

УДК 004+351  
DOI: 10.31733/17-03-2023-535-536

**Людмила РИБАЛЬЧЕНКО**  
завідувач кафедри інформаційних технологій  
Дніпропетровського державного  
університету внутрішніх справ,  
кандидат економічних наук, доцент

## **ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В СУЧАСНИХ УМОВАХ**

Швидкі зміни, які відбуваються в сучасному інформаційному просторі, потребують ефективного захисту національної інформаційної безпеки, яка має гарантувати українцям безпечне функціонування усіх сфер життєдіяльності. Забезпечення інформаційної безпеки на усіх рівнях соціально-економічного розвитку, удосконалення законодавчого та нормативно правового забезпечення щодо захисту інформації, виявлення можливих загроз та їх попередження, співпраця з іншими державами та міжнародними організаціями є важливою стратегією міжнародної та національної безпеки держави, особливо під час воєнного стану в Україні.

До основних нормативно-правових документів та законів щодо інформаційної безпеки України належать: Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про захист персональних даних» та документи у сфері захисту персональних даних, Закон України «Про доступ до публічної інформації», Закон України «Про національну безпеку України» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші.

Питання інформаційної безпеки пов'язано з інформаційними технологіями, які використовуються для забезпечення інформаційної безпеки. Захист інформаційної безпеки полягає не лише у застосуванні несанкціонованого доступу до інформації, а й використанні відповідних методів щодо її безпеки та захисту [1].

Збереження інформаційного суверенітету та формування ефективної системи безпеки в інформаційній сфері, на сьогоднішній час є першочерговим питанням для нашої країни. Забезпечення цілісності суспільства, захист національного інформаційного простору та протидія усім негативним інформаційним впливам є важливим питанням для України.

Забезпечення надійної інформаційної безпеки в державі надасть захист інтересам громадян щодо отримання правдивої та якісної інформації. Інформаційна безпека представляє собою одну із важливих складових національної безпеки країни. Саме інформаційна безпека відображає стан захищеності інтересів громадян та держави від негативних інформаційних впливів і небезпек, які можуть бути пов'язані із несанкціонованим доступом та втручанням до особистої чи державної інформації, а також її розповсюдженням [2].

Питання гарантування інформаційної безпеки в Україні стали найбільш актуальними в умовах війни через вплив та розповсюдження російської пропаганди засобами масової інформації на свідомість громадян України та на громадськість в усьому світі.

Зараз відбуваються суттєві загрози в національному інформаційному просторі України, які несуть небезпеку нашій державі, її суверенітету, цілісності, політичному та економічному розвитку. Створення загроз національній безпеці України в інформаційній сфері становить небезпеку життю кожного її громадянина, має негативний інформаційний вплив на свідомість громадян, інформаційну, технічну та критичну інфраструктуру держави.

Стрімкий розвиток інформаційних технологій став значним поштовхом для створення нових проявів безпеки, що викликані ситуацією нового технологічного рівня. Розподіл сфер впливу у кіберпросторі постійно посилюється. Спроможність держави захистити свої національні інтереси є пріоритетною складовою кібербезпеки кожної країни. Створення в державі кібервійськ сприятиме потужному забезпеченню захисту інформаційної інфраструктури від можливих кібератак, надійному захисту від втручання в

національний інформаційний простір, а також управління інформаційними системами противника та їх руйнування.

До основних кіберзагроз належать порушення цілісності даних, несанкціонований доступ, конфіденційність інформації, втручання в корпоративну чи державну таємницю, тощо. Такі загрози впливають на функціонування будь-якої інформаційної системи, сфери діяльності підприємства чи установи, а також забезпечення національної безпеки.

Тому для управління будь-якими небезпеками, необхідно створити потужний захист від можливих та потенційних загроз із залученням висококваліфікованого персоналу та з використанням сучасних програмних засобів.

Питаннями національного рівня є визначення кіберзагроз, заходів та можливостей кібербезпеки, розробка основних показників кібербезпеки, їх дослідження за певними ознаками та створення відповідних груп показників кібербезпеки для аналізу та розробки заходів щодо їх уникнення. Усі державні органи та приватні структури взаємодіють між собою для запобігання та подолання негативних наслідків.

Оскільки зараз триває війна в Україні, зростає необхідність у забезпеченні безпеки проти загроз у кіберпросторі. Пріоритетними перспективами є прийняття таких стратегічних рішень, які б були направлено на управління ризиками підприємства та зміцнення їх стійкості щодо забезпечення безпеки. Більшість керівників підприємств бачать кіберстійкість пріоритетом бізнесу в їх організації. Перехід від кібербезпеки до кіберстійкості є важливим кроком до більш надійного та стабільного майбутнього.

Міністерство цифрової трансформації України та Державна служба спеціального зв'язку і захисту інформації проводять роботу щодо посилення захисту від кіберзлочинності через оновлення та реформування законодавчої бази, вдосконалення механізму кіберзахисту органів державної влади, їх інформаційно-телекомунікаційних систем, проведення аналізу стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури [3].

Але сучасний розвиток цифрових технологій йде значно швидше і сприяє поширенню кіберзлочинності, ніж існуюче нормативно-правове законодавство, яке направлено на врегулювання даного виду економічної злочинності.

Таким чином, в умовах військової агресії російської федерації в Україні, сучасний національний інформаційний простір нашої держави є недостатньо захищеним від негативних інформаційних впливів і загроз. Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, протидія кібератакам і загрозам є стратегічними завданнями держави. Тому на державному рівні має бути удосконалено чинне законодавство в напрямку посилення правового забезпечення захисту національної інформаційної безпеки, у тому числі в сфері кібербезпеки та кіберзахисту, через плідну співпрацю з підрозділами провідних країн світу.

---

1. Rybalchenko L., Kosyuchenko O., Klynitskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. Scientific journal «Philosophy, Economics and Law Review». 2022. Vol. 2 (1). Pp. 71-81.

2. Rybalchenko L., Kosyuchenko O. Peculiarities of using visual means of information and analytical activity in legal and law enforcement sphere. Scientific journal «Philosophy, Economics and Law Review». 2022. Vol. 2 (2). Pp. 162-169.

3. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua>.