УДК 342.951
DOI https://doi.org/10.24144/2307-3322.2022.76.2.8

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО ТА ІНФОРМАЦІЙНА БЕЗПЕКА. НОВІ ВИКЛИКИ ТА ШЛЯХИ ПОДОЛАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Килимник І.І.,
кандидат юридичних наук, доцент, завідувач кафедри правового забезпечення господарської діяльності,
Харківський національний університет міського господарства імені О.М. Бекетова
https://orcid.org/0000-0003-3225-6257
Kilimnikinna1@gmail.com

Килимник І.І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз.

У статті проаналізовано поняття «інформаційне суспільство», «інформація», «інформаційна безпека». Метою статті є розв'язання проблеми забезпечення інформаційної безпеки як ключового напряму розвитку інформаційного суспільства, та визначення основних напрямків правового забезпечення інформаційної безпеки з урахуванням досвіду країн Європейського Союзу.

У статті досліджено взаємозв'язок інформаційного суспільства та інформаційної безпеки, який підкреслює зростаючу важливість інформаційної безпеки в епоху цифрових технологій і ризики, пов'язані з кіберзагрозами. Розглядається роль інформаційних технологій у сприянні обміну інформацією та виклики, які виникають у зв'язку з використанням таких технологій.

У статті також стверджується, що зростання інформаційного суспільства призвело до зростання кіберзагроз, які становлять значний ризик для безпеки інформації, підкреслюється важливість заходів інформаційної безпеки для захисту конфіденційної інформації та захисту від кібератак. У статті також підкреслюється необхідність усвідомлення окремими особами та організаціями ризиків, пов'язаних із використанням інформаційних технологій, і вжиття проактивних заходів для пом'якшення цих ризиків.

Загалом стаття підкреслює важливість інформаційної безпеки в інформаційному суспільстві та необхідність для окремих осіб і організацій брати на себе відповідальність за захист своєї конфіденційної інформації. Основні складові інформаційної безпеки – це сукупність елементів, що включає відкритість, конфіденційність та цілісність інформаційних ресурсів та підтримуючої інфраструктури. Вивчення досвіду зарубіжних країн необхідно для створення оптимальної системи правового забезпечення інформаційної безпеки України. Європейська модель розвитку інформаційного суспільства, яка характеризується соціальною орієнтацією і активним залученням держави та міжнародних інституцій, є найбільш оптимальною для України.

Ключові слова: інформація, інформаційне суспільство, інформаційна безпека, інформаційні ресурси.

Kilimnik I. Information society and information security. New challenges and new ways to overcome the information threats.

The article analyzes the concepts of "information society", "information", "information security". The purpose of the article is to solve the problem of ensuring information security as a key direction in the development of the information society, and to determine the main directions of legal provision of information security, considering the experience of the countries of the European Union.

The article explores the relationship between the information society and information security, highlighting the growing importance of information security in the digital age and the risks associated with cyber threats. The role of information technologies in facilitating the exchange of information and the challenges that arise in connection with the use of such technologies are considered.

The article also argues that the growth of the information society has led to an increase in cyber threats that pose a significant risk to information security, emphasizing the importance of information security measures

to protect sensitive information and protect against cyber attacks. The article also emphasizes the need for individuals and organizations to be aware of the risks associated with the use of information technology and to take proactive measures to mitigate these risks.

Overall, the article emphasizes the importance of information security in the information society and the need for individuals and organizations to take responsibility for protecting their confidential information. The main components of information security are a set of elements that includes openness, confidentiality and integrity of information resources and supporting infrastructure. Studying the experience of foreign countries is necessary to create an optimal system of legal support for information security of Ukraine. The European model of information society development, which is characterized by social orientation and active involvement of the state and international institutions, is the most optimal for Ukraine.

Keywords: information, information society, information security, information resources.

