поставлено завдання постійного моніторингу інформації, виділення необхідної інформації із загальної інформації та збору інформації відповідно до виявлених інформаційних потреб. Необхідний перехід до спеціальних інформаційних сервісів; трансформуючий аналіз інформації та інтеграція; джерела інформації відповідно до потреб споживачів.

Виконання цих завдань потребує побудови системи інформаційного забезпечення споживачів інформації. У цій системі споживач інформації виступає вирішальним елементом у створенні інформаційно-аналітичних документів.

В Україні також був створений чат-бот у Telegram для пошуку даних про захисників, які не виходять на зв'язок з певних причин. Наприклад, за допомогою чат-боту "Розшук по даних Національного інформаційного бюро" створили спеціальні інструменти, за допомогою яких рідні та близькі українських оборонців, які потрапили у полон до ворога або зникли безвісти за особливих обставин, можуть здійснити швидкий пошук даних про них. Для того щоб родич міг визначити статус військовослужбовця, який перебуває в розшуку, необхідно надати наступну інформацію: ідентифікаційний код, прізвище, ім'я та по батькові, номер телефону та дата народження розшукуваної особи, прізвище, ім'я та по батькові, дата народження та ідентифікаційний код особи, яка розшукується. У результаті пошуку рідні та близькі зможуть отримати у чат-боті один із поточних статусів полоненого: про особу немає даних у реєстрі НІБ. Якщо їх не вносили, чат-бот запропонує додати ці відомості; дані є, але в базі даних НІБ немає відомостей, чи перебуває особа в полоні; дані є, особа, ймовірно, перебуває в полоні (бракує підтвердження від Міжнародного комітету Червоного Хреста – МКЧХ); дані про особу є в базі НІБ, перебування в полоні підтверджено МКЧХ; полонена особа звільнена під час обмінів.

Враховуючи вищевикладене, хочемо зробити висновок, що в активну фазу війни на території України метою є підтримання на високому рівні всієї розвідувально-аналітичної діяльності, а також злагодженої роботи всіх напрямів.

У сфері штучної зброї з часом з'являється багато нових технологій, які завжди вимагають кваліфікованих працівників для їх дотримання, тому необхідно постійно підвищувати кваліфікацію всіх працівників технічної сфери.

Якщо говорити про технічну складову інформаційно-аналітичної діяльності Збройних Сил України в теперішній час дії правового режиму воєнного стану на території України [1], потрібно створювати та розвивати ці бази даних та накопичувати й зберігати інформацію у різних сферах аналітичного військового процесу. А це потребує забезпечення технічними приладами і засобами європейського зразка.

1. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text.

2. Про оборону України: Закон України від 06.12.1991 р. №1932-XII. URL: https://ips.ligazakon.net/document/view/t193200?an=1&ed=2023_03_21.

3. Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III. URL: https://ips.ligazakon.net/document/view/t012331?an=ul-120&ed=2008_06_03.

Роман ОПАЦЬКИЙ
доцент кафедри адміністративного права і процесу
Дніпровського державного університету внутрішніх справ
(м. Дніпро, Україна),
доктор юридичних наук, доцент
https://orcid.org/0000-0002-8658-8153

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Війни програються спочатку в головах, а потім на полі бою – це загальновідома фраза, яка отримала багаторазове підтвердження в історії. Кожного разу країна, народ якої втрачав віру в свою армію, неодмінно зазнавала поразки, і ворог святкував перемогу.

Спочатку гібридна війна, а потім і повномасштабне вторгнення російської федерації

показали, що бойові дії супроводжуються шаленим інформаційним тиском, вкидом неправдивої, фейкової інформації, спрямованої на підрив волі народу, знецінення віри у Збройні Сили України та знищення довіри до влади.

Дезінформація є не менш небезпечним інструментом ведення війни, ніж зброя, який часто використовує державу чи недержавні суб'єкти для досягнення своїх стратегічних цілей. Вона має багатошаровий вплив: створення паніки, розпалювання міжетнічних чи релігійних конфліктів, формування негативного іміджу країни на міжнародній арені, маніпулювання громадською думкою під час виборчих процесів тощо. Саме тому протидія дезінформації стала важливою складовою забезпечення національної безпеки України.

Ефективна протидія дезінформації передбачає комплексний підхід, що включає як технічні, так і соціальні інструменти. З одного боку, це розвиток сучасних технологій моніторингу та аналізу інформації, штучного інтелекту для виявлення фейкових новин, а також посилення кібербезпеки. З іншого – підвищення рівня освіченості населення у сфері медіа. Громадяни повинні вміти критично оцінювати інформацію, розпізнавати фейкові новини, перевіряти джерела та усвідомлювати, що ними можуть маніпулювати.

