

автоматизовані боти в соцмережах. Законодавство встановлює відповідальність за поширення дезінформації, як це зроблено в ЄС через Digital Services Act. Державні комунікації – сайти, пресконференції, телебачення – використовуються для швидкого реагування на фейки. Освітні кампанії, як-от проєкти з медіаграмотності в школах, формують критичне мислення у громадян. Співпраця з приватними платформами (Facebook, Twitter) дозволяє блокувати шкідливий контент. В Україні проєкт «StopFake» став прикладом ефективного інструменту для спростування російських наративів.

Протидія дезінформації та пропаганді стикається з серйозними труднощами. Швидкість поширення фейків у цифровому світі випереджає можливості реагування, адже спростування часто запізнюється. Баланс між свободою слова та цензурою викликає суперечки, адже надмірні обмеження можуть підірвати демократію. Низький рівень медіаграмотності, особливо в країнах, що розвиваються, ускладнює боротьбу з маніпуляціями. Фінансування дезінформаційних кампаній, часто приховане через офшори чи криптовалюту, важко відстежити. Нарешті, міжнародна координація ускладнюється через різні підходи до свободи інформації – те, що в одній країні вважається пропагандою, в іншій може бути законним висловленням думки.

Інформаційні загрози зростатимуть із розвитком технологій, тому управління безпекою потребує вдосконалення. Інвестиції в технології моніторингу та аналізу допоможуть випереджати дезінформацію. Розширення програм медіаграмотності, особливо для молоді, підвищить стійкість суспільства. Міжнародна співпраця має включати угоди про обмін даними та спільні кампанії проти пропаганди. Для України ключовими є створення єдиного координаційного центру з інформаційної безпеки, залучення приватного сектору та посилення комунікації з громадянами. Лише поєднання технологій, освіти та політики може захистити інформаційний простір.

Управління інформаційною безпекою в умовах глобальних викликів є критично важливим для національної безпеки, адже дезінформація та пропаганда здатні підірвати стабільність держави зсередини. Стратегії моніторингу, контрпропаганди та освіти, підкріплені технологіями та співпрацею, дозволяють протистояти цим загрозам. Україна, перебуваючи в епіцентрі інформаційної війни, демонструє як виклики, так і можливості цього процесу. Успіх залежить від швидкості реакції, довіри суспільства та готовності адаптуватися до цифрових реалій. Інформаційна безпека – це не лише захист від фейків, а й основа для міцної держави.

Олександр ПИСЬМЕННИЙ

аспірант кафедри

адміністративного права і процесу

Дніпровського державного

університету внутрішніх справ

(м. Дніпро, Україна)

<https://orcid.org/0009-0009-1065-3922>

ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ ЯК ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Держава створює різного роду реєстри та бази даних з метою забезпечення ефективного функціонування різних сфер суспільного життя. Ці реєстри та бази даних є важливим інструментом для збору, зберігання та обробки інформації, яка потрібна для прийняття рішень, контролю та надання різного роду послуг громадянам. Однією з головних причин створення реєстрів та баз даних є забезпечення ефективного контролю над різними процесами всередині державного механізму. Наприклад, державні реєстри дозволяють вести облік громадян, встановлювати їхні права та обов'язки, а також забезпечувати їхній доступ до соціальних послуг та допомоги. Такі реєстри також допомагають уникнути подвійного обліку, шахрайства та незаконного заволодіння майном громадян.

Крім того, державні реєстри та бази даних допомагають забезпечити ефективне функціонування систем охорони здоров'я, освіти, соціального захисту та інших галузей. Завдяки цим реєстрам можна вести облік медичних даних, освітніх досягнень, соціальних

пільг та інших важливих показників, що дозволяє забезпечити якісне надання послуг та аналізувати стан суспільства для прийняття ефективних рішень. Також реєстри та бази даних є важливим інструментом для забезпечення взаємодії між різними державними органами та організаціями. Вони дозволяють обмінюватися інформацією, координувати дії та виконувати різні адміністративні процедури швидко та ефективно. Таким чином, створення реєстрів та баз даних є важливим елементом державного управління, який допомагає забезпечити ефективну роботу державних структур, контроль за процесами та надання послуг громадянам.