Постановка проблеми. Поняття «інформаційне суспільство» з'явилося в процесі наукового опрацювання змін у житті суспільства, які стали проявлятися з настанням останньої третини минулого століття, особливо на межі XX і XXI століть. Домінування інформації і знань у функціонуванні та розвитку різних сфер суспільного життя (матеріальне виробництво, зайнятість і соціальна структура, професійна діяльність і спосіб життя, культура, комунікації та ін.) є основою цих змін. Зазначені зміни торкнулися майже всіх сфер суспільного життя. Так, в економічній сфері, інформаційні продукти і послуги в останні роки стали відігравати ключову роль у валовому внутрішньому продукті. У політичній сфері доступність інформації, що стосується державної діяльності і політичних процесів, розширює можливості для встановлення ефективного зворотного зв'язку влади і населення, що сприяє розвитку соціальних ініціатив і громадянського суспільства. У сфері комунікацій: значне розширення можливості спілкування і взаємодії в діапазоні від міжособистісного спілкування за допомогою чатів, -блогів, Інтернет-форумів, онлайн-конференцій до взаємодії за допомогою так званих інформаційних мереж в межах глобального інформаційного простору на міждержавному і міжкультурному рівні.

Аналіз джерел. Термін «інформаційне суспільство» запропонований японським теоретиком К.Коямою. В Японії ще в 1972 була прийнята програма «План інформаційного суспільства: національна мета до 2000 р», на основі праць теоретика. Однак вперше термін «інформаційне суспільство» використав професор Токійського технологічного інституту Ю. Хаяші в 1969 році. Велику роль в затвердженні та популяризації цієї концепції зіграла робота іншого японського дослідника І. Масуди «Інформаційне суспільство як постіндустріальне суспільство», а також книги західних футурологів О. Тофлера, Дж. Нейсбіта і ін. [1] З початку 90-х років минулого століття цей термін увійшов в широкий науковий обіг.

Завданням статті є розв'язання проблеми забезпечення інформаційної безпеки як ключового напряму розвитку інформаційного суспільства, та визначення основних напрямків правового забезпечення інформаційної безпеки з урахуванням досвіду країн Європейського Союзу.

Виклад матеріалу. Інформаційна безпека – це сукупність методів, способів та дій, орієнтованих на захист від несанкціонованих дій із даними. Закон України «Про інформацію» визначає, що інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2]. Інформація є відомостями, що передаються в усній та письмовій формах за допомогою знаків, технічних механізмів, жестів, програм.

Інформація та складові її принципи досі вивчаються експертами для підвищення ефективності зберігання та використання даних.

Інформація, безпеку якої необхідно забезпечити, використовується у різноманітних сферах життя: політичній, економічній, соціальній та духовній. Важливо оберігати її від витоку, щоб мінімізувати можливі несприятливі наслідки.

Інформація вважається безпечною, якщо вона у повному обсязі захищена від будь-яких видів загроз. Найпоширенішими вважаються випадки витоку інформації про платежі та персональні дані (близько 80 % випадків). Правильний підхід у забезпеченні захищеності – це здійснення запобіжних заходів, здатних зменшити згубний вплив усередині та зовні системи.

Також є більш вузьке значення інформаційної безпеки:

Інформаційна безпека – це практична діяльність, спрямована на попередження недозволеного доступу, застосування, виявлення та перетворення даних. Внутрішні та зовнішні інформаційні загрози можуть завдати шкоди загальнодержавним та міжнародним відносинам, конкретним громадянам.

Захист інформації – сукупність юридичних, технічних та організаційних засобів попередження несанкціонованих дій з даними. Вона встановлюється в інформаційних системах та характеризується комплексом заходів та дій, спрямованих на захист даних від стороннього впливу.

Інформаційна безпека - це також наука про забезпечення збереження ресурсів інформації, недоторканності волі, законних прав особи та суспільства. Проникнення в інформаційний простір – це відкрита (іноді латентна) дія, яка спеціально або збіг обставин впливає на об'єкт захисту, що призводить до витоку або розкриття інформації. Безпека інформаційних технологій базується на наступних вступних:

1. Навіщо, кого та що захищати?
2. Від яких зовнішніх та внутрішніх факторів уберігати?
3. Яким чином провадити захист від загрози?

