УДК 304

І. Ю. Глєбов
С. Г. Денисюк

КІБЕРПРОСТІР В УКРАЇНІ: ПРАВОВИЙ АСПЕКТ

Вінницький національний технічний університет

Анотація
У статті проаналізовано заходи України щодо забезпечення безпечного кіберпростору та кібербезпеки нації в цілому.
Ключові слова: *кіберпростір, кібербезпека, законопроект, об'єкти та суб'єкти.*

Abstract
The article analyzes Ukraine's measures to ensure safe cyberspace and cybersecurity of the nation as a whole.
Keywords: *cyberspace, cybersecurity, legislative bill, objects and subjects.*

Вступ

Сучасна тенденція розвитку IT-сектору та інформаційного простору безперечно є прогресивним показником суспільства 21-ого століття. Але, разом з багатьма можливостями, які з'явилися як наслідок прогресу у сфері інформаційних технологій, з'явилося чимало проблем різного характеру, основними з яких є законодавчі, а саме, врегулювання кіберпростору. Створення нормативних інструментів для регулювання та забезпечення кібербезпеки на національному рівні є необхідним для сучасної України.

Метою роботи є висвітлення основних положень щодо контролю кіберпростору та стан кібербезпеки в Україні та подальші плани на розвиток цієї галузі в Україні.

Основна частина

Початок серйозних обговорень регулювання кіберпростору почався 26 травня 2017 року – повторно розглядався законопроект № 2126а «Про основні засади забезпечення кібербезпеки України» [1]. На той час не було цілісного уявлення про те, як саме держава повинна регулювати надзвичайно небезпечні кіберзагрози. Вже 27 червня 2017 року Україна та ще декілька країн були атаковані вірусом «Ransom:Win32/Petya» [2]. Цей вірус відноситься до класу шифрувальника. Він блокує комп'ютери та потребує викуп у біткоїнах за дешифровку файлів. Постраждало більш ніж 80 приватних та державних компаній, зокрема банки, аеропорти, державна залізнична компанія, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування тощо. Цей прецедент дав змогу зрозуміти беззахисність України під дією таких атак, тому необхідно було створити інструменти своєчасного виявлення, запобігання та нейтралізації реальних та потенційних загроз у кіберпросторі у майбутньому.

У сучасному законопроекті «Про основні засади забезпечення кібербезпеки України» чітко визначаються права та обов'язки державних органів щодо кібербезпеки, визначаються основні поняття в галузі кіберзахисту. Проблемою залишається нечітка термінологія, яку необхідно комплексно доповнювати на регулярному базисі у зв'язку з постійним розвитком інформаційної галузі. Опис термінів також є проблематичним, адже доволі важко зрозуміло формулювати складні терміни неоригінальною мовою, що стає ще проблематичніше, якщо терміни описуються іншими поняттями.

Розглянемо головних акторів, які згадуються в законопроекті. Відповідно до статті 5 законопроекту, суб'єктами кібербезпеки є: Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України; Кабінет Міністрів України та міністерства; центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних

правочинів, електронними комунікаціями, захистом інформації та кіберзахистом, авторизованими електронними майданчиками [3].

Головними суб'єктами національної системи кібербезпеки виступають Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Суб'єкти у межах своєї компетенції мають спряти запобіганню використання кіберпростору в цілях воєнних, терористичних та загалом злочинних дій, виявляти подібні дії та усувати їх наслідки, розповсюджувати інформацію щодо реалізованих та потенційних загроз тощо.

Об'єктами тут є захисники суб'єктів. Для цього будуть залучені об'єкти, до яких відносяться комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси або використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів і військових формувань; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб або у сферах е-урядування, електронних державних послуг, електронної комерції, е-документообігу. До таких об'єктів можуть бути віднесені підприємства та установи, державні або приватні, які надають послуги будь-якого характеру.

Іншими словами, якщо підприємство визначать як критичну інфраструктуру, треба створити необхідні умови та впровадити систему захисту інформації, запросити компанію-аудитора, яка перевірить усі стандарти дотримання законопроекту та отримати сертифікат відповідності.

Висновок

У законопроекті № 2126а «Про основні засади забезпечення кібербезпеки України» висвітлені основні поняття, опис термінів та умови дотримання безпечної умови праці у кіберпросторі. Але, на жаль, це лише початок формування повноцінних галузевих стандартів щодо кібербезпеки в Україні. У сучасному вигляді законопроект має багато недоліків, які повинні обговорюватися. Для здійснення оптимального контролю за впровадженням заходів кібербезпеки на підприємствах та організаціях та загальним контролем над суб'єктами з питань інформаційного захисту необхідно створити єдиний орган для виконання цієї ролі. Тільки такий організований підхід дозволить реагувати та запобігати таким інцидентам, як атака вірусу Petya. Також у теперішньому формулюванні, Служба безпеки України матиме право проводити таємні перевірки всієї критичної інфраструктури. Так як під це поняття підпадає і приватний сектор, така можливість дає змогу службі атакувати та маніпулювати приватним бізнесом, що є неприпустимо. Україні необхідно звернутися до інших країн за прикладом у регулюванні кіберпростору, зокрема до США та держав ЄС, у яких вже є позитивний досвід регулювання кіберзлочинності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Законопроект № 2126а «Про основні засади забезпечення кібербезпеки України на 2017 рік». URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#Text
2. Опис вірусу Petya та його наслідки. URL: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Petya.E&threatId=-2147240672
3. Законопроект № 2126а «Про основні засади забезпечення кібербезпеки України на жовтень 2020 рік». URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20201024#Text

Глєбов Іван Юрійович – студент групи 1ІСТ-17б, факультету комп'ютерних систем та автоматики, Вінницький національний технічний університет, м. Вінниця, e-mail: morpice0009@gmail.com

Денисюк Світлана Георгіївна – доктор політичних наук, професор, професор кафедри суспільно-політичних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: svetadenisiyk@gmail.com

Hliebov Ivan Yuriyovich – student of 1IST-17b, Faculty of Computer Systems and Automation, Vinnytsia Na-tional Technical University, Vinnytsia, e-mail: morpice0009@gmail.com

Svitlana G. Denysiuk – Doctor of Politician science (Eng.), professor, professor of social and political sciences de-partment, Vinnytsia National Technical University, Vinnytsia, e-mail: svetadenisiyk@gmail.com