УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2023-12/27

ДЕЯКІ АСПЕКТИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

SOME ASPECTS OF REGULATORY AND LEGAL SUPPORT OF INFORMATION TECHNOLOGIES IN THE CONTEXT OF INFORMATION SECURITY OF UKRAINE

Садковський С.П., аспірант кафедри галузевого права та загальноправових дисциплін
Заклад вищої освіти «Відкритий міжнародний університет розвитку людини «Україна»

У цій статті проаналізовано деякі нормативно-правові документи у сфері інформаційних технологій та інформаційної безпеки.

Висвітлено, що під нормативно-правовим забезпеченням інформаційних технологій в Україні розуміється форма владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування та ефективного забезпечення.

Визначено поняття інформаційної безпеки. Інформаційна безпека – це стан захищеності інформації особистості, суспільства та держави від випадкових або цілеспрямованих впливів природного або штучного характеру з можливістю нанесення ними критичної та непоправної шкоди для суб'єктів інформаційних відносин.

Проаналізовано низку законів України, в тому числі закон України «Про захист інформації в автоматизованих системах» № 81/94-ВР від 05.07.1994 р. який регулює правові відносини у сфері захисту інформації за умови дотримання права власності на інформацію фізичних та юридичних осіб, права доступу і обмеження на доступ до неї. Закон гарантує, що без дозволу власника доступ до інформації, яка обробляється в автоматизованих системах, здійснюється лише згідно з правилами розмежування доступу.

Розглянуто, що інформаційні технології, які використовуються окремими користувачами в інформаційному просторі, зобов'язані відповідати вимогам та критеріям зовнішньої безпеки використання та внутрішньої безпеки їхньої будови. Виходячи з цього, по всьому світу проводиться безліч досліджень комп'ютерних пристроїв та операційних систем, а також на їх основі доповнюються та змінюються вже існуючі міжнародні акти у сфері інформаційної безпеки.

Узагальнено, що безпека інформаційних технологій та систем є однією із найважливіших складових проблеми забезпечення безпеки. Перехід до нових форм управління в Україні в умовах дефіциту та суперечливої правової бази призвів до низки проблем з погляду захисту даних та інформації. Це своєрідність формування відносин, відсутність обґрунтованих концепцій реформ та відставання у сфері застосування сучасних інформаційних технологій. Загострення цих проблем висвітлило питання національної, соціальної та корпоративної безпеки, у тому числі в інформаційній сфері.

Ключові слова: інформаційні технології, нормативно-правове забезпечення, інформаційна безпека, інформація, суспільство, інформаційна сфера, безпека, закон України, законодавство.

This article analyzes some regulatory and legal documents in the field of information technology and information security.

The author highlights that the regulatory and legal support of information technologies in Ukraine is understood as a form of governmental legal influence on public information relations exercised by the State with a view to their regulation and effective provision.

The concept of information security is defined. Information security – is the state of protection of information of an individual, society and the State from accidental or targeted natural or artificial influences with the possibility of causing critical and irreparable damage to the subjects of information relations.

The author analyzes a number of laws of Ukraine, including the Law of Ukraine "On Protection of Information in Automated Systems" № 81/94-BP from 05.07.1994, which regulates legal relations in the field of information protection subject to the right of ownership of information of individuals and legal entities, the right of access and restrictions on access to it. The law guarantees that without the owner's permission, access to information processed in automated systems is carried out only in accordance with the rules of access control.

The author considers that information technologies used by individual users in the information space must meet the requirements and criteria of external security of use and internal security of their structure. On this basis, a lot of research is being conducted around the world on computer devices and operating systems, and on their basis, existing international acts in the field of information security are being supplemented and amended.

In general, the security of information technologies and systems is one of the most important components of the security problem. The transition to new forms of governance in Ukraine in the context of a deficient and contradictory legal framework has led to a number of problems in terms of data and information protection. These include the peculiarity of the formation of relations, the lack of sound reform concepts, and the lag in the use of modern information technologies. The aggravation of these problems has highlighted the issues of national, social and corporate security, including in the information sphere.

Key words: information technology, regulatory support, information security, information, society, information sphere, security, legislation.