Основні складові інформаційної безпеки – це сукупність елементів, що включає відкритість, конфіденційність та цілісність інформаційних ресурсів та підтримуючої інфраструктури. До елементів безпеки часто відносять захист від несанкціонованого доступу, що є ключовою складовою захищеності даних.

Розглянемо систему основних складових інформаційних даних:

- Доступність – це ознака, що дозволяє користувачам у певних випадках безперешкодно отримати інформацію, що їх цікавить. Винятком є дані, приховані від загального огляду, розголошення яких може завдати серйозної шкоди суб'єктам та інформації. Наприклад, доступними є матеріали, які може одержати кожна людина: купівля квитків, послуги у банках, оплата комунальних платежів.
- Цілісність – один із елементів інформації, що гарантує її стабільність при навмисному (ненавмисному) перетворенні чи знищенні певних даних. Вона буває статичною (стабільність основних об'єктів від початкового стану) та динамічною (точна реалізація послідовних дій). Якщо буде порушено єдність інформації, це може призвести до серйозних негативних наслідків. Ця характеристика є основною та актуальною в інформаційному просторі.
- Конфіденційність – основна властивість, що дозволяє доступ до інформації виключно юридично-правомочним суб'єктам: клієнтам, платформам (програмам), процесам. Конфіденційність – це найдослідженіший, опрацьований аспект інформаційної безпеки.

Метою конфіденційної інформації є обмеження доступу осіб до даних, юридичний режим яких встановлено спеціалізованими нормативними актами у загальнодержавних та недержавних галузях, промисловості та соціальній діяльності.

Особливої актуальності інформаційна безпека набуває в умовах приєднання України до глобальної кіберцивілізації – рівню розвитку інформаційного суспільства, за якого ефективність життєдіяльності його складових визначається досягненнями науково-технічного прогресу: освоєнням комп'ютерних інформаційних технологій як засобів глобальної телекомунікації [3]. На тлі становлення глобального інформаційного суспільства та входження України у світовий інформаційний простір особливу актуальність набуває підвищення ефективності правового регулювання інформаційної безпеки. Тим більше, що людина, його життя та здоров'я, честь та гідність, недоторканність та безпека зізнаються в Україні найвищою соціальною цінністю [4]. Найважливішою ознакою інформаційного суспільства є можливість кожного створити інформацію та знання, мати до них доступ, користуватися та обмінюватися ними. Основна мета інформаційного суспільства – надати можливість людям реалізовувати свій інтелектуальний потенціал, свої можливості та здібності, сприяючи постійному розвитку та підвищення рівня свого життя. У практиці формування інформаційного суспільства у різних країнах виділяють три основні моделі: європейську, американську та азіатську.

Європейська модель розвитку інформаційного суспільства характеризується соціальною орієнтацією і активним залученням держави та міжнародних інституцій. Органи ЄС реалізують низку програм розвитку інформаційного суспільства та створення єдиного європейського інформаційного простору. Ці програми орієнтовані на забезпечення прав і свобод громадян, розвитку інформаційної інфраструктури, вільного доступу до неї та поінформованості товариства, створення пільгових умов для розвитку підприємництва у сфері інформаційних технологій. Ознакою європейської моделі інформаційного суспільства є варіативність політичної спрямованості програм побудови та розвитку національних складових об'єднаної Європи, зумовлених новою регіональною геополітикою, становленням інформаційною (інтелектуальної) економіки держав, інформаційного законодавства, різними можливостями пост-індустріального розвитку [1].

Американська модель відрізняється тим, що основне навантаження щодо інформатизації, розвитку інформаційної інфраструктури припадає на приватний сектор. Держава забезпечує регулювання інформаційної діяльності, вільну конкуренцію, бере участь у реалізації найбільш масштабних проектів. Враховуючи передову роль приватного сектора, ця модель є більш комерціалізованою, тобто орієнтованою на насичення ринку комерційними інформаційними продуктами та послугами.

