Віта Нор,
здобувачка третього рівня вищої освіти ступеня доктора філософії
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
e-mail: v.nor@khai.edu,
ORCID: 0009-0001-6461-1500

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Електронне урядування є одним з інструментів розвитку інформаційного суспільства, впровадження якого сприятиме створенню умов для відкритого і прозорого державного управління. Електронне урядування - форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян.

Головною складовою електронного урядування є електронний уряд – єдина інфраструктура міжвідомчої автоматизованої інформаційної взаємодії органів державної влади та органів місцевого самоврядування між собою, з громадянами і суб'єктами господарювання [1].

Виходячи з важливості електронного урядування необхідно забезпечити захист від несанкціонованого впливу. Саме для забезпечення цієї мети спрямовані нормативно правові акти: з яких саме актів

Розглянемо основні поняття та терміни які використовуються в правовому забезпечення інфо-ресурсів електронного урядування, а саме Закон України Про основні засади забезпечення кібербезпеки України та Постанова Кабінету міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури

Так відповідно до ст.1. Законну України «Про основні засади забезпечення кібербезпеки України», кібератака це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

Відповідно то п.п. 5 ст. 1 вказаного вище Закону «Про основні засади забезпечення кібербезпеки України» кібербезпека є захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У п.п. 6 Закону України «» визначається так кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Об'єктами кіберзахисту є: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади та органів місцевого самоврядування. Відповідно до ст. 5. Закону України «Про основні засади забезпечення кібербезпеки України» для забезпечення кібербезпеки електронних ресурсів місцевого самоврядування покладаються повноваження на суб'єкти місцевих державних адміністрацій та органів місцевого самоврядування [3].

При цьому відповідно до п.1 ст. 8. вище вказаного нормативного акту покладається на Державну службу спеціального зв'язку та захисту інформації України яка забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

Враховуючи що на сучасному етапі розвитку соціальних відносин та адміністративно-управлінських послуг, доступ до електронних ресурсів та обмін інформацією між громадянами та органами місцевого самоврядування електронними засобами є життєво важливими, тому в разі порушення нормального їх функціонування передбачена відповідальність, зокрема кримінальним Законом. Це, зокрема, ст. 361 (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж); ст. 361-1 (створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут); ст. 110 (посягання на територіальну цілісність і недоторканність України); ст. 111 (державна зрада); ст. 113 (диверсія) [4].

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту відповідно до ст. 13 Закону «Про основні засади забезпечення кібербезпеки України» є кошти державного і місцевих бюджетів [2].

В результаті проведеного аналізу нормативно-правової бази із забезпечення кібербезпеки інформаційного ресурсу електронного урядування можно зробити висновок про те, що з точки зору публічного права є можливості більш широкого використання заходів які сприятимуть інформаційній безпеці діяльності органів публічного управління.

Список використаних джерел:

1. Про схвалення Концепції розвитку електронного урядування в Україні. Кабінет Міністрів України; Розпорядження, Концепція від 13.12.2010 № 2250 р [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/main/index)

2. Закон України Про основні засади забезпечення кібербезпеки України URL https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 04.04.2024)

3. Постанова Кабінету міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури URL https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8

4. Кримінальний кодекс України URL https://zakon.rada.gov.ua/go/2341-14& (Дата звернення 27.04.2024)