виявляти і блокувати бот-мережі та фейкові акаунти, які використовуються з такою метою. Також вкрай важливо оперативно реагувати на кібератаки проти органів державної влади та ЗМІ, не дозволяючи зловмисникам досягти своїх цілей.

Зокрема, уваги потребує захист персональних даних громадян від витоків та кібератак. Адже в умовах хаосу зростають ризики незаконного збору та використання особистої інформації для шахрайських, пропагандистських чи інших цілей. Держава має убезпечити бази персональних даних, а громадян просвітити щодо цифрової гігієни та захисту приватності.

Окремого значення набуває посилення боротьби з кіберзлочинністю, що завжди активізується в умовах хаосу. Необхідно жорстко протидіяти різноманітним проявам шахрайства в мережі, крадіжкам грошей із банківських рахунків, поширенню шкідливого програмного забезпечення тощо. Адже такі дії підривають довіру громадян до цифрових технологій. Пов'язаність вчинення кіберзлочину з комп'ютерною технікою та інформаційними технологіями дає змогу розглядати як кіберзлочини як усі види злочинів, що можуть бути вчинені з її використанням, так і лише ту групу злочинів, що безпосередньо визначена у КК України саме як кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку [3].

Для ефективного забезпечення кібербезпеки вкрай важливу роль відіграє співпраця держави, ІТ-компаній та небайдужих громадян. Залучення фахівців ІТ-сфери допоможе посилити кіберзахист на технологічному рівні. А інформування та освіта населення щодо цифрової безпеки зменшать ризики уразливості перед кіберзагрозами. Тільки об'єднавши зусилля, можна забезпечити надійний захист кіберпростору України.

Також дуже важливо налагодити конструктивну співпрацю на міжнародному рівні, зокрема з країнами НАТО та ЄС. Адже глобальні виклики вимагають глобальної координації та об'єднання зусиль у сфері кібербезпеки. Спільними силами можна досягти значно більшого результату у протидії кіберзагрозам, ніж поодинці.

Отже, забезпечення надійної кібербезпеки в умовах воєнного стану потребує комплексу заходів як на державному рівні, так і на рівні бізнесу та суспільства. Лише об'єднавши зусилля та убезпечивши ключову інфраструктуру, дані та системи, можна гарантувати цифровий суверенітет та безпеку України від зовнішніх і внутрішніх загроз кіберпростору.

1. Про основні засади кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19.

2. Горінова П.В. та Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал*. № 1/2023. URL : http://lsej.org.ua/1_2023/63.pdf.

3. Харитоненко І. О. Правові засади забезпечення кібербезпеки україни в умовах цифрового комунікативного середовища. *Часопис Київського університету права*, 2023, 2: 61 – 64. URL : https://chasprava.com.ua/index.php/journal/article/view/858.

УДК 004.492:341.31:351.74
DOI: 10.31733/15-03-2024/2/338-341

Олександр КАРПАНЕЦЬ
ад'юнкт відділу організації
освітньо-наукової підготовки
Харківського національного
університету внутрішніх справ

СУЧАСНИЙ СТАН ТА ПРІОРИТЕТИ ВДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ОРГАНІВ МВС УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ПРОТИДІЇ ЗБРОЙНІЙ АГРЕСІЇ

У сучасних умовах протидії збройній агресії, спрямованої проти України, питання забезпечення кібербезпеки для нашої держави відіграє ключове значення. На сьогоднішній день в Україні ухвалено цілу низку нормативно-правових актів, які спрямовані на

унормування суспільних відносин у сфері реалізації функцій оборони та забезпечення державної безпеки, одним зі складових елементів якої є кібербезпека. Важливу роль у системі реалізації державної стратегії кібербезпеки держави відіграють органи Міністерства внутрішніх справ України (далі – МВС України), що свідчить про необхідність удосконалення нормативно-правового регулювання у зазначеній сфері та обґрунтовано сучасними умовами протидії збройній агресії.

Основним нормативно-правовим актом, положеннями якого врегульовано правові та організаційні засади забезпечення інтересів людини і громадянина, суспільства і держави, національних інтересів у кіберпросторі, цілі, принципи та напрями державної політики у сфері кібербезпеки, а також повноваження органів державної влади, місцевого самоврядування, юридичних та фізичних осіб, виступає Закон «Про основні засади забезпечення кібербезпеки України». Визначення поняття «кібербезпека» закріплено у п. 5 ч. 1 ст. 1 зазначеного законодавчого акту, у відповідності до якої під зазначеною категорією розглядається як захищеність життєво важливих інтересів людини і громадянина, держави та суспільства у процесі використання кіберпростору, коли має місце забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація існуючих та потенційних загроз національній безпеці у кіберпросторі [5].

