ОСНОВНІ БЕЗПЕКОВІ ПРОБЛЕМИ КІБЕРПРОСТОРУ УКРАЇНИ

Валерія Войтович, Ростислав Гриник

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

In this work, the main task is to consider the basic problems of providing Ukraine in cyberspace and propose solutions to improve the security of cyberspace and in our country.

Keywords: Cyberspace, information security, cybersecurity.

На сьогоднішній день в умовах створення глобального інформаційного суспільства, інформаційна безпека країни, не виключенням є і Україна, починає відігравати одну з основних ролей у забезпеченні державної безпеки загалом. Насамперед це відображається у тому, що Україна є європейською державою і не може обминати всі проблеми й небезпеки, створені інформаційним суспільством. І це не дивно, адже інформація є безпосередньо головним елементом кіберпростору, а саме того віртуального простору, де кожен з нас, що найменше, є учасником, щодня.

У даній роботі розглядаються основні проблеми захисту кіберпростору. Поява кіберпростору призвела до значимих змін у суспільстві, функціонуванні держави, принципах роботи економіки, а також в соціальних взаємозв'язках. Більшість науковців, як вітчизняних так і закордонних, вважають, що кіберпростір – це середовище, що взаємодіє з комп'ютерною технікою, зокрема, мережею та системами, у рамках яких створюються, відбуваються, змінюються та припиняються правові відносини. Однією з основних джерел загроз інформаційній безпеці України можна вважати соціальні мережі, які можуть використовуватись окремими країнами, організаціями чи особами для пропаганди власних ідей та внесенні деструктивних чинників у соціум. Важливо виділити, що на сьогоднішній час існує велика кількість ускладнень, що перешкоджає формуванню належного захисту кіберпростору, до них можна віднести:

- Відсутність державного і приватного сектору стандартів кібернетичної безпеки на основі визнаних міжнародних стандартів;
- Відсутні системні міжнародні нормативно-правові документи, які точно давали б визначення кіберпростору та всім елементам та чинникам котрі впливають на безпеку кіберсередовища;
- Розвиток новітніх інформаційних технологій на низькому рівні, особливо зазначимо, що розвиток виробництва конкурентоспроможного національно-інформаційного продукту, а саме сьогоднішніх засобів й систем захисту інформаційних ресурсів;
- Рівень фінансового забезпечення державних структур наразі обмежений, адже саме ці системи функціонують в управлінні державою, забезпечують потреби захисту і безпеки держави.

Розглянувши вище перечисленні проблеми, я пропоную наступні етапи вирішення завдання, щодо забезпечення безпечного кіберпростору України.

В першу чергу, варто розпочати з суттєвого доопрацювання понятійного апарату сфери забезпечення кіберпростору, адже на сьогодні не існує жодних офіційних трактувань даної термінології, що змушує кожну країну самостійно виробляти підходи у цій сфері. Безумовно, потрібно, щоб для законодавства поняття "кіберпростір", "кібератака", "кібербезпека", а також низка інших пов'язаних з ними термінів стали на рівень вивченості і розуміння про що йдеться.

Наступним це є реформування нормативно-правових документів, що мають за основу визначення сучасних загроз кібернетичній безпеці України, а також механізмів реагування на них. Створення рамкового акту, що містить основні юридичні визначення і принципи використання норм права. Це дозволить вирішити саме політичну частину проблеми.

Для України важливим є те, що застосування інформаційних технологій дає можливість підвищити якість підготовки і прийняття важливих рішень влади. Основним завданням розвитку інформаційних технологій в Україні є сприяння кожній людині широкого використання сучасних інформаційно-комунікативних технологій (ІКТ), можливість створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, реалізовуючи свій потенціал, повною мірою підвищувати якість свого життя. Розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів, являється одним з найвагоміших напрямів державної політики. Передбачається розвиток інформаційних технологій, насамперед у тих ділянках, де минулорічні розробки відповідають світовому рівню. Це стосується, зокрема, нейромережних технологій, створення засобів інтелектуалізації широкого призначення.

Наразі в Україні на низькому рівні є фінансове забезпечення державних систем, що взаємодіють працюють у кіберпросторі з різними типами інформації і не тільки. Для підвищення потрібно сприяти розробці інноваційної продукції, що може бути використана для посилення кібернетичної безпеки держави. Також, оптимізація системи підготовки кадрів у сфері кіберпростору для потреб органів системи безпеки та оборони України. Важливим є активна робота державних безпекових інституцій щодо інформування населення про різні загрози кібернетичного характеру. Постійно має бути присутнім підвищення кваліфікації військовослужбовців, державних службовців та працівників, які працюють у даній структурі. Додатком до цього повинна існувати підтримка багатосторонніх навчань з протидії кібератакам на державні ресурси та інформаційний світ нашої держави, а також ініціювання нових навчань у цій інфраструктурі.

Висновок. На сьогодні існує ряд основних проблем, через які унеможливлюється створення ефективної системи протистояння загрозам у кіберпросторі. Такими проблемами є: понятійна невизначеність, відсутність правого забезпечення, залежність України від іноземних інноваційних продуктів, складнощі у політичній структурі, економічні негаразди в країні. Створення національної системи кібербезпеки вимагає введення нової системи організації та навчання для інформаційної боротьби, що матимуть деякі органи, у секторах безпеки і оборони України. Необхідно запроваджувати в Україні найліпші здобутки закордонних країн, які є на першому місці з питань кібепростору.

Література

1. 1. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management. 2. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
2. 2. ISO/IEC TR 18044:2004. Information technology - Security techniques - Information security incident management.
3. 3. ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice.
4. 4. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. - Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р.
5. 5. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах" №2594-IV від 31.05.2006.
6. 6. Указ Президента України “ДОКТРИНА інформаційної безпеки України" № 514/2014 від 6.06.2014.
7. 7. Сташевський З.П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / З.П. Сташевський, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2012. – Вип. 22.10. – С. 79-96.