УДК 342.9
DOI https://doi.org/10.32782/2408-9257-2024-4-13

Шевчук М. О.,
кандидат юридичних наук, докторант кафедри конституційного, адміністративного та фінансового права Хмельницького університету управління та права імені Леоніда Юзькова

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ

ORGANIZATIONAL AND LEGAL PRINCIPLES OF INFORMATION PROTECTION

У статті розглянуті організаційно-правові засади захисту інформації, як складової безпеки та інформаційні відносини в інформаційній сфері. Основою організаційних заходів є використання та створення законодавчих та нормативних документів у сфері інформаційної безпеки, що покликані на правовому рівні врегулювати доступ користувачів до інформації. Досліджено проблему захисту інформаційного простору. Організаційно-правові засади захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня інформаційної безпеки. Створити стовідсотковий захист інформації неможливо за жодних обставин, тому метою є досягнення не теоретично максимального рівня захисту, а скоріше мінімального, необхідного за даних конкретних умов і з огляду на рівень можливої загрози. Система захисту має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не вартістю його організації, а здатністю адекватно реагувати на всі загрози.

Організаційні засоби захисту – це засоби організаційного характеру, які регулюють функціональний процес системи обробки даних, використання її ресурсів, діяльність персоналу, а також послідовність взаємодії користувачів із системою з метою зробити реалізацію загроз інформаційній безпеці неможливою або настільки важкою, наскільки це можливо.

Правові заходи захисту інформації включають розробку норм, що визначають відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалення кримінального та цивільного законодавства, судочинства.

Проаналізовано теоретичні підходи до визначення сутності поняття комплексної система захисту інформації, розглянуто інформаційне право, як галузь юридичної науки, всебічно досліджені організаційні засади захисту інформації та реалізація інформаційних правовідносин, охарактеризовано специфіку організаційно-правових засад захисту інформації, надано практичні рекомендації щодо вдосконалення правої основи захисту інформації.

Ключові слова: *інформаційна безпека, інформаційні відносини, захист у сфері інформації, інформаційне право, інформаційно-правові норми, правові методи.*

The article deals with the organizational and legal framework for information protection as a component of security and information relations in the information sphere. The basis of organizational measures is the use and creation of legislative and regulatory documents in the field of information security, which are intended to regulate users' access to information at the legal level. The problem of information space protection is investigated. The organizational and legal framework for information security includes measures and actions to be taken by officials in the process of creating and operating a system to ensure a given level of information security. It is impossible to create one hundred percent protection of information under any circumstances, so the goal is not to achieve the theoretical maximum level of protection, but rather the minimum level necessary under the given specific conditions and given the level of possible threat. The protection system must be sufficient, reliable, effective and manageable. The effectiveness of information protection is measured not by the cost of its organization, but by the ability to adequately respond to all threats.

Organizational security measures are organizational measures that regulate the functional process of the data processing system, the use of its resources, the activities of personnel, as well as the sequence of user interaction with the system in order to make the implementation of information security threats impossible or as difficult as possible.

Legal measures to protect information include the development of rules that determine liability for computer crimes,

The article analyzes theoretical approaches to defining the essence of the concept of a comprehensive information security system, considers information law as a branch of legal science, comprehensively examines the organizational principles of information security and the implementation of information legal relations, characterizes the specifics of the organizational and legal principles of information security, and provides practical recommendations for improving the legal basis for information security.

Key words: *information security, information relations, protection in the field of information, information law, information and legal norms, legal methods.*

Постановка проблеми. Актуальність проблеми правового регулювання суспільних відносин у сфері інформаційної безпеки зумовлена підвищенням ролі інформації в усіх сферах і видах діяльності. Розвиток нових інформаційних відносин потребують збереження та захисту прав і законних інтересів суб'єктів інформаційної сфери.

Комплексна система захисту інформації складається з захисту від несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів, захисту інформації від витоку технічними каналами, захисту від спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Право людини на інформацію в цивільному законодавстві в широкому сенсі містить такі елементи, як безпосередньо право на інформацію – ст. 302 Цивільного кодексу України, право на інформацію про стан свого здоров'я – ст. 285 ЦК, право на таємницю про стан здоров'я – ст. 286 ЦК, право на особисте життя та його таємницю – ст. 301 ЦК, право на особисті папери й таємницю кореспонденції – ст. 303, 306 ЦК, право на свободу літературної, художньої, наукової та технічної творчості – ст. 309 ЦК, право на повагу до гідності й честі, недоторканність ділової репутації – ст. 297, 299 ЦК, право на достовірну інформацію про стан довкілля – ст. 293 ЦК [4].

Закон України «Про інформацію» від 02.10.1992р, № 2657-XII зі змінами й доповненнями, внесеними 23.06.2005р № 2707-IV, встановлює комплекс відносин, що виникають у сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації, закріплює право особи на інформацію.

