ОСОБЛИВОСТІ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Тимошенко Д.О.
Науковий керівник – к. техн. н., доц. Пронюк Г. В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. охорони праці,
тел.: (057)702-13-60)
E-mail: magnatolia1@gmail.com

In this work we pay attention to the importance of developing and implementing tools to protect critical infrastructure facilities. In given work, we give several recommendations on the development of a policy, the basic principles of which are: adherence to the principle of voluntariness, encouraging the inclusion of security requirements at the design stage of the project, encouraging further investments in cyber security.

У кожному суспільстві можна виділити сектори, системи або мережі, від яких життєво залежить суспільство і порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівні. Тому в наш час забезпечення безпеки об'єктів критичної інфраструктури (ОКІ) є одним із першочергових завдань суспільства.

Європейський Союз, а саме European Programme for Critical Infrastructure Protection (2006) визначає **критичну інфраструктуру** як системи, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисного поведінки, може істотно негативно вплинути на безпеку ЄС і добробут громадян.

Мета роботи - звернути увагу на важливість розробки і впровадження способів захисту об'єктів критичної інфраструктури.

За статистикою провідного німецького оператора зв'язку Deutsche Telekom за останні 5 років по всьому світу стрімко зросла кількість кібератак на важливі об'єкти критичної інфраструктури, Україна не стала винятком. Тільки за 2018 рік, за даними Нацполіції, було скоєно шість тисяч злочинів у сфері кібербезпеки, тому питання про захист об'єктів КІ України є актуальним і має пріоритет. За даними авторитетного журналу «Новое время» з 2014 року об'єкти критичної інфраструктури піддавалися 12 найбільшим кібератакам. Однією з найсильніших стала вірусна програма Petya.A, яка порушила роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ.

У 2017 році спільно з США український уряд почав розробку Концепції щодо захисту об'єктів КІ, на жаль, нормативне регулювання не встигає за розвитком як новітніх загроз, так і технологій, необхідних для їх стри-

мування. Інтернету властивий швидкий постійний розвиток, що в поєднанні з його глобальним охопленням вимагають гнучких рішень, швидко адаптуються до нових і мінливих обставин.

Дуже важливо дозволити підприємствам добровільно впроваджувати інновації для захисту критично важливої інфраструктури, тому що тільки розпорядження та приписи не сприятимуть захисту. Слід заохочувати включення вимог безпеки ще на етапі розробки проекту, так як додавання функцій безпеки до систем, мереж або пристроїв вже після їх запуску і введення в експлуатацію має ряд вразливих місць і недоліків, з яких не останнім є необхідність відключати системи під час оновлення – важко здійснювана вимога, якщо мова йде про енергосистеми.

Стимулювання подальших інвестицій в засоби кіберзахисту ОКІ може включати наступні напрямки:

1. Податкові пільги - заохочення для компаній, що інвестують в кіберзахист, в тому числі прискорене нарахування зносу і податкові пільги за впровадження зарекомендованих технологій безпеки;
2. Реформи страхування - держава могла б стимулювати ринок страхування, розробивши комплекс заходів підтримки даного ринку;
3. Розсекречення більшої кількості даних про загрози - державним структурам необхідно підвищити якість і кількість даних про загрози. Це означає, що слід розсекретити більше категорій даних про загрози і активно ділитися такою інформацією. Державним структурам слід надавати допуск до самих конфіденційних і потенційно найбільш цінних масивів і категорій даних про загрози набагато більшій кількості уповноважених представників компаній.

Таким чином, знищення або виведення з ладу матеріальної та інформаційної інфраструктури ОКІ в результаті стихійних лих, кібератак чи інших причин завдає великої шкоди населенню і країні в цілому, тому завдання забезпечення захисту критичних інформаційних систем і мереж носить глобальний характер. Сучасна інформаційна інфраструктура цілком залежить від взаємозв'язку і сумісності інформаційних систем по всьому світу. В силу цього завдання забезпечення захисту критично важливої інформаційної інфраструктури в глобальному масштабі вимагає впровадження ефективних міжнародних стратегій і рішень.

Список використаних джерел

1. European Programme for Critical Infrastructure Protection [Електронний ресурс]. – 2006. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: від 23 серпня 2016 р. № 563. /Постанова Кабінету Міністрів України.