ПРАВОВІ ЗАСАДИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Пекарський Сергій Петрович,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки Донецького державного
університету внутрішніх справ

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначає Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [1]. Своєю чергою правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури, що є складовою законодавства у сфері національної безпеки визначає Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX [2].

У зв'язки з тим, що відповідно до вимог статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [3, ч. 2 ст. 19] зазначаємо аксіому про те, що кіберзахист об'єктів критичної інфраструктури в нашій державі має відповідне правове регулювання.

В контексті предмету дослідження зазначаємо, що до об'єктів критичної інфраструктури відносяться об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [2, п. 13, ст. 1]. Під охороною об'єктів критичної інфраструктури необхідно розуміти комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб'єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об'єктах критичної інфраструктури [2, п. 15, ст. 1].

Визначившись з поняттям охорони об'єктів критичної інфраструктури нам необхідно визначитися з сутністю кіберзахисту об'єктів критичної інформаційної інфраструктури. В Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII надано визначення загальному поняттю «кіберзахист» під яким розуміємо сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [1, п. 7, ст. 1].

Під об'єктом критичної інформаційної інфраструктури розуміємо комунікаційну або технологічну система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [1, п. 19, ст. 1]. А критична інформаційна інфраструктура – це сукупність об'єктів критичної інформаційної інфраструктури [1, п. 15, ст. 1]. У свою черга безпека об'єкта критичної інфраструктури – це стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг [4].

До об'єктів кіберзахисту безпосередньо відносяться:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1, ст. 4].

Постановою Кабінету Міністрів України від 9 жовтня 2020 року № 943 затверджено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» [4]. Згідно вимог зазначеного Порядку для оцінки критичності об'єкта інформаційної інфраструктури використовуються наступні критерії:

- необхідність об'єкта інформаційної інфраструктури як для стійкого та безперервного функціонування об'єкта критичної інфраструктури, так і для надання ним основних послуг;
- кібератака, кіберінцидент, інцидент з інформаційної безпеки на об'єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг;
- у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури відсутній альтернативний об'єкт (спосіб) для їх надання.

Отже, на підставі викладеного та проведеного відповідно до предмету дослідження аналізу правових засад зазначаємо організаційні та технічні заходи кіберзахисту на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Організаційні та технічні заходи повинні забезпечувати:

- формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;
- мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

- доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури [5].

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (редакція станом на 17.08.2022). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX (редакція станом на 05.12.2022). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
3. Конституція України від 28 червня 1996 року (редакція станом на 01.01.2020). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
4. Порядок формування переліку об’єктів критичної інформаційної інфраструктури: затв. постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 року № 943 (редакція станом на 07.09.2022). URL: https://zakon.rada.gov.ua/laws/show/943-2020-n#n16.
5. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури: затв. постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (редакція станом на 07.09.2022). URL: https://zakon.rada.gov.ua/laws/show/518-2019-n#n8.