УДК 342.95
DOI: 10.31733/17-03-2023-562-563

Олександр КАРПЕНКО
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

РОЛЬ ПРАВОВОГО РЕГУЛЮВАННЯ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Почнемо з того, що обрана тематика є дуже актуальною в сучасному світі, оскільки з розвитком технологій та інформаційного простору зростає кількість загроз інформаційній безпеці.

Інтернет, соціальні мережі та інші електронні засоби зв'язку стали невід'ємною частиною нашого життя, але водночас є потенційними джерелами ризиків і загроз для нашої приватності, конфіденційності та безпеки. За допомогою комп'ютерних технологій можна викрадати, розповсюджувати, підробляти, шкодити інформації, втручатися в особисте життя, відслідковувати користувачів та багато іншого.

Інформаційна безпека являє собою сукупність заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, зміни, втрати або руйнування. Це важливе явище, яке забезпечує захист інформації як ресурсу, який є одним з найважливіших для бізнесу, держави та громадян.

Заходи, які вживаються для забезпечення інформаційної безпеки, можуть включати в себе різні аспекти. Наприклад, це можуть бути технічні заходи, такі як захист комп'ютерних систем від хакерських атак та вірусів, захист мережі від несанкціонованого доступу та перехоплення інформації, а також шифрування інформації для захисту від несанкціонованого доступу [1, с.174].

Крім технічних заходів, важливим елементом інформаційної безпеки є правові заходи, такі як захист права на конфіденційність та особисте життя, захист права на інтелектуальну власність, а також захист персональних даних.

Інформаційна безпека є особливо важливою в умовах сучасного інформаційного суспільства, де інформація є основою бізнесу, науки та технологій, а також має значення для захисту національних інтересів та безпеки країни. Відсутність або недостатність заходів забезпечення інформаційної безпеки може призвести до серйозних наслідків, таких як виток конфіденційної інформації, порушення правил використання персональних даних, а також кібератаки на критичну інфраструктуру.

Процес забезпечення інформаційної безпеки - це системний підхід до забезпечення безпеки інформації, який включає в себе комплекс заходів технічного, організаційного та правового характеру для забезпечення конфіденційності, цілісності та доступності інформації.

Основні етапи процесу забезпечення інформаційної безпеки:

Аналіз загроз інформаційній безпеці - на цьому етапі встановлюються потенційні загрози для інформаційної безпеки, їхні наслідки та шляхи захисту.

Розробка політики інформаційної безпеки - на цьому етапі встановлюються загальні принципи та вимоги до забезпечення інформаційної безпеки, визначається порядок використання і захисту інформації, а також встановлюється система управління інформаційною безпекою.

Розробка технічних та організаційних заходів забезпечення інформаційної безпеки - на цьому етапі розробляються конкретні заходи для забезпечення безпеки інформації, такі як захист комп'ютерних систем від хакерських атак, встановлення систем контролю доступу до інформації, підвищення кваліфікації персоналу з питань безпеки інформації тощо.

Впровадження системи забезпечення інформаційної безпеки - на цьому етапі виконуються заходи з впровадження розроблених технічних та організаційних заходів, а також встановлюється система моніторингу та аналізу інформаційної безпеки [2, с.89].

Роль правового регулювання у забезпеченні інформаційної безпеки є надзвичайно

важливою, оскільки воно визначає правила використання інформації та відповідальність за її порушення. Правові акти, такі як закони, постанови, нормативні акти, регулюють використання технологій, захищають права на конфіденційність, інтелектуальну власність, персональні дані, встановлюють відповідальність за їх порушення, а також встановлюють механізми контролю за використанням інформації.

Наприклад, Закон України «Про захист персональних даних» встановлює правила збору, збереження, використання та захисту персональних даних громадян, які обробляються в Інтернеті та інших мережевих сервісах. Закон «Про інформацію» встановлює вимоги до забезпечення цілісності інформації, а також відповідальність за її порушення. Закон «Про основні засади забезпечення кібербезпеки України» визначає правила використання технологій та інформаційних систем, захисту від кіберзлочинів та кібератак, а також встановлює механізми координації дій забезпечення кібербезпеки.

Правове регулювання є важливим інструментом для забезпечення безпеки в інформаційному просторі, оскільки воно визначає правила використання інформації та встановлює відповідальність за її порушення. Встановлення надійних механізмів правового регулювання забезпечення інформаційної безпеки забезпечує захист інформації як ресурсу, який є одним з найважливіших для бізнесу, науки, технологій та держави в цілому. Необхідність правового регулювання пояснюється тим, що в сучасному інформаційному суспільстві інформація займає центральне місце і має значення для захисту національних інтересів, економічного розвитку, технологічного прогресу, інновацій та наукових досліджень.

Правове регулювання забезпечення інформаційної безпеки має на меті встановити стандарти і вимоги до зберігання, обробки, передачі та захисту інформації. Воно визначає обов'язки та права власників інформації, користувачів та постачальників послуг в галузі інформаційної безпеки. Правові норми, що регулюють інформаційну безпеку, також встановлюють механізми відповідальності за порушення правил забезпечення інформаційної безпеки [3, с.104].

Окрім цього, правове регулювання забезпечення інформаційної безпеки встановлює механізми контролю за використанням інформації, які є необхідними для забезпечення безпеки в інформаційному просторі. Такі механізми включають в себе системи моніторингу та аудитування, які дозволяють виявляти можливі порушення правил забезпечення інформаційної безпеки та приймати відповідні заходи для їх усунення.

Отже, правове регулювання є надзвичайно важливим для забезпечення інформаційної безпеки, оскільки воно визначає правила використання інформації та встановлює відповідальність за її порушення. Встановлення правових норм і механізмів контролю за їх дотриманням є необхідним для забезпечення захисту інформації як цінного ресурсу, який є ключовим для розвитку суспільства в цілому. Крім того, правове регулювання є важливим фактором створення довіри в інформаційному просторі, яке є передумовою для розвитку електронної комерції, електронного урядування та інших інформаційних послуг.

Забезпечення інформаційної безпеки є складним та багатоаспектним процесом, в якому принципово важливою є системність та комплексність підходу. Правове регулювання є одним з ключових елементів цього підходу, який визначає правила використання інформації, встановлює механізми контролю та відповідальності за її порушення, а також встановлює стандарти технічного та організаційного забезпечення безпеки інформації. Відповідальне виконання правових вимог щодо забезпечення інформаційної безпеки є важливим фактором для забезпечення ефективного захисту інформації та забезпечення довіри в інформаційному просторі.

1. Козаченко І. О. Роль правового регулювання у забезпеченні інформаційної безпеки держави. *Проблеми законності*. 2020. № 150. С. 170-175.

2. Черній А. Ю. Правове регулювання забезпечення інформаційної безпеки в Україні: актуальні питання. *Юридичний журнал*. 2021. № 1. С. 87-91.

3. Денисенко Л. О. Правове регулювання забезпечення інформаційної безпеки в Україні: проблеми та перспективи. *Вісник Харківського національного університету внутрішніх справ*. 2021. Вип. 97. С. 99-105.