На жаль, не можна назвати точну кількість реєстрів та баз даних, що існують в Україні, оскільки вона постійно змінюється і залежить від різних факторів, таких як законодавчі зміни, реформи та потреби державних органів.

Зі збільшенням кількості реєстрів та дій, які відбуваються у віртуальному полі щодо запитуваної послуги, без попереднього паперового оформлення заяви чи клопотання, паралельно збільшується і кількість незаконних дій. Такі дії здійснюються або умисно особами, що мають сертифікований доступ до вказаних баз даних, або не навмисно особами, які через неухважність або необізнаність порушили правила ведення відповідного реєстру, і ці дії кваліфікуються за ст. 362 Кримінального кодексу України як злочин.

Так, на прикладі Державного реєстру речових прав на нерухоме майно маємо наступну структуру: є спеціальний Закон України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень», якому відповідає Порядок державної реєстрації речових прав на нерухоме майно та їх обтяжень, затверджений постановою Кабінету Міністрів України № 1127 від 25.12.2015. З метою контролю діяльності державних реєстраторів було утворено Колегію з розгляду скарг у сфері державної реєстрації, діяльність якої регламентується Положенням про Колегію з розгляду скарг на рішення, дії або бездіяльність державного реєстратора, суб'єктів державної реєстрації, територіальних органів Міністерства юстиції, затвердженим наказом Міністерства юстиції України № 71/5 від 09.01.2020.

Зупинимось більш детально на організації захисту даних, що містяться у реєстрах. Відповідно до наказу Міністерства внутрішніх справ України № 988 від 30.10.2012 «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» основним завданням зазначеного управління є: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням [3].

Проаналізувавши опубліковані звіти про результати роботи Департаменту кіберполіції Національної поліції України за 2022 та 2023 роки, хочемо навести наступні статистичні дані та окреслити виявлену динаміку.

У 2022 р. припинено діяльність 23 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 81 учасник (23 організатори та 51 активний виконавець), якими вчинено 269 кримінальних правопорушень (у тому числі 240 тяжких та особливо тяжких), з яких: 178 шахрайств, 59 – у сфері використання електронно-обчислювальних машин, 12 – у сфері обігу наркотичних засобів, 3 – за ст. 255 Кримінального кодексу України (створення, керівництво злочинною спільнотою, а також участь у ній), 2 крадіжки, 3 – у сфері господарської діяльності (легалізація (відмивання) майна, одержаного злочинним шляхом), 1 – привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем. Також, у 2022 р. кіберполіцейськими здійснювалось супроводження 5 тис. кримінальних правопорушень, виявлено 2,3 тис. кіберзлочинів, повідомлено про підозру 1 тис. осіб за вчинення 2,3 тис. кримінальних правопорушень. Затримано понад 100 кіберзлочинців, задокументовано та притягнуто до відповідальності 30 педофілів та 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних проваджень за обвинуваченням 840 осіб [4].

У 2023 р. скеровано до суду кримінальні провадження щодо протиправної діяльності 42 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 191 учасник; ними вчинено 731 кримінальне правопорушення (у тому числі 547 тяжких та особливо тяжких), з яких: 438 шахрайств, 20 крадіжок, 12 – за ст. 255 КК України (створення, керівництво злочинною спільнотою, а також участь у ній), 11 сутенерств, 3 – привласнення, розтрата майна, 46 – у сфері господарської діяльності, 33 – у

сфері використання електронно-обчислювальних машин, 14 – у сфері службової діяльності, 7 – у сфері обігу наркотичних засобів, 147 – інші. Також у 2023 р. кіберполіцейськими здійснювалось супроводження понад 6,4 тис. кримінальних проваджень, виявлено 3,6 тис. кіберзлочинів, повідомлено про підозру 1,7 тис. особам за вчинення 3,7 тис. кримінальних правопорушень. До суду з обвинувальними актами скеровано 4 тис. кримінальних проваджень за обвинуваченням 1,3 тис. осіб [5].