Постановка проблеми. Важливим чинником розвитку сучасного суспільства є його трансформація в інформаційний простір. Однією із провідних функцій цих перетворень є забезпечення зв'язку між державними органами влади, установами і організаціями та суспільством. Інформаційні технології, які використовуються окремими користувачами в інформаційному просторі, зобов'язані відповідати вимогам та критеріям зовнішньої безпеки використання та внутрішньої безпеки їхньої будови.

Аналіз останніх досліджень та публікацій. У наукових працях вітчизняних науковців практично відсутні комплексні дослідження, що присвячені аналізу нормативно-правової бази України у сфері інформаційних технологій. Цій проблематиці присвячена низка наукових праць провідних зарубіжних та вітчизняних науковців, серед них: Краснер Г. Е., Поп С. Т., Ліпкан В. А., Максименко Ю. Є., Ситніченко В. Г., Пацера М. Проте залишаються питання, що потребують подальшого вивчення та аналізу.

Мета статті проаналізувати нормативно-правову базу України у сфері інформаційних технологій.

Виклад основного матеріалу. За роки незалежності в Україні відбулися достатньо вагомі зміни у нормативно-правовому забезпеченні у сфері інформаційних технологій. Під нормативно-правовим забезпеченням інформаційних технологій в Україні розуміється форма владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування та ефективного забезпечення [1].

Розвиток інформаційного сектору став невід'ємною частиною життя сучасного суспільства, а оскільки інформація є одним із найцінніших та найважливіших ресурсів будь-якого процесу.

Інформаційна безпека включає комплекс заходів, спрямованих на запобігання та усунення несанкціонованого доступу, обробки, спотворення, форматування, аналізу, неузгодженого оновлення, виправлення та знищення даних. Простіше кажучи, це набір заходів, стандартів та технологій, необхідних для захисту конфіденційних даних.

У цьому контексті розглянемо поняття «інформаційна безпека». Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих суб'єктів інформаційних ресурсів, інформаційних технологій та законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах [2].

Отже, інформаційна безпека – це стан захищеності інформації особистості, суспільства та держави від випадкових або цілеспрямованих впливів природного або штучного характеру з можливістю нанесення ними критичної та непоправної шкоди для суб'єктів інформаційних відносин [3].

Згідно з Закону України «Про інформацію» захист інформації представляє собою прийняття правових, організаційних та технічних заходів, спрямованих на: 1) реалізацію захисту інформації та від несанкціонованого доступу, видалення, зміни, передачу, копіювання, закриття доступу та інших можливих незаконних дій стосовно інформації; 2) ригоризм дотримання захищеності інформації закритого доступу; 3) здійснення законного права на доступ та використання інформації. Основне завдання інформаційної безпеки – мінімізація та запобігання ризиків та загроз, а не ліквідація наслідків. Саме прийняття превентивних заходів щодо забезпечення конфіденційності цілісності та доступності інформації є найбільш дієвим підходом під час створення системи інформаційної безпеки . Об'єктами інформаційної безпеки є те, на що спрямовані дії негативного характеру завдають шкоди та дії , що запобігають перші. Об'єкти, на яких зосереджені негативні наслідки в інформаційній сфері, є: 1) всі види джерел інформації – інформація, записана на матеріальному носії з реквізитами, що дозволяють їх ідентифікувати; 2) система створення, поширення та використання інформації (інформаційні системи та технології, ЗМІ, бібліотеки, архіви, кадри, нормативні документи тощо) [4].

Жодна система не може існувати без інформаційних потоків, порушення або їх недостатність призводить до збоїв і втрат в ефективності та рентабельності, зниження динаміки розвитку. Інформація є найважливішим складником будь-якої системи. Інформаційна сфера є системним фактором життя суспільства та активно впливає на стан політичної, економічної, оборонної та інших складових безпеки, особливо під час війни на території України.

Проблема забезпечення національних інтересів і національної безпеки в інформаційній сфері поки перебуває на стадії становлення. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері. Для створення і підтримання належного рівня національної безпеки в інформаційній сфері розробляється система правових норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності органів державного управління, формуються або перетворюються органи та сили забезпечення інформаційної безпеки і механізм контролю та нагляду за їх діяльністю.

