УДК 342.72
DOI https://doi.org/10.32837/yuv.v0i2.1701

Ю. Хоббі,
кандидат юридичних наук,
доцент кафедри юридичних дисциплін
Донецького юридичного інституту Міністерства внутрішніх справ України

ПРАВО ЛЮДИНИ НА КІБЕРБЕЗПЕКУ: ПРОБЛЕМИ ВИЗНАЧЕННЯ ТА ГАРАНТУВАННЯ

Ми живемо в цифровому світі, де кіберзагрози й кібератаки стають усе частішим явищем. Ще 10 років тому було важко уявити, що покупки, банківські операції, спілкування, навіть робота й навчання може вміститись в одному смартфоні. Сучасні інформаційні технології відкривають значні можливості, але одночасно підвищують рівень незахищеності людини та її прав і свобод у кіберпросторі. Права людини стають найбільш проблемною сферою захисту, оскільки не всі усвідомлюють значимість кібербезпеки, про що свідчать значні прогалини в законодавстві, його відставання від нових технологій та можливостей використання мережі «Інтернет» і відсутність уніфікованих правил, які застосовуються в разі кібератаки. Тому право на кібербезпеку посідає особливе місце, оскільки воно зумовлює всі інші права, реалізація яких перейшла в кіберпростір.

Дослідженням проблем гарантування кібербезпеки держави займались О.О. Бакалінська, В.А. Ліпкан, І.В. Тімкін, Н.Є. Новіков, І.В. Діордіца, С.В. Мельник, О.М. Супрун та інші. Проте гарантування кібербезпеки як права людини майже не досліджувалось.

Тому метою статті є дослідження права людини на кібербезпеку як одного з інформаційних прав людини, для чого пропонується авторське визначення права на кібербезпеку й визначення проблем його гарантування.

Для того, щоб з'ясувати, чи можна віднести право на кібербезпеку до інформаційних прав людини, розглянемо, що таке кібербезпека та право на кібербезпеку.

Часто кібербезпеку та інформаційну безпеку ототожнюють, але це різні поняття. Відповідно до ст. 1 Закону України «Про основні засади гарантування кібербезпеки України» кібербезпека розуміється як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [1].

Необхідно зауважити те, що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги, пов'язані зі змістом інформації, яка обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі «Інтернет» (включно з блог-платформами, відеохостингами, іншими веб-ресурсами), а також не стосується інформаційно-телекомунікаційних систем, у яких циркулює інформація, яка становить державну таємницю [2, с. 103].

Зі свого боку, інформаційна безпека розуміється як стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запо-

бігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, котра використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації (ст. 13 Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки) [3].

Проаналізувавши ці два визначення, можна зробити висновок, що інформаційна безпека здебільшого стосується захисту саме інформації та доступу до неї, а кібербезпека – захисту прав і свобод людини під час використання кіберпростору, водночас це стосується не лише інформаційних прав.

Варто також додати, що гарантування кібербезпеки має базуватись на принципах верховенства права й поваги до прав та свобод людини і громадянина (ч. 10 Розділ 1 Стратегії кібербезпеки України) [4].

З огляду на вищевикладене *право на кібербезпеку* можна розглядати як невід'ємне, невідчужуване право особи на захищеність її важливих інтересів, зокрема й інформаційних прав, під час використання кіберпростору. Тобто право на такий правопорядок, за умов якого забезпечуються, охороняються й захищаються права і свободи людини під час використання кіберпростору.

Хоча право на кібербезпеку зачіпає всі права особи, але ми вважаємо доцільним віднести його саме до інформаційних прав, які в сучасних реаліях необхідно трактувати дещо ширше, ніж просто доступ до інформації та її захист.

Чинне законодавство до інформаційних прав відносить лише деякі. Так, згідно з Конституцією України, до інформаційних прав відноситься таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31); захист особистого та сімейного життя шляхом недопущення збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім окреслених у законі випадків, право спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної й моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (ст. 32); право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб (*через соціальні мережі та інтернет – Ю. С.*) – на свій вибір (ст. 34) [5].