Окремі положення правового регулювання відносин у сфері інформації відображено в указах та розпорядженнях Президента України, Постановах та розпорядженнях Кабінету Міністрів України, нормативних актах міністерств і відомств.

Стан опрацювання. У вітчизняній юридичній літературі проблема організаційно-правового захисту інформації, досліджується рядом вчених. Найбільш широко питання досліджували Р. Калюжний, В. Хавловський, В. Цимбалюк та М. Гуцалюк. У результаті досить серйозного аналізу інформаційного законодавства України автори підкреслюють складність застосування організаційно-правових заходів захисту інформації та методів провідних правових напрямків в інформаційному праві.

Інформаційне законодавство зароджується та розвивається в правовій системі держави, а тому система організаційно-правових заходів захисту інформації тільки напрацьовується та удосконалюється. Тому в рамках загальної проблеми дослідження організаційно-правового захисту інформації в України актуальним є завдання визначення цих заходів захисту інформації, їх переліку та змісту. Заходи з захисту інформації складають методологічну основу правозастосовної роботи, і від правильного вибору захисту значною мірою залежить ефективність інформаційних відносин.

Метою даного дослідження є конкретизація та визначення організаційно-правових заходів захисту інформації в Україні.

За своєю природою інформаційні відносини мають двоякий характер. З одного боку, вони мають самостійний, самодостатній характер, а з іншого боку відіграють допоміжну роль у здійсненні переважної більшості інших відносин у суспільстві. Насправді майже всі соціальні відносини передбачають інформаційні потоки або, іншими словами, інформаційні відносини.

Організаційні засоби захисту – це засоби організаційного характеру, які регулюють функціональний процес системи обробки даних, використання її ресурсів, діяльність персоналу, а також послідовність взаємодії користувачів із системою з метою зробити реалізацію загроз інформаційній безпеці неможливою або настільки важкою, наскільки це можливо. Організаційні принципи захисту даних, це захист від втрати даних через стихійні події, збоїв в електромережі, некомпетентність співробітників, захист від навмисного пошкодження комп'ютерних і мережевих пристроїв, крадіжки даних безпосередньо з пристроїв, захист від викрадення даних[12].

До організаційних заходів інформаційної безпеки належать також такі заходи як, обме-

ження доступу до приміщень, де готується та обробляється інформація, допуск лише перевірених посадових осіб, що мають право обробляти та передавати конфіденційну інформацію, зберігання носіїв інформації та журналів у сейфах, які зачиняються для сторонніх осіб, запобігання перегляду сторонніми особами вмісту оброблених матеріалів через дисплей, принтер тощо, використання криптографічних кодів при передачі цінної інформації по каналах зв'язку, запобігання знищенню матеріалів, що містять фрагменти цінної інформації. Регламентуються засоби захисту інформації, процеси функціонування інформаційної системи, використання її ресурсів, діяльність персоналу, а також порядок, у якому користувачі взаємодіють із системою таким чином, щоб ускладнити або запобігти порушенню безпеки.

Організаційні заходи захисту інформації включають комплекс заходів щодо відбору та перевірки персоналу, який бере участь у підготовці та реалізації програм та інформації, а також чітку регламентацію процесу розробки та функціонування інформаційної системи. Тільки комплексне використання різноманітних заходів може забезпечити надійний захист інформації, оскільки кожен метод чи захід має слабкі та сильні сторони.

Правові методи – це правила використання інформації та відповідальність за їх порушення. До правових методів захисту інформації належить патентний захист, закон про комерційну таємницю, ліцензійні угоди та контракти, закон про авторське право[8].

Реалізація інформаційних правовідносин неминуче охоплює цілий спектр суспільних відносин, які регулюються іншими галузями права. Тому організаційно-правові заходи захисту інформації називають комплексними. Захист інформаційних систем передбачений законодавством України. Може використовуватися альтернативна система захисту інформації відповідно до європейських стандартів ISO/IEC серії 27.

Деякі норми інформаційного права, поступово зростають, мають диспозитивний характер, згідно з яким суб'єкт інформаційного права отримує право обирати свою поведінку в його межах або ситуації.

Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», зареєстровані в Міністерстві юстиції України 22 червня 2015 року за № 736/27181 встановлюють єдині вимоги щодо створення управлінських документів і роботи зі службовими документами, а також порядок їх архівного зберігання в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях незалежно від форм власності. Обмеження доступу до інформації, що містять управлінські документи, і надання їм відповідних грифів («Для службового користування», «Конфіденційно», «Таємно» тощо) здійснюються відповідно до законодавства [7].

