Голубош В.В.
кандидат юридичних наук, начальник ГУНП в Івано-Франківській області

Holubosh V.V.
PhD, Head of National Police Department in Ivano-Frankivsk region

ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ ТА ЇЇ ЗАХИСТ: ІНФОРМАЦІЙНИЙ ВИМІР

Нині безпека є найбільш важливою проблемою, особливо коли йдеться про об'єкти захисту критичної інфраструктури (далі – КІ). Загроза їх нормальному функціонуванню підриває життєдіяльність цілих регіонів, міст, держав. Наприклад, хакерські атаки є реальною небезпекою не лише власників персональних комп'ютерів, а насамперед великих промислових технологічних та інформаційних систем. Результати таких збоїв є катастрофічними, саме тому в Україні активно обговорюється законопроект про КІ та її захист.

Приємно, що вказаний законопроект розроблений. Сама назва викликає зацікавленість до обговорення не лише у фахівців, а й пересічних громадян. Водночас у багатьох залишаються сумніви щодо можливості реалізації його на практиці.

Процес розроблення та прийняття законопроекту про КІ та її захист повинен бути виваженим, щоб врахувати та охопити максимальну кількість обставин та ситуацій, завадити поспішним крокам, котрі можуть призвести до прогалин у майбутньому законодавчому акті.

Після прийняття законопроекту власники КІ, на наше переконання, зобов'язані провести низку технічних та інформаційних заходів, спрямованих на захист об'єктів КІ. Без сумніву, це потребує значних капіталовкладень. З іншого боку, якщо відбувається певний інцидент, то наслідки є плачевними. Прикладом цьому може слугувати велика кількість кібератак, котрі трапляються постійно.

Абсолютна більшість цивілізованих країн задається питанням захисту та безпеки власних об'єктів КІ, особливо коли мова йде про захист інформаційних систем (т.з. кібербезпеки тощо). Бо ж в умовах глобального світу безпека держави обмежується не лише її кордонами, вона стає спільною справою багатьох.

Потенційні збитки компаній і держструктур, котрих вони можуть понести у разі завдання шкоди чи руйнування об'єктів КІ, є непоправними, насамперед коли говорити про отруєння води, флори, фауни, всього живого.

Держава у будь-який час повинна бути готовою до належного захисту своїх об'єктів КІ у разі раптового нападу ворога, реальної загрози стихії чи у випадку воєнного стану. Задля цього має бути вибудувана міцна система захисту об'єктів КІ, котра постійно працюватиме на випередження з метою уникнення негативних обставин, усунути котрі часто є не можливим.

Щодо інформаційної складової, то до об'єктів КІ можна зарахувати інформаційні системи, інформаційно-телекомунікаційні мережі державних органів, а також автоматизовані системи управління технологічними процесами, що функціонують в оборонній промисловості, сфері охорони здоров'я, транспорту, зв'язку, кредитно-фінансовій сфері, енергетиці, паливній, атомній, ракетно-космічній, гірничодобувній, металургійній та хімічній промисловості [1].

Як результат, ми приходимо до таких висновків:

- загроза нормальному функціонуванню об'єктів КІ підриває життєдіяльність цілих регіонів, міст, держав, що загрожує безпеці всього суспільства. Безпека держави не є її внутрішньою проблемою, вона набуває транснаціонального масштабу; є реальною загрозою не лише для власників персональних комп'ютерів, а й великих промислових технологічних та інформаційних систем, компаній і держструктур. У випадку певного інциденту, наслідки часто є плачевними. Прикладом цьому є велика кількість кібератак, котрі трапляються постійно.

- законопроект про КІ та її захист потребує реального вдосконалення та обговорення не лише з боку фахівців, а й пересічних громадян на т. з. Інтернет-платформах. Держава повинна зробити усе можливе, щоб основні положення вказаного законопроекту були втілені в життя.

- процес розроблення та прийняття законопроекту має бути виваженим, щоб врахувати та охопити максимальну кількість ситуацій і обставин, завадити поспішним крокам, котрі можуть призвести до прогалин у вказаному законодавчому акті; після прийняття законопроекту власникам КІ доречно було б провести низку технічних та інформаційних заходів, спрямованих на захист об'єктів КІ, що потребує значних капіталовкладень.

- держава у разі несподіваного нападу ворога, реальної загрози стихії, у випадку воєнного стану чи за інших надзвичайних умов повинна бути готовою до негайного захисту об'єктів КІ; має бути вибудувана міцна система захисту об'єктів КІ, котра безперервно працюватиме на випередження, щоб уникнути негативних наслідків, котрі можуть завдати непоправної шкоди суспільству.

- до інформаційних об'єктів КІ можна зарахувати: інформаційні системи, інформаційно-телекомунікаційні мережі державних органів, автоматизовані системи управління технологічними процесами, що функціонують в усіх сферах людської життєдіяльності.

1. О безопасности критической информационной инфраструктуры Российской Федерации: от 26.07.2017 № 187-ФЗ (последняя редакция) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

Голубош В.В. Про критичну інфраструктуру та її захист: інформаційний вимір

Безпека є найбільш важливою проблемою, особливо коли йдеться про об'єкти захисту критичної інфраструктури. Загроза їх нормальному функціонуванню підриває життєдіяльність цілих регіонів, міст, держав. Наприклад, хакерські атаки є реальною небезпекою не лише власників персональних комп'ютерів, а насамперед великих промислових технологічних та інформаційних систем. Результати таких збоїв є катастрофічними, саме тому в Україні активно обговорюється даний законопроект.

Абсолютна більшість цивілізованих країн задається питанням захисту та безпеки власних об'єктів, особливо коли мова йде про захист інформаційних систем (т.з. кібербезпеки тощо). Бо ж в умовах глобального світу безпека держави обмежується не лише її кордонами, вона стає спільною справою багатьох.

Потенційні збитки компаній і держструктур, котрих вони можуть понести у разі завдання шкоди чи руйнування об'єктів КІ, є непоправними, насамперед коли говорити про отруєння води, флори, фауни, всього живого.

Ключові слова: інформаційне суспільство, критична інфраструктура.

Holubosh V.V. On critical infrastructure and its protection: information dimension

Security is the most important issue, especially when it comes to critical infrastructure. The threat to their normal functioning undermines the vital functions of entire regions, cities and states. For example, hacker attacks are a real danger not only to such objects owners, but especially to large industrial technology and information systems. The results of such failures are catastrophic, which is why this bill is being actively discussed in Ukraine.

The vast majority of civilized countries are concerned with the protection and security of their CI facilities, especially when it comes to protecting information systems (so-called cybersecurity, etc.). Because in the global world, the security of the state is limited not only by its borders, it becomes a common cause of many.

The potential losses of companies and government agencies, which they may suffer in the event of damage or destruction of critical infrastructure facilities, are irreparable, especially when it comes to poisoning of water, flora, fauna, all living things.

Key words: information society, critical infrastructure.