Відповідні положення містить і Закон України «Про інформацію», ст. 5 якого гарантує кожному право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та *захисту інформації* (*курсив наш – Ю. С.*), необхідної для реалізації своїх прав, свобод і законних інтересів [6]. Додатково ч. 1 ст. 7 цього Закону передбачає, що держава гарантує всім учасникам інформаційних відносин рівні права й можливості доступу до інформації. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Ці положення здаються дещо застарілими в сучасних реаліях, тому їх необхідно переглянути, враховуючи модернізацію способів та засобів одержання, поширення, зберігання та захисту інформації. Саме захисту держави в особі її органів варто приділити значну увагу й не лише тієї інформації, яка циркулює в державних комунікаційних системах та системах автоматизованої обробки даних, а і приватної. Цього можна досягти через захищеність цих систем, боротьбу з розповсюдженням шкідливого програмного забезпечення і програм, контенту, інтернет-шахрайством та оперативним реагуванням правоохоронних органів на факти кібератак не лише на життєво важливі сис-

теми, а й на приватні технічні засоби комунікації.

Про відставання національного законодавства свідчить і те, що ООН визнала право на доступ до мережі «Інтернет» одним із невід'ємних прав людини. Зазначена позиція ООН відображена в резолюції Ради із прав людини від 5 липня 2012 року про право на свободу слова в інтернеті [7]. Право на доступ до інтернету передбачає, що всі люди повинні мати можливість доступу до мережі «Інтернет» із метою здійснення й користування своїми правами на свободу висловлення думки, переконань та інших основних прав людини. Держава повинна нести відповідальність за те, щоб доступ до інтернету був широкодоступним. Держави не можуть необґрунтовано обмежувати доступ індивідів до інтернету. І вже кілька держав унесли відповідні зміни у своє законодавство, на відміну від України [8]. Резолюція, звісно, носить рекомендаційний характер, але відповідає вимогам сучасності, й нашій державі варто взяти це до уваги, оскільки інтернет є зараз основним джерелом як доступу до інформації та обміну нею, так і загроз правам людини.

У 2015 році до Верховної Ради України було додано законопроєкт про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до інтернету) № 2849, який пропонував доповнити Цивільний кодекс України ст. 302-1. (Право на доступ до інтернету), але у 2019 році він був відкликаний [9].

Це далеко не вичерпний перелік інформаційних прав людини, оскільки більшість інших прав також пов'язані з інформацією та доступом до неї, зокрема через мережу «Інтернет». Та необхідно наголосити, що реалізація цих прав можлива лише в умовах інформаційної та кібернетичної безпеки й відповідного захисту, як індивідуального, так і з боку держави та її органів, зокрема і правоохоронних.

Ураховуючи вищезазначене, право людини на кібербезпеку можна віднести до інформаційних прав, оскільки кіберпростір зараз розглядається як окрема (поряд із традиційними «Земля», «Повітря», «Море» та «Космос») сфера ведення бойових дій, де головну роль відіграє інформація, зокрема й персональні дані.

Важливою умовою реалізації цього права є як нормативне закріплення та регулювання, так і захист, зокрема кіберзахист. У цьому напрямі Україна ратифікувала Конвенцію Ради Європи «Про кіберзлочинність» 2001 року, затвердила Стратегію кібербезпеки України 2016 року і прийняла Закон України «Про основні засади гарантування кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Але проблема цих нормативних актів полягає в тому, що вони носять формальний характер і встановлюють лише загальні положення без практичного наповнення.

Так, Закон України «Про основні засади гарантування кібербезпеки України» визначає правові та організаційні основи гарантування захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основна мета, 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 з гарантування кібербезпеки. Але він не містить практичних механізмів реалізації цих положень.

Хоча п. 7. ст. 1 цього Закону містить визначення кіберзахисту як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем [1]. Цікавим є те, що до об'єктів кібербезпеки Закон відносить конституційні права і свободи

людини і громадянина (п. 1. ч. 1 ст. 4). Однак до об'єктів кіберзахисту відносить лише:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, котрі використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного врядування, електронних державних послуг, електронної комерції, електронного документообігу (ч. 2 ст. 4). Бачимо, що об'єктом кіберзахисту права і свободи не є, натомість є об'єкти критичної інформаційної інфраструктури, визначення яких у Законі надається, а ось переліку немає.