Проведення захисних заходів пов'язане з певними труднощами. Єдиної теорії системного захисту не існує, виробники засобів захисту пропонують переважно окремі засоби захисту. Принципи захисту відрізняються залежно від типу інформації. Стаття 32 Конституції України гарантує кожній людині право на таємницю її конфіденційної інформації та проголошує, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених у випадках зазначених у регламенті та лише в інтересах національної безпеки, економічного добробуту та прав людини.

Статтею 21 Закону України «Про інформацію» визначено: «Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено на умовах визначених законом». До конфіденційної інформації відноситься інформація, яка становить особисту або сімейну таємницю особи, наприклад інформація про сімейний стан, стан здоров'я, фінансовий стан, інформація про дату народження тощо, а також будь-яка інша інформація, яку особа бажає зберегти в таємниці.

Закон України «Про інформацію» регулює відносини щодо отримання та поширення інформації. Ст. 6 Закону України «Про інформацію» визначає зміст державної інформаційної політики, її головні напрями та способи.

Закон «Про захист персональних даних» визначає захист та обробку персональних

даних, закон «Про доступ до публічної інформації» дає право отримувати інформацію, якою володіють розпорядники. Для всіх розпорядників інформації Закон України «Про доступ до публічної інформації встановлює загальне правило обмеження доступу до публічної інформації, яке полягає в обов'язковому застосуванні положень частина 2 статті 6 Закону №2939-VI при розв'язанні питання доцільності обмеження доступу до публічної інформації шляхом віднесення її згідно із законом до таємної або службової». У частині четвертій статті 13 Закону «Про доступ до публічної інформації» зазначено, що «усі розпорядники інформації незалежно від нормативно-правового акту, на підставі якого вони діють, при розв'язанні питань щодо доступу до інформації мають керуватися цим Законом». Особа, якої стосується інформація, не має права визначати режим доступу до такої інформації[11].

Обмеженню доступу підлягає інформація, а не документ. Стаття 9 Закону України «Про доступ до публічної інформації» встановлює вимоги до офіційної інформації. Відповідно до вимог частини другої статті 6 цього закону до службової інформації може бути віднесено інформацію, що міститься в документах суб'єктів і являють собою внутрішньовідомчу службову кореспонденцію, звіти, рекомендації, якщо вони пов'язані з розробкою напрямів діяльності установи або виконанням органами державної влади контрольно-наглядових функцій, інформація зібрана в рамках оперативно-розшукової та контррозвідувальної діяльності у сфері оборони країни не віднесені до державної таємниці, мають гриф «для службового користування». Доступ до таких документів надається відповідно до частини другої статті 6 закону «Про доступ до публічної інформації».

Перелік відомостей, що становлять службову інформацію створюються органами державної влади, органами місцевого самоврядування та іншими суб'єктами владних повноважень. Керівник установи у встановленому порядку делегує повноваження щодо надання дозволу на користування, зберігання документів в системі безпеки керівникам структурних підрозділів, в яких документи опрацьовуються або зберігаються. Налаштування прав доступу співробітників до інформаційної системи в організації, налаштування обмеження доступу дозволяє забезпечити захист комерційних даних та безпеку.

Для запобігання несанкціонованому використанню даних застосовують криптографічний захист інформації. Криптографічний захист інформації реалізується у вигляді програм або пакетів програм, захищається безпосередньо сама інформація, а не доступ до неї, наприклад, зашифрований файл неможливо прочитати навіть у разі викрадення носія, зашифроване повідомлення можливо прочитати лише за наявності ключа, зміна ключа має призвести до значної зміни характеру зашифрованого повідомлення, навіть якщо використовується той самий ключ. При симетричному шифруванні створюється ключ, файл з цим ключем пропускається через програму шифрування і результат передається адресату, а сам ключ окремо передається адресату через інший безпечний канал зв'язку. При асиметричному шифруванні потрібні два взаємозалежних ключі, де закритий ключ відомий лише одержувачу повідомлення. Якщо не забезпечено досить надійне управління ключовою інформацією, то заволодівши нею, зловмисник отримує необмежений доступ до всієї інформації.

Управління ключами це інформаційний процес, що містить такі три елементи, як генерацію ключів, накопичення ключів, розподіл ключів. Вибір типу реалізації криптозахисту для конкретної інформаційної системи залежить від її особливостей і передбачає всебічний аналіз вимог, що пред'являються до системи захисту інформації.

Практично всі інформаційні дані зберігають на CD або DVD дисках, флешкартах, картах пам'яті, ноутбуках чи комп'ютерах. Вилучення інформації з електронних носіїв загрожує ослабленням або руйнуванням бізнесу через втрату конфіденційних даних, моральними, матеріальними витратами. Для інформаційно-телекомунікаційних систем із відкритою інформацією, що підлягає обов'язковому захисту, відповідно до НД ТЗІ 3.7-003-200543 має бути також передбачено створення комплексу засобів захисту від несанкціонованого доступу[6].

