Для забезпечення комплексного підходу до подальшого кіберзахисту України всі вони підягають ретельному вивченню.

1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Site. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0887.
2. Austrian Cyber Security Strategy. Enisa.Europa.EU. Site. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf.
3. Belgian National Risk Assessment. National Crisis Center. Site. URL: https://crisiscenter.be/en/what-does-national-crisis-center-do/risk-assessment-and-protection-critical-infra structures/belgian.
4. Cyber defence of critical infrastructure. Republic of Estonia Information System Authority. URL: https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure.
5. National Center for Infrastructure Protection and Cybersecurity (CNPIC) – Spain. Cyber Security Intelligence. URL: https://www.cybersecurityintelligence.com/national-center-for-infra structure-protection-and-cybersecurity-cnpic-spain-7799.html.
6. Critical Infrastructure and the IT Security Act. URL: https://kpmg.com/de/en/home /services/advisory/consulting/services/cyber-security/critical-infrastructure-and-it-security-law.html.
7. Portugal: Cybersecurity. One Trust DataCuidance. URL: https://www.dataguidance.com/opinion/portugal-cybersecurity.
8. Cyber Security Protection of Critical Infrastructures. ICI Bucureşti. URL: https://www.ici.ro/en/ research-structures/cybersecurity-and-critical-infrastructure/
9. Data protection and cybersecurity laws in Hungary. CMS Law Tax Future. URL: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/hungary.
10. Cybersecurity – Securing Critical Infrastructure. Business Finland 27.4.2022. URL: https://www.businessfinland.fi/en/whats-new/events/2022/cybersecurity--securing-critical-infrastructure.
11. The Critical Infrastructure Protection in France. SGDSN.Gouv.Fr. URL: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

УДК 342.95+351
DOI: 10.31733/17-03-2023-524-526

Алла ГІРМАН
доцент кафедри міжнародних економічних
відносин та регіональних студій
Університету митної справи та фінансів,
кандидат політичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СУЧАСНИХ УМОВАХ

XXI століття з усією впевненістю можна назвати століттям постінформаційних технологій. Життя в суспільстві нерозривно пов'язане з отриманням, обробкою, зберіганням
та передачею інформації. Наразі важко уявити собі сферу людської діяльності, яка не застосовує інформаційне наповнення за допомогою дії інформаційних технологій. Окремою складовою цього процесу, очевидно, є інформаційно-телекомунікаційна мережа «Інтернет». Життя без мережі «Інтернет» для будь-якого обивателя вже неможливе.

Відносини у сфері інформаційного простору та його вплив на суб'єкти правозастосування вимагають свого ефективного регламентування і це
вже не просто визнання важливості інформації як інструменту впливу на особистість, групу людей та їх поведінку, а констатація факту необхідності адекватного регулювання її отримання, обробки, зберігання та поширення.

Розвиток інформаційних технологій, масове поширення інструментів отримання та обробки інформації (гаджети, комп'ютери, мобільні станції, поява соцмереж, відеохостингів та ін.) з одного боку суттєво полегшило доступ до отримання будь-якої інформації, включаючи особисту, але, з іншого – створило передумови для ефекту масового зловживання нею, у тому числі, вторгненням у сферу особистих прав та свобод людини.

Відсутність ефективного механізму регулювання правовідносин у мережі «Інтернет»,

вже зараз негативно впливає на захист прав та законних інтересів пересічних громадян, організацій, а часом і інтересів держави (наприклад, в галузі державних автоматизованих систем, авторських та (або) суміжних прав, персональних даних, інтернет-торгівлі та ін.). Всім відома словесна формула: «Хто володіє інформацією, той володіє всім світом» знаходить все більше підтвердження у тих глобальних геополітичних

і соціально-економічних процесах, що відбуваються в сучасному світі, свідками яких ми є. Знання та інформація стали стратегічними ресурсами держави та суспільства, ресурсами соціально-економічного, технологічного та культурного розвитку. Масштаби їх використання можна порівняти з використанням традиційних ресурсів, а величина сумарних витрат на них вже має макроекономічну значимість.

Призначення інформації зазвичай визначається її змістом. За даним критерієм інформацію поділяють на: економічну, правову, соціальну, технічну, організаційну та інші види залежно від її змісту та цілей подання. За своєю природою, сутнісним наповненням інформацію можна створювати, обробляти, передавати, отримувати, зберігати. Така можливість визначає ризик використання її недоброзичливцями (як окремими особами та групами, так і цілими державами) та може завдати шкоди державі та суспільству. Саме з цих позицій обґрунтовано виникнення цілого окремого наукового інституту «інформаційна безпека» та вжиття практичних кроків у вирішенні завдань забезпечення інформаційної безпеки різними акторами такої діяльності: починаючи від приватних осіб та закінчуючи цілими державами та міждержавними утвореннями.

Ураховуючи викладене, важливо розглянути і термін «безпека» також у окремому контексті. Етимологічний аналіз поняття «безпека» дозволяє зробити висновок, що під ним розуміється відсутність небезпеки, тобто створення умов, за яких відсутня небезпека того чи іншого явища та властивості. Зазіхання на ту чи іншу інформацію, що має важливе значення, може спричинити згубні наслідки.