Під суб'єктами інформаційних відносин розуміються як власник, так і користувачі інформації та підтримуючої інфраструктури. Для того, щоб регулювати поведінку суб'єктів інформаційної сфери існує низка нормативно-правових актів з метою реалізації прав та обов'язків, які спрямовані на забезпечення захисту об'єктів правовідносин. Тут же законодавець вводить обмеження на інформаційні права та свободи з метою захисту інтересів громадян, суспільства та держави. При формуванні норм права, встановлення прав та обов'язків застосовуються методи цивільного, адміністративного та конституційного права. Для забезпечення інформаційної безпеки в Україні в цілому, так її суб'єктів та об'єктів на законодавчому рівні були прийняті наступні нормативно-правові акти: Закон України «Про інформацію» від 02.10.1992 № 2657-XII; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР; Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII; Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, Цивільний кодекс України [4, 5, 6, 7, 8].

Таким чином, сфера інформаційної безпеки має досить велику законодавчу базу, яка безсумнівно розвивається. Для цього враховуються всі основні аспекти захисту інформації, які теж, у свою чергу, не перестають удосконалюватися . Необхідно брати до уваги основні категорії інформаційної безпеки, відомі ще з кінця минулого століття та доопрацьовувати їх , шукаючи нові, менше витратні та більше ефективні способи вирішення проблем [9].

Закон України «Про захист інформації в автоматизованих системах» № 81/94-ВР від 05.07.1994 р. регулює правові відносини у сфері захисту інформації за умови дотримання права власності на інформацію фізичних та юридичних осіб, права доступу і обмеження на доступ до неї. Закон гарантує, що без дозволу власника доступ до інформації, яка обробляється в автоматизованих системах, здійснюється лише згідно з правилами розмежування доступу [10].

Майкл Шредер та Джері Зальцер 1975 року у статті « Захист інформації в комп'ютерних системах» стали першими у світі, хто класифікував збої в отриманні, зберіганні та передачі інформації, розділивши їх умовно на три категорії: неавторизований відмова у доступі до інформації, неавторизована розкриття інформації та неавторизоване зміна інформації. Після цього дану класифікацію удосконалили та стандартизували як вид, яким користуються і досі як основним:

1. Конфіденційність (анг. confidentiality) – здатність інформації бути недосяжною для третіх осіб або процесів, іншими словами, бути доступною тільки для авторизованих та допущених до системи осіб. Цей компонент є основним та першорядним в інформаційній середовищі . Однак перед фактичним використанням розроблених заходів щодо її реалізації в Україні постає велика кількість перешкод та проблем. Наприклад , відомості про технічні шляхи втрати інформації є закритими для сторонніх осіб, через що безліч легальних користувачів не мають можливості оцінити можливі ризики. Також існує цілий ряд юридичних та технічних проблем, які перешкоджають самостійній криптографії як основний інструмент для захисту персональних даних.

2. Цілісність (анг. integrity) – здатність інформації зберігати правильність та цілісність активів, тобто властивість інформації, яка характеризує його стійкість до випадкового або навмисному знищення або нелегітимному перетворення. Даний критерій умовно ділиться на статичну та динамічну цілісність (незмінність інформаційних об'єктів і пов'язану з правильним виконанням транзакцій відповідно). Цілісність інформаційної безпеки стає самим головним аспектом у разі, коли за допомогою різної інформації та на її основі користувачі приймають рішення про подальші діях.

3. Доступність (анг. availability) – здатність інформації бути доступною та готовою до використання за запитом користувача, що має до неї доступ. Іншими словами, це властивість інформаційної системи та всіх її даних та процесів надати доступ або зробити обмін інформацією між зареєстрованими у спільній мережі користувачами. Основна мета інформаційного середовища щодо її користу-

вачів – це надання будь-яких легітимних інформаційних послуг, таких як передача, зберігання, обробка запитуваної інформації і так далі. Однак, якщо з якоїсь причини надання запитуваних послуг неможливо, то це завдає шкоди особам, які запросили інформацію [11].

Головна роль описуваного критерію особливо очевидна у таких типах систем управління як виробнича, транспортна тощо. У сукупності ці три ключові критерії інформаційної безпеки іменуються тріадою CIA. У 1998 році член Асоціації обчислювальної техніки, дослідник та консультант з інформаційної безпеки Донн Паркер доповнив тріаду CIA ще трьома пунктами: справжність, володіння та контроль, користь. Удосконалену модель назвали Паркерівською гексадою (від hexad з англ. – «Група із шести предметів»), продемонстровану відповідно до таблиці 1.