Для азіатської моделі характерно те, що більшість питань інформатизації вирішуються в справах взаємодії держави та великих корпорацій. Крім цього, приділяється увага також забезпечення повсякденних потреб суспільства, доступності інформаційних продуктів та послуг.

Україна не стоїть осторонь процесу формування інформаційного суспільства. Одним з головних пріоритетів є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати знання та інформацію, мати вільний доступ до них, обмінюватися, користуватися ними, сприяючи таким чином суспільному та особистому розвитку та підвищенню якості життя. Більше того, в Україні сформовано правові засади побудови інформаційного суспільства: прийнято закони України «Про Концепцію Національної програми інформатизації» та «Про Національну програмі інформатизації», інші нормативні правові акти, які регулюють громадські відносини щодо створення інформаційних електронних ресурсів, захисту інтелектуального власності на ці ресурси, запровадження електронного документообігу, захисту інформації. Ці та інші передумови дозволяють вважати, що український ринок інформаційно-комунікаційних технологій перебуває у стані активного становлення і може стати фундаментом розвитку інформаційних технологій інформаційного суспільства в Україні.

Наразі, Україна все більш активно намагається привести усі сфери діяльності до європейських нормативів та стандартів. Це пов'язано з активним розвитком нашої країни та її активною співпрацею з Європейським союзом. Окрім того, швидкість розвитку цифрового забезпечення збільшується. Саме тому виникає необхідність всебічного вивчення досвіду міжнародно-правового забезпечення інформаційної безпеки, його систематизація, формування стратегій для подальшого вдосконалення національної системи забезпечення інформаційної безпеки, з обов'язковим врахуванням тенденцій розвитку України.

Незважаючи на те, що проблематика інформаційної безпеки привертає значну увагу дослідників та науковців, наразі досі відсутнє єдине та системне наукове дослідження питання вдосконалення правового забезпечення інформаційної безпеки України з урахуванням досвіду зарубіжних країн, а особливо країн Європи.

Дослідження досвіду зарубіжних країн у сфері забезпечення інформаційної безпеки в першу чергу необхідно почати з 1991 року, коли країни Європи (на той момент, ще не Європейського Союзу) розробили перший стандарт інформаційної безпеки «Європейські критерії безпеки інформаційних технологій». У цьому документі було визначено задачі забезпечення інформаційної безпеки, а саме захист інформаційних ресурсів від несанкціонованої модифікації чи знищення, задля забезпечення конфіденційності та цілісності інформаційних ресурсів, а також забезпечення працездатності усіх систем за допомогою протидії загрозам відмови в обслуговуванні. А вже у 1996 році, після створення Європейського Союзу, стандарти інформаційної безпеки були офіційно опубліковані в документі «Єдині умови безпеки інформаційних технологій». Відповідно до нього, для опису основних критеріїв інформаційної безпеки було застосовано модель тріади CIA (CIA TRIAD). Основними характеристиками інформаційної безпеки цієї моделі є:

- конфіденційність;
- цілісність;
- доступність.

Пізніше, в 2001 році Європейською Комісією було представлено документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», у якому було визначено сучасний підхід Європейського Союзу до проблем у сфері інформаційної безпеки. Цей документ визначив основні напрями європейської політики у сфері інформаційної безпеки, а саме підвищення обізнаності усіх користувачів про можливість загрози під час роботи з комунікаційними мережами; створення єдиної європейської системи інформування та попередження щодо нових загроз; забезпечення всебічної технологічної підтримки; підтримка та просування ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, протидія кіберзлочинності; зміцнення інформаційної безпеки загалом на державному рівні шляхом впровадження ефективних та єдиних засобів забезпечення інформаційної безпеки та заохочення до використання електронних

підписів при наданні державних онлайн послуг країн-членів тощо; розвиток міжнародного співробітництва у сфері інформаційної безпеки.