Головною метою будь-якої системи забезпечення безпеки є створення умов запобігання загрозам, тобто недопущення розкрадання, розголошення, втрати, витоку, спотворення та знищення різних об’єктів, які потребують забезпечення безпеки. Крім того, важливо не ототожнювати поняття інформаційної безпеки та комп’ютерної безпеки, що можна спостерігати останнім часом. Це взаємопов’язані категорії, проте комп’ютерна безпека є лише одним із елементів інформаційної безпеки [1]. У свою чергу, поняття «інформаційна безпека» має певну специфіку. Вона полягає у тому, що сама суть слова «інформаційна» зводиться не лише до поняття «інформація», а й до забезпечення безпеки держави, тобто до інформаційної сфери, яку у загальному вигляді можна визначити, як сукупність суспільних відносин щодо інформації, її змісту, і навіть щодо технічних засобів обробки інформації.

До змісту інформаційної безпеки входять такі категорії як: доступність, цілісність, конфіденційність. Доступність – це можливість за прийнятний час отримати потрібну інформаційну послугу. Під цілісністю мається на увазі актуальність та несуперечність інформації, її захищеність від руйнування та несанкціонованої зміни. Зрештою, конфіденційність – це захист від несанкціонованого доступу до інформації.

До системи забезпечення інформаційної безпеки входять такі елементи:

- діяльність у сфері забезпечення інформаційної безпеки;
- засоби здійснення заходів;
- суб’єкти реалізації заходів [2].

Варто зауважити, що слід окремо виявити характеристику поняття інформації з позицій цивільного права. Легальне визначення інформації закріплено у ст. 200 ЦК України, згідно з якою інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Ідентичне визначення інформації закріплено і у ст. 1 Закону України «Про інформацію» [3].

Отже інформація – результат такої форми взаємодії особи із зовнішнім світом, за якої особа отримує всю складну різноманітність про неї, перетворюючи це на знання, а потім на кінцевий продукт інтелектуальної діяльності. Інформація відповідає ознакам нематеріальності, але при цьому її природа передбачає можливість фіксації на матеріальних носіях: паперових, комп’ютерних, магнітних, аудіо-відео носіях та ін. Також до однієї з особливостей, властивих інформації, можна віднести її властивість, що вона може вільно і необмежено поширюватися, звертатися, використовуватись, втілюватись у різних формах, споживатися.

У сучасних умовах воєнних дій в Україні розробка та реалізація практичних заходів

щодо забезпечення інформаційної безпеки є особливо актуальними. Інформаційна війна, на думку американських експертів, належить до одного із новітніх факторів, що має комплексний та динамічний характер і здійснює все більш значущий вплив на інфраструктуру держави. Це по суті новий вид війни, а це, відповідно, потребує системних заходів на рівні державної політики:

– вдосконалення правового забезпечення інформаційної безпеки;

– актуалізації системи ліцензування організацій, які працюють з інформацією чи здійснюють її захист;

– розвиток систем і засобів контролю;

– підготовки кадрів у сфері захисту інформації, крім того, одним із найважливіших напрямів є розширення міжнародної співпраці, участь в міжнародних системах сертифікації.

Отож, швидше за все, питання інформаційної безпеки в майбутньому вирішуватиметься
в комплексі нових проблем, що лежать і в площині високих технологій, і в логіці всього світового розвитку.

1. Кодинець А. О. Інформація як об'єкт цивільно-правової охорони. Науковий вісник Ужгородського національного університету. 2016. Вип. 39. С. 59.

2. Кодинець А. О. Цивільно-правове регулювання зобов'язальних інформаційних відносин. К. : Алерта, 2016. 582 с.

3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12/ed20101013.

4. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL: https:// ips.ligazakon.net/document/T030435?an=14.

УДК 342.95+004
DOI: 10.31733/17-03-2023-526-528

Володимир ПЯДИШЕВ
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного
університету внутрішніх справ,
доктор юридичних наук, професор

СУЧАСНІ АСПЕКТИ КІБЕРЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР: ЗАРУБІЖНИЙ ДОСВІД

Можна без перебільшення стверджувати, що сьогодні увага світової спільноти прикута до подій в Україні, де тривають постійні атаки на критичні інфраструктури з боку російської федерації. Згідно зі звітом Microsoft про цифровий захист за 2022 рік, кібератаки, спрямовані на критичну інфраструктуру в усьому світі, становили до 40 % усіх атак на національні держави. Це сталося в основному через те, що російські хакери атакували українську інфраструктуру та союзників України у триваючій війні [1].

Сьогодні Україна стоїть на передовій лінії, і колись у всьому світі будуть ретельно вивчатися саме її передові практики щодо протистояння кібератакам на критичні інфраструктури. Але ми вважаємо, що наразі нам слід знати та ефективно впроваджувати увесь накопичений у світі досвід боротьби з кібератаками на критичні інфраструктури.

За даними Агентства з кібербезпеки та безпеки інфраструктури США [2], у державі розрізняють 16 секторів критичної інфраструктури:

– хімічний сектор;
– сектор комерційних об'єктів;
– сектор зв'язку;
– критичний виробничий сектор;
– сектор дамб;
– сектор оборонно-промислової бази;