Кабінет міністрів України своєю Постановою від 23 серпня 2016 року № 563 затвердив «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [10], але й тут чіткого переліку немає, лише зазначається, що інформація, яка міститься в переліку, є інформацією з обмеженим доступом. А з огляду на ч. 5 п. 2 цього Переліку об'єктом критичної інфраструктури можуть бути підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, котрі є стратегічно важливими для функціонування економіки й безпеки держави, суспільства та населення [10].

Необхідно додати, що до Верховної Ради України було внесено «Проєкт Закону про критичну інфраструктуру та її захист» № 10328 від 27.05.2019, ст. 9 якого містила критерії віднесення об'єктів до критичної інфраструктури, й навіть установлювались категорії критичності (ст. 10). А ст. 11 регулювала складення та ведення Національного переліку об'єктів критичної інфраструктури Уповноваженим органом у сфері захисту критичної інфраструктури [11]. Але вже в серпні 2019 року він був відкликаний. Тому питання про перелік об'єктів критичної інфраструктури та відповідального органу за його ведення залишається відкритим.

Таким чином, права і свободи людини і громадянина, зокрема й щодо кібербезпеки, під кіберзахист не підпадають. Єдине, що п. 3. ч. 2. ст. 2 Закону України «Про основні засади гарантування кібербезпеки України» до принципів застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону відносить гарантування захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання у приватне життя й захисту персональних даних [1].

Також варто зазначити, що, відповідно до Розділу 3 Стратегії кібербезпеки України, саме на Національну поліцію України покладається обов'язок гарантування захисту прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [4].

Із цією метою, відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого наказом Національної поліції від 10.11.2015 № 85, було створено Департамент кіберполіції Національної поліції України як міжрегіональний територіальний орган Національної поліції України, який, відповідно до законодавства України, забезпечує

реалізацію державної політики в галузі протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції. Одним із завдань департаменту є забезпечення своєчасного розгляду звернень та запитів громадян, підприємств, установ, організацій із питань, віднесених до компетенції кіберполіції, контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку й розгляду. Також кіберполіція має проводити серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті [12], але в якій формі це має відбуватись, не зрозуміло.

Тобто теоретично за реалізацією свого права на кібербезпеку та захист можна звертатись до цього Департаменту, але до його функцій не входить безпосередньо гарантування кібербезпеки громадян, а лише попередження, виявлення та припинення кримінальних правопорушень у галузі протидії кіберзлочинності.

Ураховуючи вищенаведене, можна дійти таких висновків:

1) право на кібербезпеку можна розглядати як невід'ємне, невідчужуване право особи на захищеність її важливих інтересів, зокрема й інформаційних прав, під час використання кіберпростору;

2) право на кібербезпеку можна віднести до інформаційних прав людини, оскільки кіберпростір розглядається як окрема сфери протиборства і складається з інформації;

3) серед проблем забезпечення цього права необхідно зазначити відсутність нормативно-правового визначення, застарілість законодавства в інформаційній сфері та здебільшого декларативність положень новітнього законодавства без практичного складника їх реалізації, невизначеність органу, на який би покладався обов'язок забезпечення права особи на кібербезпеку й кіберзахист, оскільки Національна поліція та її спеціалізовані підрозділи підключаються тільки на стадії встановлення факту кіберзлочину.

У статті досліджено кібербезпеку як складник інформаційних прав людини. Проаналізовано основне законодавство України у сфері кібербезпеки, на підставі чого зроблено висновок, що кібербезпека – це наступний рівень інформаційної безпеки. Оскільки інформаційна безпека здебільшого стосується захисту саме інформації та доступу до неї, а кібербезпека – захисту прав і свобод людини під час використання кіберпростору.

Надано авторське визначення права на кібербезпеку як невід'ємне, невідчужуване право особи на захищеність її важливих інтересів, зокрема й інформаційних прав, під час використання кіберпростору. Тобто право на такий правопорядок, за якого забезпечуються, охороняються й захищаються права і свободи людини під час використання кіберпростору.

