УДК 004.056

Коваль В.О.
Кіровоградський національний технічний університет

Огляд нормативно-правових засад кібербезпеки в Україні

Проблеми інформаційної безпеки України в сучасних умовах є надзвичайно актуальними і вимагають поглибленого вивчення. Дослідження інформаційної безпеки буде мати успіх лише за умови наявності понятійного апарату. І тому необхідно зробити огляд нормативно-правових засад для забезпечення кібербезпеки в Україні.

Останнім часом проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів. Для протистояння кібершахраям в світі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюються, а технічні можливості посилюються. Наприклад – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013 року [1].

У світі боротьба з кіберзлочинністю, однозначно, посилюється. Так, зокрема, Європа і США ідентифікували цю проблему як одну з найбільш небезпечних і ухвалюють велику кількість нормативних документів для захисту інформації від кіберзлочинності [1].

Українське ж законодавство у сфері захисту інформації, на думку експертів у цій області, вимагає дуже серйозного доопрацювання. Потенційно існує ймовірність того, що кіберзлочинність може перебиратись з Європи в Україну [1].

Аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності.

На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави.

Діяльність із забезпечення кібербезпеки ґрунтується на таких основних принципах [2, 3]:

верховенства права, законності та неухильного додержання прав і свобод людини і громадянина;

пріоритетності для держави захисту особистої інформації людини і громадянина;

комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів;

пріоритетності запобіжних заходів;

невідворотності відповідальності за вчинення кіберзлочинів та інших правопорушень, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів, забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої кіберзлочинами або відповідними правопорушеннями;

взаємодії держави та приватного сектору у виробленні нових рішень у сфері кібербезпеки та участі інституцій громадянського суспільства у забезпеченні кібербезпеки держави;

відповідальності суб'єктів забезпечення кібербезпеки за належне функціонування об'єктів кіберзахисту;

дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в кіберпросторі;

співпраці на міжнародному рівні з метою вироблення єдиних підходів та ефективної взаємодопомоги з питань протидії кіберзагрозам.

В Україні в системі забезпечення кібербезпеки держави задіяно низку військових та правоохоронних органів: Міністерство оборони України (та його спеціальні підрозділи – зокрема Головне управління розвідки), Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, Міністерство внутрішніх справ України, Службу зовнішньої розвідки.

Президент Петро Порошенко підписав Наказ «Про Національний координаційний центр кібербезпеки» - який є робочим органом Ради національної безпеки і оборони України.

Серед основних завдань Центру [4]:

1) здійснення аналізу:

стану кібербезпеки;

результатів проведення огляду національної системи кібербезпеки;

стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю;

стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;

стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;

даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення;

2) участь у розробленні галузевих індикаторів стану кібербезпеки;

3) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України;

4) розроблення концептуальних засад та пропозицій щодо забезпечення кібербезпеки держави, спрямованих на підвищення ефективності заходів щодо виявлення і усунення чинників, які формують потенційні та реальні загрози у сфері кібербезпеки, підготовка проектів відповідних програм та планів щодо їх попередження та нейтралізації;

5) узагальнення міжнародного досвіду у сфері забезпечення кібербезпеки;

6) участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків;

7) оперативне, інформаційно-аналітичне забезпечення Ради національної безпеки і оборони України з питань кібербезпеки;

8) розроблення і внесення Раді національної безпеки і оборони України, її Голові в установленому порядку пропозицій щодо кібербезпеки;

9) здійснення моніторингу стану розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО;

10) опрацювання питань щодо визначення шляхів, механізмів та способів вирішення проблемних питань, що виникають під час реалізації державної політики у сфері забезпечення кібербезпеки;

11) участь у забезпеченні здійснення контролю за станом виконання рішень Ради національної безпеки і оборони України з питань кібербезпеки держави, введених у дію указами Президента України;

12) вивчення міжнародного досвіду створення і функціонування національних систем кібербезпеки, поширення його між організаціями, установами і закладами відповідно до компетенції, проведення моніторингу щодо його впровадження в Україні;

13) участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки, розроблення відповідних методичних документів і рекомендацій.

Згідно з Положенням [4], Центр має право в установленому порядку запитувати та отримувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами.

Діяльність Центру дозволить забезпечити координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління в формування та реалізації державної політики в сфері кібербезпеки [5].

На мою думку, актуальною залишається проблема імплементації необхідної термінології до законодавства України, що на сьогоднішній день ускладнено особливостями юридичного характеру. Вбачається доцільним закласти ключові терміни кібербезпекової сфери (а заразом і сфери інформаційної безпеки в цілому) у нову редакцію Закону України „Про інформацію”. Щодо діючих нормативно-правових документів, які визначають функціонування сектору безпеки (зокрема – його завдання), то в них доречним було б внести певні зміни, що відображали б посилення актуальності кібербезпекової проблематики [6].

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

Список використаних джерел

1. *Кіберзлочинність в Україні 03/21/2013 Scientific Social Community URL: https://www.science-community.org/ru/node/16132*
2. *«Ліга:Закон» : головний правовий портал України. - URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N268A.html.*
3. *Офіційний веб-портал Верховна Рада України. - URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.*
4. *Указ Президента України «Про Національний координаційний центр кібербезпеки». - URL: http://zakon2.rada.gov.ua/laws/show/242/2016.*
5. *Официальное интернет-представительство Президент Украины Петр Дорошенко. - URL: http://www.president.gov.ua/ru/news/prezident-zatverdiv-polozhennya-pro-nacionalnij-koordinacijn-37329*
6. *"Сучасні тренди кібербезпекової політики: висновки для України". Аналітична записка. - URL: http://www.niss.gov.ua/articles/294/*