

УДК 681.518.54

Зозуля О.Ф. студент гр. УБіт-14-1
Науковий керівник: Мешков В.І., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У МІСТІ ДНІПРО

Останніми десятиріччями у світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різного походження. Щодня світові ЗМІ повідомляють про природні й техногенні катастрофи, збройні конфлікти, терористичні акти, тяжкі злочини, вчинені і злочинними організаціями, і окремими особами, акти піратства на морі тощо. І дедалі частіше в результаті таких надзвичайних подій жертвами стає велика кількість людей, а життєво важливим для існування держав системам, об'єктам і ресурсам завдається серйозна шкода [1].

На засіданні верховної ради 5 жовтня 2017 року, було прийнято Закон про основні засади кібербезпеки України.

Цей Закон визначає 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 [2].

Згідно новому закону: критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [2].

Також розглянемо визначення поняття: об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [2].

З-поміж загроз критичній інфраструктурі називають пандемії, промислові аварії, терористичну та злочинну діяльність, кібератаки, стихійні лиха тощо. Держава має забезпечувати захист об'єктів критичної інфраструктури від усіх суттєвих загроз, які можна віднести до трьох категорій: техногенні, природного характеру та соціально-політичні [1].

Оскільки на даний момент по відношенню до України проявляється агресія (зона АТО), то можливе ведення диверсійної війни на території міста Дніпро. Мета диверсійної війни в проведенні спеціальних операцій по виведенню з ладу (пошкодження, руйнування, підпал, підриг та інше) критично важливих об'єктів. Наприклад гучного резонансу набула серія вибухів, вчинених у Дніпропетровську 27 квітня 2012 р. (постраждало 29 осіб). Прокурором Дніпропетровської області порушено кримінальну справу за частиною 2 ст. 258 КК (терористичний акт). Терористичні акти завжди мають значний резонанс. Однак при цьому не слід забувати про те, що техногенні аварії часто можуть мати наслідки тяжчі, ніж у випадку деяких терактів. Наприклад, вибух природного газу в 10-поверховому будинку у Дніпропетровську, що став- ся 13

жовтня 2007 р., забрав життя 23 людей (у т.ч. семи дітей). Кримінальну справу було порушено за ст. 367 КК (службова халатність), а на лаві підсудних опинилися три представника ВАТ «Дніпрогаз» – генеральний директор, його перший заступник і головний інженер.[1]

З наведених вище прикладів робимо висновок, що об'єкти критичної інфраструктури міста Дніпро повинні надавати більшого значення загрозам терористичних атак.

На підтвердження даної думки можна привести наступну інформацію:

Президент України Петро Порошенко прийняв в дію рішення Ради національної безпеки і оборони “Про вдосконалення заходів забезпечення захисту об'єктів критичної інфраструктури”. Про це йдеться в указі Президента №8 від 16 січня. Цим рішенням від 29 грудня 2016 року РНБО доручив Кабінету Міністрів впродовж 2 місяців розробити і прийняти концепцію створення державної системи захисту критичної інфраструктури і план заходів що до їх реалізації.

На території міста Дніпро знаходяться та функціонують наступні об'єкти критичної інфраструктури:

- ДТЕК Дніпрообленерго;
- Південний машинобудівний завод імені О.М. Макарова;
- ПАО “Дніпротяжмаш”;
- ПАО “Дніпровський агрегатний завод”,

та багато інших підприємств, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі.

Надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я.

Або є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню.

ВИСНОВОК

На території міста Дніпро діє велика кількість критично важливих об'єктів. Безпека яких є пріоритетною задачею державних служб та відомств. Прийняття Закону про основні засади кібербезпеки України – це великий крок до зміцнення безпеки об'єктів критичної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аналітична доповідь: «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні», автор Бірюков Д.С., Кондратов С.І. Закон України «Про основні засади забезпечення кібербезпеки України», документ 2163-19, прийняття від 05.10.2017.