Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського
державного університету
внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Інформаційне суспільство є одним із типів суспільств, які розвиваються внаслідок соціального прогресу. Сьогодні ми можемо спостерігати активну фазу переходу суспільства від індустріального до інформаційного простору. Можливості глобальної мережі, що активно використовуються у всіх сферах суспільного життя, засновані на інформаційних ресурсах і являють собою сукупність даних, які організовані в інформаційних системах для отримання достовірних відомостей у різних сферах знань та практичної діяльності. Однак одночасно зі збільшенням ролі інформації підвищується і важливість її захисту за допомогою інструментів інформаційної безпеки. Актуальності це питання набуває в особливий правовий режим – воєнний стан, що діє на території нашої країни починаючи з 24 лютого 2022 року у зв'язку з активною фазою вторгнення російської федерації. У сучасних воєнних реаліях важко та навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати у війні не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх суперечностей. Така тактика є характерною для війн нового формату – гібридних, де безпосередньо військовий фактор є лише однією зі складових цілого [1].

Відповідно до законодавства України, поняття «інформаційна безпека» має таке визначення: «Стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди державі через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [2].

Інформаційна безпека містить:

- стан захищеності інформаційного простору, завдяки якому забезпечується його формування та розвиток на користь держави, громадян та організацій;
- стан інформації, що унеможливлює або значно впливає на порушення таких її властивостей, як цілісність, конфіденційність та доступність;

- стан інфраструктури, що дозволяє використовувати інформацію суворо за призначенням та без негативного впливу на систему;
- економічну складову, що містить телекомунікаційні та інформаційні системи та структури управління, такі як системи збору, кумуляції та обробки даних, загальноекономічного аналізу та прогнозування господарського розвитку управління, координування та ухвалення рішень;
- фінансову складову, що охоплює інформаційні мережі та бази даних, системи фінансових розрахунків та обміну.

Варто зазначити, що інформаційна боротьба стає тим чинником, що вплине на саму війну, її початок, процес і результат. Це підтверджується агресією росії проти України. На початку 2021 року ухвалена нова Стратегія інформаційної безпеки, що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегії кібербезпеки України, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України [2]. У змісті Стратегії інформаційної безпеки конкретизуються потенційні інформаційні загрози: «інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав» [1].

Ключовою характеристикою сутності інформаційної безпеки під час військового стану є властивість захищеності, що містить два різновиди захисту: активний та пасивний.

Активний – захист спрямований на попередження несанкціонованого доступу до інформації. Пріоритетами цього захисту є: захист особистих даних, тобто соціальних цінностей та інших конфіденційних відомостей громадян та держави в цілому; експлуатація засобів інформаційної безпеки; експлуатація та захист об'єктів критичної інфраструктури; міжнародні інтереси.

Пасивний – захист поширюється на суспільство та економічний розвиток. Пріоритетними напрямами пасивного захисту можна визначити: розвиток культури; розвиток онлайн-демократії; розвиток економіки; розвиток ІТ-сектору; міжнародне співробітництво.

Якщо говорити про «забезпечення інформаційної безпеки», то потрібно розуміння основних принципів «забезпечення інформаційної безпеки»: [3]:

1. Принцип системності. Відповідно до нього, захисні заходи повинні бути спрямовані на запобігання інформаційним атакам з боку зовнішніх та внутрішніх джерел. Засоби захисту повинні використовуватись адекватно ймовірним видам загроз та функціонувати у вигляді комплексної системи захисту.
2. Принцип міцності. Встановлює, що правила забезпечення інформаційної безпеки повинні охоплювати всі зони безпеки, мати рівну надійність захисту та дозволяти визначати ймовірні загрози.
3. Принцип багаторівневого захисту. Орієнтований створенням кордонів захисту інформаційної системи, що складається з послідовно розташованих зон безпеки, ключова з яких розташовується всередині всієї

системи.

4. Принцип безперебійності. Відповідно до нього функціонування системи інформаційної безпеки має бути безперервним та безперебійним.

5. Принцип розсудливості. Виражається в розумності застосування захисних заходів із необхідним ступенем безпеки. В основі цього принципу лежить доцільність високих матеріальних витрат та раціональність, їх подальшого використання.

Сутність інформаційної безпеки під час військового стану час полягає у формуванні активного захисту щодо пріоритетних інтересів, пов'язаних з використанням інформаційних ресурсів, у спрямованості на створення умов нормального розвитку нашого суспільства та економіки. Забезпечення інформаційної безпеки є комплексним завдання, що обумовлено складністю та багатоплановістю інформаційного середовища. Вирішення проблеми із забезпечення інформаційної безпеки вимагає застосування організаційних, законодавчих та програмно-технічних заходів, які мають бути задіяні в сукупності, оскільки у разі нехтування хоча б одним з цих аспектів підвищується ймовірність втрати інформації, роль якої в сучасному житті суспільства набуває все більшого значення.

Отож в період особливого воєнного стану саме інформація є тією зброєю «масового ураження». Здійснення інформаційної безпеки в умовах воєнного стану є комплексною діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У сьогоднішніх реаліях інформаційна безпека відіграє важливу роль в житті суспільства і людини, тому захист інформаційної безпеки в нашій державі повинен мати та має пріоритетний напрям.

---

1. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. Вип. 1. С. 150–155.

2. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 року № 685/202. URL: http://surl.li/lospu

3. Milov O., Hrebeniuk A., Nalyvaiko A., Pasko I., Rzayev Kh., Salii A., Soloviova O., Synytsina U. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system Eastern-European Journal of Enterprise Technologies, № 6/2 (108), ISSN ISSN 1729-3774 Scopus, DOI: 10.15587/1729-4061.2020.218660, 2020. S. 30–52. URL: http://surl.li/lotwp