Протидія дезінформації повинна забезпечуватися на рівні держави за наступними напрямами:

– правове забезпечення. На сьогодні в Україні існує ціла система нормативних актів, які певною мірою убезпечують країну від негативного впливу дезінформації, зокрема Закон України «Про інформацію», в якому встановлено, що «інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини» [1]; Закон України «Про Раду національної безпеки і оборони України», яким передбачено функціонування Центру протидії дезінформації як робочого органу Ради національної безпеки і оборони України. Відповідно до Закону України від 05 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України» державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [3]. Це лише основні нормативні акти, що регулюють протидію дезінформації, із загального масиву. Однак на сьогодні доцільним є прийняття спеціалізованого Закону України «Про протидію дезінформації», який би цілеспрямовано регулював організацію протидії цьому небезпечному явищу;

– міжнародна взаємодія. Важливим компонентом боротьби з дезінформацією є міжнародна співпраця. Дезінформаційні кампанії часто виходять за межі однієї країни, тому міжнародні організації, такі як НАТО, ЄС чи ООН, відіграють важливу роль у розробці спільних підходів до протидії інформаційним загрозам. Україна, яка вже тривалий час є об'єктом агресивних інформаційних атак, може поділитися відповідним досвідом з іншими країнами тощо;

– взаємодія із засобами масової інформації. Особливу увагу слід приділити ролі засобів масової інформації у протидії дезінформації. Незалежні медіа, які підтримують журналістські стандарти, можуть стати бар'єром для поширення фейкових новин. Журналісти повинні відповідально ставитися до перевірки фактів, уникати маніпулятивних формулювань та працювати над підвищенням довіри;

– формування інформаційної культури в споживача інформаційного продукту. На сьогодні масовий та легкий доступ до всесвітньої мережі Інтернет вимагає від кожного споживача відповідального ставлення до спожитої інформації. Перш ніж прийняти отриману інформацію за правдиву, повірити в неї та, як результат, репродуктувати її, особа повинна спочатку перевірити її за допомогою декількох незалежних і бажано антагоністичних джерел, щоб не стати черговим «інфоциганом»;

– активна антидезінформація. З метою дієвої протидії проявам дезінформації держава через органи та посадові особи спільно з засобами масової інформації та громадськими об'єднаннями повинна активно займатися «фактчекінгом» (англ. fact-checking), тобто відслідковувати дезінформацію (фейки) та оперативно реагувати на неї шляхом її спростування через, як правило, ті самі ресурси, де її було оприлюднено.

Отже, протидія дезінформації – це багатогранний процес, який потребує злагоджених дій державних органів, громадянського суспільства, медіа та міжнародних партнерів. У сучасному світі деінформація стала потужною зброєю, і здатність держави захищати свій інформаційний простір є вирішальним фактором забезпечення національної безпеки. Для України, яка перебуває в умовах гібридної війни, це завдання має особливе значення, адже саме інформаційна стійкість допоможе зміцнити незалежність, суверенітет та стабільність держави.

1. Про інформацію : Закон України від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Про національну безпеку України : Закон України від 21 червня 2018 р. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Катерина ПИЛИПЕНКО
професор кафедри економіки та готельно-ресторанного бізнесу Мелітопольського державного педагогічного університету імені Богдана Хмельницького (м. Запоріжжя, Україна), доктор економічних наук
https://orcid.org/0000-0003-3170-1208

Ольга МАЛЕЦЬКА
доцент кафедри обліку і оподаткування Львівського національного університету природокористування (м. Львів, Україна), кандидат економічних наук
https://orcid.org/0000-0002-0004-7605

ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: СУЧАСНІ МЕХАНІЗМИ ЗАХИСТУ БУХГАЛТЕРСЬКОГО ОБЛІКУ

У сучасних умовах цифрової трансформації інформаційні технології дедалі активніше інтегруються до всіх сфер діяльності підприємств, включаючи бухгалтерський облік. Цей процес відкриває нові можливості для підвищення ефективності управління фінансами, проте одночасно створює нові виклики, пов'язані із забезпеченням безпеки даних. Захист фінансової інформації набуває критичного значення, оскільки вона є цінним активом компанії, а її компрометація може мати серйозні фінансові та репутаційні наслідки.

Бухгалтерський облік традиційно є однією з найбільш вразливих систем, оскільки містить конфіденційні дані про фінансовий стан підприємства, його господарські операції, розрахунки з контрагентами та персоналом. Основні загрози, з якими стикаються компанії у цьому контексті, включають несанкціонований доступ до інформації, втрату чи знищення даних, кібератаки, фальсифікацію фінансової звітності та внутрішнє шахрайство. Наслідки таких порушень можуть варіюватися від фінансових збитків і юридичних санкцій до підриву довіри інвесторів, партнерів і клієнтів:

1) Несанкціонований доступ до інформації: отримання доступу до конфіденційних даних особами, які не мають на це права.

2) Втрата або знищення даних: випадкове або навмисне видалення інформації, що може призвести до втрати важливих фінансових записів.

3) Кібератаки: зловмисні дії, спрямовані на порушення роботи системи або крадіжку даних.

4) Фальсифікація фінансової звітності: навмисне спотворення фінансових показників з метою введення в оману користувачів звітності.

5) Внутрішнє шахрайство: недобросовісні дії співробітників, спрямовані на