних на вашому мобільному телефоні. Телефони можуть бути скомпрометовані різними способами, ось деякі з них: доступ до вашої особистої інформації через загальнодоступний Wi-Fi, впровадження жучка, використання помилки в операційній

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,