Логічним є факт, що з розвитком комп'ютерних технологій кількість злочинів стає дедалі більшою. Навіть стовідсоткове розкриття злочинів не зменшить їхню кількість, бо статистика розкриття злочинів не є протидією їх скоєнню.

Завданням держави є забезпечити безпеку громадян; з цим завданням держава частіше не справляється, ніж навпаки, оскільки кожен має приклад ошукування людей шляхом розсилки фішингових листів. Так, наприклад, щодня від Нотаріальної палати України надходять повідомлення про фішингову розсилку на офіційні електронні поштові скриньки нотаріусів листів зі шкідливими програмним вкладенням, метою якого є отримання несанкціонованого доступу до реєстрів, що перебувають у користуванні нотаріусів. Трохи дивним є рекомендація для нотаріусів не відкривати дивні листи, або відкривати їх спочатку на мобільному пристрої, або не переглядати пошту на комп'ютерах, на яких встановлено реєстри. Тобто замість вирішення питання захисту реєстрів від фішинга фаєрволом нотаріусам рекомендують просто придбати окремий комп'ютер для реєстрів. Тобто вирішити саму проблему не можуть, а лише радять ситуативні методи, якими нотаріус сам себе повинен захищати від дій правопорушників, хоча згідно з Законом України «Про нотаріат» такі функції у нотаріусів відсутні.

З огляду на проблеми сучасності в Україні на кожний новий електронний реєстр чи державну базу даних створюється свій керівний чи контролюючий орган, що ніяк не покращує кримінальний простір в цифровому полі, тому неминучим стає утворення на базі Міністерства цифрової трансформації України багаторівневої Національної служби цифрового простору з аналітичною, контролюючою та правозахисною метою, щоб усім цифровим простором держави опікувався один орган. Створення одного працюючого органу, який займатиметься вирішенням різних питань в окресленій сфері, може мати декілька переваг для громадян.

Саме тому одним із можливих способів захисту інформації у державних реєстрах є впровадження сучасних технологій криптографічного захисту даних. Це включає використання шифрування для збереження конфіденційності даних та електронних підписів для забезпечення цілісності та автентичності інформації. Криптографічні алгоритми можуть ускладнити доступ до даних для несанкціонованих осіб та зменшити ризик незаконних змін.

Крім того, важливо забезпечити фізичну безпеку серверів та баз даних, де зберігається інформація реєстру. Це може включати використання контрольно-пропускних систем, відеоспостереження та обмеження доступу до приміщень з серверами, а саме надання його лише для авторизованих осіб.

Також необхідно регулярно проводити аудит безпеки, щоб виявляти потенційні вразливості та вживати заходів для їх усунення. Це може включати перевірку наявності оновлень програмного забезпечення та відповідних політик доступу, а також проведення незалежних перевірок зовнішніми експертами.

Отже, захист інформації у державних реєстрах вимагає комплексного підходу. Впровадження сучасних технологій криптографічного захисту, фізична безпека, регулярний аудит та освіта співробітників можуть сприяти забезпеченню надійного захисту реєстру та запобіганню незаконному доступу до нього.

1. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України від 01 липня 2004 р. URL : <https://zakon.rada.gov.ua/laws/show/1952-15#Text>.

2. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : постанова Кабінету Міністрів України від 25 грудня 2015 р. № 1127. URL : <https://zakon.rada.gov.ua/laws/show/1127-2015-п#Text>.

3. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС : наказ Міністерства внутрішніх справ України від 30.10.2012 № 988. URL : <https://zakon.rada.gov.ua/rada/show/v0988320-12#Text>.

4. Звіт про результати роботи Департаменту кіберполіції у 2022 році. Кіберполіція. URL : <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--rocz-969/>.

5. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році. Кіберполіція. URL : <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--rocz-4792/>.