Створити стовідсотковий захист інформації неможливо за жодних обставин, тому метою є досягнення не теоретично мак-

симального рівня захисту, а скоріше мінімального, необхідного за даних конкретних умов і з огляду на рівень можливої загрози. Для додаткового захисту інформації необхідно забезпечення несанкціонованих утручань в інформаційну систему, резервування масивів інформації, використання засобів парольного захисту, блокування екрана та клавіатури. Для захисту інформації на рівні апаратного забезпечення використовуються апаратні ключі, системи сигналізації, засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

Система захисту має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не вартістю його організації, а здатністю адекватно реагувати на всі загрози. Власники та користувачі інформації оцінюють важливість інформації, щоб визначити відповідні заходи для її захисту. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373.

Правові заходи захисту інформації включають розробку норм, що визначають відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалення кримінального та цивільного законодавства, судочинства. До правових заходів відносяться також питання громадського контролю за розробниками комп'ютерних систем і прийняття міжнародних угод про обмеження дії, якщо розробники комп'ютерних систем зачіпають або можуть вплинути на військові, економічні та соціальні аспекти життя.

Закон «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Віднесення інформації до державної таємниці здійснює спеціальний суб'єкт – державний експерт з питань таємниць.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію» конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Порядок ведення обліку, зберігання, використання та знищення документів і інших матеріальних носіїв інформації, що містять службову інформацію, детально прописаний у типовій інструкції, затвердженій Постановою Кабінету Міністрів України від 19.10.2016 № 736.

Стаття 6 Закону України «Про поштовий зв'язок» від 4 жовтня 2001 року, зобов'язує операторів і провайдерів телекомунікацій вживати технічних та організаційних заходів, щодо захисту поштових відправлень, телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом та інформації, що передається цими мережами.

Законом «Про науково-технічну інформацію» регулюються правові та економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

Авторське право є інструментом, що дає можливість заробляти й отримувати справедливу частину винагороди за свої знання та досвід. 1 січня 2023 року набув чинності Закон України «Про авторське право і суміжні права».

Закон України «Про авторське право і суміжні права» регулював право на бази даних. Зараз вони захищені авторським правом, якщо розташування компонентів є результатом творчої діяльності.

Висновки. Організаційні заходи захисту інформації включають комплекс заходів. У міністерствах, відомствах і на підприємствах незалежно від форм власності і відповідно до законів та нормативно-правових актів створюються спеціальні служби безпеки для захисту інформації. Правові основи захисту інформації базуються на нормативно-правових актах, які закріплюють права і свободи людини та встановлюють відповідальність за злочини у сфері інформаційної безпеки. В Україні прийнято низку законів та нормативно-правових актів, щодо забезпечення інформаційної безпеки, і це закон «Про захист інформації в інформаційно-телекомунікаційних системах», закон «Про державну таємницю», закон «Про захист пер-

сональних даних», закон «Про авторське право і суміжні права». Виникає необхідність викладення Закону України «Про інформацію» та інших законів в новій редакції з урахуванням стандартів Ради Європи.

Інформаційна безпека це невід'ємна частина загальної системи безпеки країни і являє собою діяльність органів державної влади, недержавних структур і громадян в інформаційній сфері на основі законодавства та .

ЛІТЕРАТУРА:

1. Про інформацію: Закон України № 2658-XII (2658-12) від 02.10.92. *ВВР*, 1992, № 48, ст.651.

2. Бєликов К. Організаційно-правові проблеми формування державної інформаційної політики України. *Право України*. 2004. № 10. С 125-129.

3. Борисова Л. В. Правові заходи захисту інформації. Харків: ХНУВС, 2013. 212 с.

4. Вертузаєв О. Інформаційне право: риси інституціонального характеру змістовного інформаційного ресурсу України. *Юридична Україна.* 2016. №1. С.54-62.

5. Гетманцев Д. До питання про інформаційне право як самостійну галузь права України. *Підприємництво, господарство і право*. 2007. № 3. С.88-91.

6. Гонцяж Я С. Свобода інформації та навчання. Київ: Міленіум, 2009. С 25-129.

7. Логінова Н. І. Правовий захист інформації. Одеса : Фенікс, 2015. 264 с

8. Манжай О. В Правові заходи захисту інформації. Харків : Панов, 2020. 162с.

9. Мацюк В.Я. Інформаційне суспільство – новий щабель суспільної формації. *Часопис Київського університету права*. 2006. № 2. С.102-106.

10. Остапов С. Е. Технології захисту інформації. Харків : Вид. ХНЕУ, 2013. 476с.

11. Синєокий О. В. Інформаційне право. Запоріжжя : ЗНУ, 2008. 125 с.

12. Цимбалюк В.С. Основи інформаційного права України. Київ: Знання, 2004. 274 с.