

БАЗОВІ НАПРЯМИ ДЕРЖАВНО-ПРАВОВОЇ ПОЛІТИКИ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВИХ ПОСЛУГ В УКРАЇНІ

Передерій О. С.

*кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
Харківський національний університет імені В. Н. Каразіна
м. Харків, Україна*

Кулачок-Тітова Л. В.

*кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
Харківський національний університет імені В. Н. Каразіна
м. Харків, Україна*

Цифрові послуги як дороговартісний і складний технологічний інформаційний продукт може бути під загрозою неправомірного посягання, що, у свою чергу, тягне за собою комплексні ризики для системи кібербезпеки України. Задля недопущення цього, чинна Стратегія кібербезпеки України від 14.05.2021 р. передбачає систему організаційно-правових заходів забезпечення безпеки цифрових послуг [1]. У зазначеному документі визначено, що безпечні цифрові послуги досягаються шляхом забезпечення державою балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійністю та безпекою цифрових послуг протягом усього їхнього життєвого циклу. Вказане є однією з умов досягнення стану кіберстійкості держави.

Аналіз положень національного законодавства України дає підстави виокремити декілька базових організаційно-правових заходів убезпечення цифрових послуг від загроз. Зокрема, це

1) зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформування громадськості про їх безпечність та надійність. Зауважимо, що впродовж останніх п'яти років держава досягла певних позитивних результатів у справі довіри громадян до цифрових послуг. Так, Міністерство цифрового багато цифрових послуг для громадян і українського бізнесу. Зокрема, Україна стала першою країною у світі, в якій цифровий паспорт має таку ж силу, що й паперовий чи пластиковий

аналог. У застосунку «Дія» українці використовують 4,7 млн ID-карток, 12,2 млн закордонних паспортів та 6,6 млн водійських посвідчень, а серед найпопулярніших послуг для підприємців – реєстрація ФОП та ТОВ на порталі Дія, що є найшвидшою реєстрацією бізнесу у світі [2] Держава активно працює в напрямі забезпечення безпеки користувачів Дії (кілька разів було проведено програму Bug Bounty, в якій етичні хакери тестували застосунок і за винагороду в 1 млн гривень шукали вразливості, але не знайшли).

2) впровадження цифрових послуг для населення та розвитку національної інформаційної інфраструктури. Ключовим, системоутворюючим елементом національної інформаційної інфраструктури є створення інформаційного ресурсу і формування оптимального правового режиму його використання. Базові кроки у цьому напрямі було зроблено. Проте, найбільш серйозною проблемою зазначеного напрямку діяльності є галузевий принцип інформатизації державних органів, який досі зберігається. Наразі триває робота з усунення зазначених чинників і впровадження у національну правову систему інноваційних правових інститутів.

3) розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів. Зазначений захід є комплексним, і відповідає інтересам розвитку цифрового бізнесу. Цифрові послуги передбачають торгівлю інформацією як товаром, а отже їх захист неможливий без запровадження управління інформаційною безпекою на основі стандартів інформаційної безпеки, яких існує значна кількість. Найбільш прийнятними серед них є ISO/IEC 2700 (міжнародний стандарт визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS), Cybersecurity Framework NIST (забезпечує гнучкий підхід до управління ризиками, пов'язаними з кібербезпекою), PCI DSS (стандарт безпеки даних індустрії платіжних карток розроблений для забезпечення того, щоб компанії, які обробляють, зберігають або передають інформацію про кредитні картки, підтримували безпечне середовище). Зазначені стандарти не є вичерпними. На їх основі формується архітектура управління інформаційною безпекою, яку організації та органи державної влади можуть створювати, і використовувати для власного захисту.

4) створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг. Головним органом є Кабінет міністрів України, який визначає організаційно-правовий порядок здійснення відповідної діяльності. Постановою Кабінету Міністрів України

від 13 вересня 2024 р. № 1062 затверджено Порядок проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг [3]. Зазначеним документом визначено механізм оцінки відповідності суб'єктів, які мають намір надавати послуги електронної ідентифікації, надавачів послуг електронної ідентифікації, юридичних осіб, фізичних осіб – підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованих надавачів електронних довірчих послуг, центрального засвідчувального органу, засвідчувального центру та послуг, які вони надають, вимогам до надавачів послуг електронної ідентифікації, кваліфікованих надавачів електронних довірчих послуг, а також вимогам до послуг, які вони надають;

5) створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг. Автентифікація – це процес перевірки справжності користувача за спроби доступу до системи чи сервісу, підтвердження того, що особа дійсно є тією, за кого себе видає. Без автентифікації безпеку цифрових послуг забезпечити неможливо. На сьогодні триває процес прийняття уніфікованих методів автентифікації для всіх міністерств і відомств;

6) підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог безпеки цифрових послуг.

Упродовж останніх кількох років, Україна продовжує проводити значний плат роботи щодо практичної реалізації зазначених заходів задля захисту цифрових послуг, забезпечення кібербезпеки і протидії кіберзлочинності.

Література:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. Офіційний вісник України. 2021. № 70. Ст. 4417

2. Михайло Федоров. Дії 3 роки. Як Україна отримала місце у світовій історії цифровізації? 14 лютого 2023. Економічна правда. URL: <https://epravda.com.ua/columns/2023/02/14/697034/> (дата звернення: 28.04.2025)

3. Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг: Постанова Кабінету Міністрів від 13.09.2024 р. № 1062. Урядовий

ЗАВДАННЯ ВІДОМЧОЇ НОРМОТВОРЧОСТІ В СИСТЕМІ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

Петрук Я. А.

*аспірант за спеціальністю 081 – Право
Донецький державний університет внутрішніх справ*

*Науковий керівник: **Стецюк Б. Р.***

*доктор юридичних наук, професор,
професор кафедри державно-правових дисциплін
та публічного управління факультету № 4
Донецький державний університет внутрішніх справ
м. Кропивницький, Україна*

Одним із важливих інструментів реалізації повноважень Міністерства внутрішніх справ України є відомча нормотворчість, яка виражається в діяльності, спрямованій на створення відомчих нормативно-правових актів, які регулюють організацію і порядок функціонування відомчих органів внутрішніх справ, та визначає правила поведінки для їх працівників.

У сучасних умовах, коли державне управління активно реформується, зростає роль якісного, своєчасного нормотворення в межах відомства. Саме тому аналіз завдань відомчої нормотворчості МВС України є актуальним для розуміння механізмів правового забезпечення діяльності цього органу, його взаємодії з іншими структурами та захисту публічного інтересу.

Відомча нормотворчість має не лише юридичне, а й суспільне значення, оскільки формує правові підстави для реалізації управлінських рішень у чітко визначених межах компетенції. Завдання такої нормотворчості полягають у забезпеченні правової визначеності, узгодженості із загальнодержавною нормативною базою та своєчасного реагування на зміни у сфері охорони правопорядку.

У зв'язку з цим дослідження завдань відомчої нормотворчості МВС України є актуальним для підвищення ефективності правового забез-