Інформаційні технології, які використовуються окремими користувачами в інформаційному просторі, зобов'язані відповідати вимогам та критеріям зовнішньої безпеки використання та внутрішньої безпеки їхньої будови. Виходячи з цього, по всьому світу проводиться безліч досліджень комп'ютерних пристроїв та операційних систем, а також на їх основі доповнюються та змінюються вже існуючі міжнародні акти у сфері інформаційної безпеки.

Безпека інформаційних технологій та систем – одна з найважливіших складових проблеми забезпечення безпеки. Перехід до нових форм управління в Україні в умовах дефіциту та суперечливої правової бази призвів до низки проблем з погляду захисту даних та інформації. Це своєрідність формування відносин, відсутність обґрунтованих концепцій реформ та відставання у сфері застосування сучасних інформаційних технологій. Загострення цих проблем висвітлило питання національної, соціальної та корпоративної безпеки, у тому числі в інформаційній сфері [13].

Таблиця 1

Модель Паркеровської гексади

Атрибут	Коментар
Справжність (автентичність)	Під атрибутом «справжність» розуміється заява про авторство та точність його походження. Наприклад, для того, щоб впевнитися у справжності підпису на паперовому чи електронному носії потрібно зробити звірку з тими документами, де вона вже була перевірена, або зробити звірку звичайного рукописного тексту де був поставлений підпис. У разі перевірки електронної інформації на авторство використовуються криптографічні програми з відкритим ключем.
Володіння та контроль	Це такий стан системи, при якому вибудовується зв'язок між особами, мають доступ до володіння та використання інформації між пристроєм чи фізичним носієм інформації, ухвала на санкціонованість доступу до певної інформації.
Користь	Під атрибутом «користування» розуміється стан системи, що забезпечує зручність для користувачів та співробітників використання системи. Так виникає менше бажання діяти в обхід даної системи.

Джерело: складено на основі [11]

Висновки. Отже, застосування інформаційних технологій у різні сфери діяльності є одним із найважливіших інструментів сталого розвитку країни, що сприяє підвищенню технологічного, економічного, соціального та культурного рівня загалом. Саме тому упорядкування законодавчої бази задля швидкого впровадження інформаційних технологій є надзвичайно актуальним завданням, яке потребує постійної уваги і певних зусиль, саме тому воно нині є пріоритетним.

ЛІТЕРАТУРА

1. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис. … канд. юрид. наук. К., 2007. 280 с.
2. Ліпкан В.А. Національна безпека України: Навч. посіб. К., 2009. 229 с.
3. Пацера М. Система управління інформаційною безпекою як важлива складова загальної системи управління банком. *Вісник* Національного банку України, № 6. 2015. С. 48–49.
4. Закон України «Про інформацію» № 2658-XII від 02.10.1992 р. *Верховна Рада України*. *Відомості Верховної Ради України*. 1992. № 48. URL: https://zakon.rada.gov.ua/laws/show/2657- 12#Text
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 р. *Верховна Рада України*. *Відомості Верховної Ради України*. 1994, № 31, ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
6. Закон України «Про державну таємницю» № 3855-XII від 21.01.1994 р. *Верховна Рада України*. *Відомості Верховної Ради України*. 1994, № 16, ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
7. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. *Відомості Верховної Ради України* (ВВР), 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Цивільний кодекс України. URL: http://zakon2.rada.gov.ua/laws/show/435–15
9. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту. К., 2013. 688 с.
10. Закону України «Про захист інформації в автоматизованих системах». № 81/94-ВР від 05.07.1994 р. *Відомості Верховної Ради України* (ВВР), 1994, № 31, ст. 287. URL: https://zakon.rada.gov.ua/laws/show/81/94-%D0%B2%D1%80#Text
11. Качинський А.Б. Безпека складних систем. К.: ТОВ «Видавництво «Юстон», 2017. 498 с.
12. Krasner, G.E., Pope, S.T. A cookbook for using the model-view controller user interface paradigm in Smalltalk-80, Journal of Object-Oriented Programming, № 1(3), 1998. С. 26–49.
13. Ситніченко В., Кісельова Г., Стоякін Є. Формування інформаційної безпеки на основі стандарту ISO/IEC 27001: 2005. Стандартизація. Сертифікація. Якість, № 2. 2010. С. 50–56.