Відповідно до п. 4 ч. 4 ст. 5 Закону «Про основні засади забезпечення кібербезпеки України», одним із суб'єктів, на яких покладено повноваження щодо безпосереднього здійснення заходів забезпечення кібербезпеки, є правоохоронні, розвідувальні та контррозвідувальні органи, а також суб'єкти оперативно-розшукової діяльності. Ч. 5 зазначеної норми закріплено перелік основних напрямів діяльності, у тому числі й органів МВС України, у сфері забезпечення кібербезпеки, якими є:

– здійснення заходів у напрямку запобігання використання кіберпростору у військовій, розвідувально-підривній, терористичній та інших протизаконних цілях;

– здійснення виявлення та своєчасного реагування на кібератаки і кіберінциденти, а також усунення їх негативних наслідків;

– здійснення інформаційного обміну з питань реалізованих та потенційних кіберзагроз;

– розробка та реалізація запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібрзахисту та кібероборони;

– забезпечення проведення аудиту інформаційної безпеки, зокрема в межах сфери управління та підпорядкування;

– здійснення інших заходів, спрямованих на забезпечення розвитку та безпечності кіберпростору [5].

Національну систему кібербезпеки визначено положеннями ст. 8 Закону «Про основні засади забезпечення кібербезпеки України». Зокрема, ч. 1 зазначеної норми передбачено, що під такою системою розуміється сукупність суб'єктів забезпечення кібербезпеки, а також пов'язаних з нею науково-технічних, політичних, інформаційних, освітніх, правових, організаційних, розвідувальних, оперативно-розшукових, оборонних, контррозвідувальних, інженерно-технічних, криптографічного і технічного захисту заходів, спрямованих на захист національних інформаційних ресурсів та кіберзахист об'єктів критичної інформаційної інфраструктури.

Положеннями ч. 2 ст. 8 Закону «Про основні засади забезпечення кібербезпеки України» визначено, що одним із суб'єктів забезпечення національної системи кібербезпеки в Україні є Національна поліція України. Саме на органи Національної поліції України покладено реалізації функцій у сфері забезпечення захисту прав та свобод людини і громадянина, суспільних і державних інтересів від кримінальних протиправних діянь у кіберпросторі, а також здійснення заходів запобігання, виявлення, припинення і розкриття злочинів у кіберпросторі, підвищення рівня інформування громадян про безпеку в кіберпросторі [5].

Ключові засади діяльності органів Національної поліції України, статусу поліцейських та порядку проходження служби врегульовано нормами Закону «Про Національну поліцію». Зокрема, у ст. 23 зазначеного законодавчого акту визначено перелік основних повноважень поліції, серед яких до питань забезпечення кібербезпеки можливо віднести наступні: здійснення превентивної та профілактичної діяльності, спрямованої на запобігання вчиненню правопорушень; виявлення причин та умов, що зумовлюють вчиненню правопорушень, а також вжиття заходів для їх усунення; вжиття заходів щодо

виявлення правопорушень та припинення їх вчинення; вжиття заходів, спрямованих на усунення загроз публічній безпеці, що зумовлено вчиненням правопорушень; здійснення своєчасного реагування на заяви і повідомлення про вчинення правопорушень; здійснення досудового розслідування кримінальних правопорушень; забезпечення захисту об'єктів критичної інфраструктури, суспільних та державних інтересів від протиправних посягань у кіберпросторі, а також здійснення заходів виявлення, припинення, розкриття та запобігання кіберзлочинам; здійснення оперативно-розшукової діяльності; здійснення боротьби із диверсійно-розвідувальними силами агресора та не передбаченими законодавством збройними і воєнізованими формуваннями, у співпраці з іншими правоохоронними органами та органами державної влади тощо [4].

Відповідно до положень діючого законодавства, кіберзлочином є комп'ютерний злочин, а саме суспільно небезпечне діяння, вчинене у кіберпросторі чи з його використанням,за яке встановлено відповідальність Кримінальним кодексом України або положеннями міжнародних договорів України [5]. Метою вчинення таких протиправних діянь виступає викрадення чи знищення інформації, що зберігається в інформаційних системах. Фактично законодавцем визнано існування проблеми кібератак в інформаційному просторі як і від ведення збройної агресії, внаслідок чого було внесено зміни до окремих нормативно-правових актів, зокрема доповнено положення кримінального та адміністративного права, враховуючи міжнародні документи та рекомендації, що сприяло вдосконаленню підстав та процесуального механізму притягнення винних осіб до відповідальності за вчинення кіберзлочинів [2, с. 126].

Зокрема, внесено зміни та доповнення до положень Законів «Про національну поліцію» та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану», що передбачали посиленні міри відповідальності за вчинення протиправних дій у кіберпросторі. Зокрема, внесено зміни до положень ст. 361 Кримінального кодексу України (далі – КК України), щодо відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих) електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [3].

Отже, зазначимо, що на законодавчому рівні було розширено сферу діяльності Національної поліції України у сфері протидії кібератакам та різноманітним загрозам в інформаційному просторі, а також у процесі розслідування кримінальних правопорушень, передбачених ст.ст. 361 та 361^1 КК України. Посилення покарання та забезпечення додаткової криміналізації діянь з питань виявлення фейкових повідомлень у соціальних мережах, недопущення вчинення кібератак, сприяють частковому стримуванню потенційних правопорушників від скоєння подібних злочинних посягань. До того ж, державна політика у напрямку правового регулювання кібербезпеки зумовлена пріоритетною значимістю національних інтересів, маючи на меті унеможливлення негативного впливу загроз на інформаційне середовище, реалізовуючи шляхом дотримання приписів діючого законодавства [2, с. 126].