Європейські стандарти інформаційної діяльності органів державної влади передбачають їхню тотальну інформаційну відкритість, за винятком обмежень, пов'язаних з дотриманням конфіденційності інформації (в першу чергу, забезпечення безпеки персональних даних). Директива 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних та вільного обігу таких даних» є основним документом, який регулює право громадян країн Європейського Союзу на захист персональних даних. Обов'язково необхідно відзначити одне з положень, а саме «Принцип гарантованої безпеки № 11», воно вимагає, щоб персональні дані були захищені розумними засобами безпеки від усіх видів загроз, наприклад таких, як втрата даних, несанкціонований доступ, руйнування, використання, модифікація або розголошення. Нові правила захисту персональних даних, були схвалені 14 квітня 2014 році, та набули чинності у 2018 році. Нововведенням у них стало запровадження більш суворого покарання за несвоєчасне повідомлення інформації щодо витіку даних. Ця директива передбачає необхідність отримання згоди користувачів на обробку їх персональних даних, яка має бути вільною, свідомою та конкретною, а також може бути відкликана у будь-який момент.

Висновки. Проаналізувавши ці положення, необхідно відзначити, що розробка правового регулювання та узгодження відповідних стандартів щодо забезпечення інформаційної безпеки, у тому числі безпеки інформаційних технологій, у країнах Європейського Союзу почала розвиватися набагато раніше, ніж в Україні, тому має більш системний та ґрунтовний характер. Окрім того, нормування забезпечення інформаційної безпеки в Європейському Союзі є більш чітким і структурованим. В першу чергу, це чітко визначені основні поняття та категорії, здійснення викладення переліку відповідних загроз інформаційній безпеці, наприклад, персональних даних особи тощо. На прикладі оцінки роботи системи в окремих країнах Європейського союзу, а саме Німеччини та Польші, можна зробити висновок, що для досягнення мети забезпечення інформаційної безпеки в будь-якій сфері суспільного життя необхідне чітке та злагоджене функціонування суб'єкта забезпечення такої безпеки, який наділений виключно спеціалізованими повноваженнями. Саме спеціалізований орган може найбільш ефективно дотримуватися забезпечення інформаційної безпеки, оскільки він здійснює накопичення спеціального досвіду, удосконалення освітньої, технічної, матеріальної, практичної бази, а також багажу від взаємодії з іншими суб'єктами правових відносин у державі та суб'єктів міжнародного права. На прикладі Німеччини чітко можна визначити те, що належною підставою для подальшого ефективного функціонування правового механізму забезпечення інформаційної безпеки в державі є, в першу чергу, ефективне та якісне нормативно-правове регулювання.[5, 6]. Однією з найважливіших тенденцій, яку необхідно запозичувати в Польщі в контексті забезпечення інформаційної безпеки, є активне залучення до усіх процесів недержавних суб'єктів, насамперед членів громадянського суспільства. Після аналізу такого впровадження і в інших країнах, необхідно відзначити позитивний вплив на усю сферу загалом, а також, що забезпечення інформаційної безпеки здійснюється шляхом прийняття насамперед ключового стратегічного документа, який спрямовує діяльність усіх суб'єктів забезпечення інформаційної безпеки, визначає ключові напрямки зазначеної діяльності та завдання, поставлені перед механізмом забезпечення інформаційної безпеки.

Таким чином, вивчивши досвід зарубіжних країн можна запропонувати окремі європейські методики для створення оптимальної системи правового забезпечення інформаційної безпеки України.

Список використаних джерел:

1. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : монографія. Київ, 2010.
2. Закон України «Про інформацію». *Відомості Верховної Ради (ВВР).* 1992. No 48. Ст. 650.
3. Цимбалюк В.С. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. *Науковий вісник академії ДПС України*. 2007. No 4. С. 174–178.
4. Конституція України. Відомості Верховної Ради (ВВР). 1996. No 30. Ст. 141.
5. Ткачук Т.Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. *Юридичний науковий електронний журнал.* 2017. № 5. URL: http://lsej.org.ua/5_2017/30.pdf.
6. Салаев Т.Г. Опыт зарубежных стран в контексте усовершенствования административно-правового обеспечения информационной безопасности в Украине. *Часопис Київського університету права.* 2020. № 5. С. 403–407.