УДК 351.865

Гайтота Є.В., Чуницька В.В., Нікуліщев Г.І.
Запорізький національний технічний університет

Про перспективи Стратегії кібербезпеки України

У зв'язку з розвитком інформаційних технологій сьогодні питання про забезпечення безпеки інформаційно-телекомунікаційних систем та захист інформаційних ресурсів в Україні стоїть дуже гостро. У відповідь на політичну ситуацію, що склалась у кінці 2014 р. – на початку 2015 р. Президент України Петро Порошенко підписав указ «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Цим указом вводиться в дію розроблена спеціалістами з кібербезпеки та затверджена на засіданні РНБОУ Стратегія кібербезпеки України. Цей документ базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, затверджений і набрав чинності 15 березня 2016 року.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Стратегія передбачає комплекс заходів, пріоритетів і напрямів забезпечення кібербезпеки України, зокрема:

- вироблення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягненні сумісності з відповідними стандартами ЄС та НАТО;
- створення вітчизняної нормативно-правової та термінологічної бази у цій сфері;
- формування конкурентного середовища у сфері електронних комунікацій;
- розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;
- підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі;
- проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;
- розвиток міжнародного співробітництва, підтримку міжнародних ініціатив у сфері кібербезпеки, поглиблення співпраці України з ЄС та НАТО.

Стратегія остаточно законодавчо визначає концепцію критичних об'єктів інфраструктури, таких як енергетичні і транспортні магістральні мережі, лінії нафто- і газопроводів, морські порти і т. д.

Основна ідея вищевказаних заходів і пріоритетів у Стратегії полягає в тому, що Україна повинна створити складну глобальну високотехнологічну систему для забезпечення безпеки і надійності зв'язку. Це здається непростим завданням, беручи до уваги поточний стан інструментів захисту і безпеки.

Стратегія передбачає створення «активного кіберзахисту», що означає здійснення воєнно-політичних, військово-технічних та інших заходів, спрямованих на розширення прав і можливостей воєнної організації держави, сектора безпеки і оборони в кіберпросторі, створення, розвиток сил, засобів та інструментів для можливої відповіді на агресію у віртуальному просторі, що може бути використаний як засіб стримування воєнних конфліктів і загроз в кіберпросторі. Іншими словами, Україна повинна створити механізм кібератак у відповідь. Але такий механізм вимагає серйозних інвестицій і знань.

Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, якої мають

дотримуватись державні органи. Одним з перших кроків з втілення Стратегії, стало створення в червні 2016 року Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України.

В цілому, структура Стратегії більше схожа на концепцію або декларацію, ніж на законодавчий акт. Її реалізація потребує внесення низки змін до українського законодавства, що мають як створити підґрунтя для втілення в життя положень Стратегії, так і посилити відповідальність за порушення в сфері кібербезпеки.

Таким чином, очевидно, що нова Стратегія є необхідною, однак не достатньою для того, щоб належним чином захистити Україну від кіберзлочинності.

В роботі авторами проведено детальний аналіз положень Стратегії кібербезпеки України. За результатами аналізу пропонуються способи вирішення проблем, які можуть виникнути в перспективі практичної реалізації цілей і задач Стратегії.

Для оперативного реагування на порушення кібербезпеки спецслужбам необхідні інструменти онлайн доступу до комп'ютерних даних абонентів, однак при цьому потрібно зберегти баланс між правом громадян на недоторканність приватного життя та інтересами національної безпеки, бо для доступу до персональних даних необхідне судове рішення. Однак у ситуації кіберзлочину – необхідна миттєва реакція розвідувальних служб, і отримання рішення суду може затримати таку реакцію.

Для вирішення цієї проблеми авторами пропонується виокремити в структурі судової системи спеціальний орган правосуддя, який розглядатиме справи лише у сфері кіберзлочинності. Це пришвидшить процес надання спецслужбам доступу до комп'ютерних даних користувачів, при цьому не порушуючи право громадян на недоторканність приватного життя.

На часі державні органи з кіберпезпеки не можуть захистити всіх суб'єктів кіберпростору. З цього випливає, що організації та комерційні підприємства мають також докладати зусиль для забезпечення власної кібербезпеки. Також важлива кібербезпека не лише на рівні держави чи організації, а й на рівні окремої особи, як найбільш слабкої ланки системи кібербезпеки.

Для попередження незначних злочинів у кіберпросторі необхідно підвищити рівень кіберграмотності громадян та культури безпечного поводження у кіберпросторі. Цьому можуть посприяти, наприклад, тренінги, на яких розповідатимуть про базові правила поводження у кіберпросторі. Слід зауважити, що ініціатива повинна виходити не тільки від влади, але й від громадських організацій, приватного бізнесу та звичайних громадян. Відповідно, і в проведенні таких заходів повинні брати участь всі вищевказані сторони. Не менш ефективним має бути розміщення статей про захист персональних даних у вигляді реклами в Інтернеті, банерах та засобах мас медіа. Це надасть змогу зменшити кількість випадків витоку приватної інформації.

Основне призначення Стратегії – це створення умов для безпечної експлуатації кібепростору. У ході аналізу Стратегії було виявлено, що вона, безсумнівно є необхідною основою для позитивних змін у сфері кіберзахисту. Тим не менш, цей документ лише визначає напрями дії. Подальший розвиток Стратегії потребує внесення значних змін у чинне законодавство, створення спеціалізованих керівних і виконавчих органів у сфері кібербезпеки, підготовку і перепрофілювання спеціалістів з кібербезпеки тощо. Цей комплекс заходів має гарантувати посилення захисту національних рубежів України у кіберпросторі.

Список використаних джерел

1. *Офіційний портал Верховної Ради України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Верховна Рада України 15.03.2016. – Режим доступу:* http://zakon3.rada.gov.ua/laws/show/96/2016.