Незважаючи на внесення таких законодавчих змін, недостатнім є рівень нормативного регулювання превентивної та роз'яснювальної роботи органів МВС, оскільки Національна поліція найчастіше комунікує з громадськістю. Саме спрямованість органів МВС України на роз'яснення населенню основних видів та способів поширення дезінформації може сприяти зниженню рівня кіберзлочинності та зменшить навантаження на відповідальні підрозділи Національної поліції при розслідуванні такої категорії кримінальних правопорушень.

Зміцнення довіри має вважатися основним інструментом захисту від гібридних загроз, особливо тих, які спрямовані на підрив демократичних держав та форм правління. Не заборони і блокування, а інформатизація суспільства, розвиток і популяризація критичного ставлення до інформації, до невідомих чи нових джерел інформації здатні створити запобіжники проти інформаційних атак. Протидіяти агресивним інформаційним проявам слід, активно застосовуючи інструменти інформаційних технологій: захищатися тими ж механізмами, працювати з тими ж соціальними групами; вести активний діалог у соцмережах, Інтернет-спільнотах; активно використовувати можливості соціальної реклами; підтримувати створення й діяльність громадських організацій тематичного спрямування [1]. Зазначені заходи підтвердили свою дієвість саме в умовах війни Росії проти України, оскільки більшість українських громадян отримує інформацію саме у соціальних мережах, вчаться самостійно її перевіряти, аналізувати і робити власні

висновки.

У зв'язку із вищевикладеним можливо зробити висновок, що органами МВС України, зокрема підрозділами Національної поліції, реалізовуються заходи захисту інформації та кіберпростору, спрямовані на протидію кіберзлочинності та потенційним кіберзагрозам, використовуючи новітні технології. Проте, в сучасних умовах існує нагальна потреба у нормативному закріпленні системи заходів, спрямованих на законодавче визначення питання дезінформації у соціальних мережах та медіа, механізмів її виявлення, протидії та притягнення винних до відповідальності.

1. Гаврильців М.Т. Інформаційна безпека держави в системі національні безпеки України. URL : http://lsej.org.ua/2_2020/54.pdf. (дата звернення: 02.03.2024).

2. Котелевець А.В. Організаційно-правові аспекти діяльності Національної поліції України у сфері забезпечення кібербезпеки та протидії гібридній інформаційній війні в умовах воєнного стану: тези доп. учасників наук.-практ. конф. (м. Вінниця, 7 груд. 2022 р.). Вінниця: ХНУВС, 2022. С. 125-127.

3. Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 року. ВВР, 2001, № 25-26, ст. 131.

4. Про національну поліцію: Закон України № 580-VIII від 02.07.2015 року. ВВР, 2015, № 40-41, ст. 379.

5. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 року. ВВР, 2017, № 45, ст. 403.

УДК 004.738.5:351.862.4: 316.472.4
DOI: 10.31733/15-03-2024/2/341-342

Руслан КУНЬО
аспірант кафедри управління
та адміністрування
Дніпропетровського державного
університету внутрішніх справ

СОЦІАЛЬНІ МЕДІА ЯК ІНСТРУМЕНТ ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

Соціальні медіа в сучасному світі стали потужним інструментом впливу на національну безпеку, як внутрішню, так і зовнішню. Завдяки своїй глобальній природі та масовому характеру використання, соціальні медіа мають значний вплив на формування громадської думки, міжнародні відносини, а також на безпеку країни.

По-перше, соціальні медіа стали платформою для поширення дезінформації та пропаганди, що може становити загрозу національній безпеці. Вони уможливлюють швидке поширення неперевіреної інформації та маніпулювання громадською думкою, що може призвести до соціальних напружень, конфліктів та навіть кризових ситуацій.

По-друге, соціальні медіа можуть бути використані як засіб для координації негативних дій терористичних організацій або інших злочинних угруповань. Вони дають змогу анонімно спілкуватись та організовувати атаки, що ускладнює роботу правоохоронних органів та збільшує загрозу національній безпеці.

Проте соціальні медіа також можуть бути використані як інструмент для зміцнення національної безпеки. Зокрема, вони дозволяють урядам та правоохоронним органам швидко реагувати на потенційні загрози та вчасно інформувати громадськість про можливі небезпеки та способи їх уникнення. Зокрема, соціальні медіа можуть бути використані для проведення кампаній з підвищення обізнаності населення з питань безпеки, пропаганди цінностей демократії та прав людини [1].

Отже, соціальні медіа є подвійним мечем у сфері національної безпеки. З одного боку, вони можуть становити серйозну загрозу через поширення дезінформації та координацію злочинних дій. З іншого боку, вони відкривають можливості для покращення спілкування між урядом та громадськістю, підвищення свідомості та обізнаності громадян з питань безпеки. Отже, важливо розвивати стратегії використання соціальних медіа з метою забезпечення національної безпеки, збалансовуючи їх позитивний та негативний вплив.