Пропонується віднести право на кібербезпеку до інформаційних прав людини, але за умов перегляду переліку та змісту цієї категорії прав у національному законодавстві, оскільки чинні нормативно-правові акти не відповідають сучасним реаліям.

На підставі аналізу законодавства у сфері кібербезпеки зроблено висновок, що конституційні права і свободи людини і громадянина, зокрема й інформаційні, розглядаються лише як об'єкт кібербезпеки, а не об'єкт кіберзахисту. До останніх відносять об'єкти критичної інфраструктури, чіткого переліку яких чинні нормативно-правові акти не містять, і не встановлено орган, котрий має відповідати за ведення цього переліку.

Наголошується, що реалізація права на кібербезпеку можлива лише за умов відповідних змін до законодавства в інформаційній сфері та визначеності державного органу, на який би покладався обов'язок гарантування права особи на кібербезпеку й кіберзахист, оскільки Національна поліція та її спеціалізовані підрозділи підключаються лише на стадії встановлення факту кіберзлочину.

Ключові слова: інформаційні права, кібербезпека, кіберзахист, об'єкт критичної інфраструктури, право на кібербезпеку, кіберполіція.

Khobbi Yu. The human right to cybersecurity: problems of definition and ensuring

The article considers cybersecurity as a component of information human rights/ The main legislation of Ukraine in the field of cybersecurity is analyzed and it is concluded that cybersecurity is the next level of information security. Since information security mainly concerns the protection of information and access to it, and cybersecurity concerns the protection of human rights and freedoms when using cyberspace.

The author's definition of right to cybersecurity as an inalienable human right to protection of his important interests, including information rights, when using cyberspace. That is, the right to such a rule of law, under which human rights and freedoms are ensured, guarded and protected during the use of cyberspace.

It is proposed that right to cybersecurity be classified as information human rights, but subject to revision of the list and content of this category of rights in national legislation, since the current regulations do not correspond to modern realities.

Based on the analysis of cybersecurity legislation, it is concluded that the constitutional rights and freedoms of man and citizen, including information, are considered only as an object of cybersecurity, and not an object of cyberdefence. The latter include objects of critical infrastructure, a clear list of which is not contained in the current regulations and there is no established body that could be responsible for maintaining this list.

It is emphasized that the realization of right to cybersecurity is possible only with appropriate changes to the legislation in the field of information and cybersecurity and the determination of the state body that would be responsible for ensuring the individual's right to cybersecurity and cyberdefense, as the National Police and its specialized units are involved only at the stage of establishing the fact of cybercrime.

Key words: information rights, cybersecurity, cyberdefense, object of critical infrastructure, right to cybersecurity, cyberpolice.

Література

1. Про основні засади гарантування кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.05.2020).

2. Бакалінська О.О., Бакалинський О.О. Правове гарантування кібербезпеки в Україні. Підприємство, господарство і право. 2019. № 9. С. 100–108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf).

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січня 2007 року № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16?find=1&text=інформаціна+безпека (дата звернення: 12.05.2020).

4. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 27.05.2020).

5. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 15.05.2020).

6. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII. URL:

https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 12.05.2020).

7. Резолюция Совета ООН по правам человека A/HRC/20/L.13 от 29.06.2012 г. URL: https://undocs.org/ru/A/HRC/20/L.13 (дата звернення 26.05.2020).

8. Право на интернет-доступ. URL: https://ru.wikipedia.org/wiki/Право_на_интернет-доступ (дата звернення: 12.05.2020).

9. Проєкт Закону про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до інтернету) № 2849 від 14.05.2015. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2849&skl=9 (дата звернення: 1.06.2020).

10. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Кабінету міністрів України від 23 серпня 2016 р. № 563. URL: https://zakon.rada.gov.ua/laws/show/563-2016-n (дата звернення: 01.06.2020).

11. Проєкт Закону про критичну інфраструктуру та її захист № 10328 від 27.05.2019. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1? pf3511=65996 (дата звернення: 29.05.2020).

12. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10 листопада 2015 року № 85. URL: http://tranzit.ltd.ua/nakaz/ (дата звернення: 01.06.2020).