Інформаційна безпека держави

УДК 354.42

О.М. Косогов

Військова частина А1906, Київ

ПРІОРИТЕТНІ НАПРЯМКИ ДЕРЖАВНОЇ ПОЛІТИКИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ НАЦІОНАЛЬНОГО КІБЕРПРОСТОРУ

На основі аналізу нормативно-правового забезпечення інформаційної безпеки України визначено проблеми забезпечення безпеки національного кіберпростору. Пропонуються шляхи вирішення проблем щодо державної політики України у зазначеній сфері.

Ключові слова: *інформаційна безпека держави, кіберпростір, кібербезпека, кіберзагрози.*

Вступ

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційно-комунікаційними технологіями, або в більш широкому розумінні – кіберпростором. Водночас, зростання залежності від інформаційних технологій (ІТ) робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору. Кожного року зростає кількість кібернападів на всі елементи життєдіяльності нашої держави. В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити (а подекуди – унеможливити повністю) наслідки від кібератак.

Джерелами загроз та викликів національній безпеці України в інформаційній сфері можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а в перспективі, не виключено, і воєнного характеру.

У зв'язку з недостатнім розвитком інформатизації в нашій країні проблеми, що безпосередньо пов'язані із проникненням в інформаційні системи, почали досліджуватися лише останніми роками. З огляду на зарубіжний досвід вивченням кіберпростору як середовища вчинення злочинів займалися М.А. Погорецький та В.П. Шеломенцев, О.О. Климчук приділяв увагу вивченню змісту поняття "кібервійна", питання захисту ін. формаційної інфраструктури від кіберзагроз досліджував О.Д. Довгань [1 – 3].

Метою статті є аналіз нормативно-правового забезпечення інформаційної безпеки України визначено проблеми забезпечення безпеки національного кіберпростору та визначення шляхів вирішення проблем щодо державної політики України у зазначеній сфері.

Основний матеріал

На законодавчому рівні інформаційна безпека держави регулюється низкою законів України, постанов Кабінету Міністрів України, указів Президента України (в тому числі – введеними в дію рішеннями Ради національної безпеки і оборони України) та відомчими документами, що регулюють стандарти забезпечення інформаційної безпеки автоматизованих систем та програмних комплексів, порядок ліцензування тощо.

Разом з тим, незважаючи на те, що сфера забезпечення інформаційної безпеки держави регулюється понад 20 законами України, переважна більшість їх положень на тлі стрімкого розвитку новітніх технологій морально застаріває, а іноді вони взагалі суперечать один одному [4].

За оцінками вітчизняних експертів з проблем інформаційної безпеки, що сформовані на основі аналізу іноземного впливу на інформаційний медіа – і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції [5]:

цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;

активізація критики вищого державного керівництва України;

здійснення рядом зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах;

посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Крім того, новим джерелом загроз інформаційній безпеці України слід вважати соціальні мережі, які можуть використовуватись окремими країнами для просування власної ідеології у світі та впливу на ситуацію в нашій країні.

Високий рівень загроз у кібернетичному просторі підтверджується дослідженнями відомого німецького оператора зв'язку Deutsche Telecom, за даними якого Україна опинилася на четвертій позиції у світі серед країн-джерел кібернетичних атак. Тільки протягом лютого 2013 р. з території України їх було здійснено 566 тисяч [6].

Підрозділом реагування на комп'ютерні надзвичайні події України CERT-UA, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України, протягом 2012 року зафіксовано та вжито заходи з реагування на 31 комп'ютерний інцидент, які стосувалися захищеності інформаційних ресурсів державних органів [6].

Найбільш розповсюдженими різновидами атак були: несанкціонований доступ до автоматизованих систем (17 випадків) та DDoS атаки (6 випадків) на державні інформаційні ресурси. До того ж 150 вебсайтів українського сегменту мережі Інтернет з метою протидії несанкціонованому втручанню спецслужбами України було вжито заходів з блокування/видалення фішингового контенту [6].

При цьому маємо враховувати, що за перше півріччя 2013 р. кількість таких інцидентів вже становить 33, що однозначно свідчить про зростання відповідних загроз.

Тривожною є і порівняльна статистика. Якщо за весь 2012 рік було зафіксовано лише 5 випадків експлуатації технічних уразливостей систем, то лише за першу половину 2013 року кількість таких випадків становить 13. Інший небезпечний показник: якщо протягом всього 2012 року був зафіксований лише 1 випадок цільового ураження державних інформаційних ресурсів, то лише за першу половину 2013 року таких випадків зафіксовано 6. Все це свідчить не просто про кількісне зростання спроб стороннього впливу на державні інформаційні ресурси, а про збільшення кількості цілком свідомих атак на певні системи [6].

Протягом останніх років керівництвом держави було здійснено декілька важливих кроків, спрямованих на посилення боротьби із кіберзагрозами, та здійснено ряд заходів спрямованих на розбудову повноцінної національної системи кібербезпеки. Важливим етапом на шляху реалізації цих завдань було прийняття оновленої "Стратегії національної безпеки України" (Указ Президента України № 389/2012 від 8 червня 2012 року) [7], який звертає увагу на кібербезпекову проблематику. В документі вказується, що «на тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам".

Шляхами вирішення зазначеної проблеми можуть бути:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;
- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, систем управління об'єктами критичної інфраструктури;
- розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність;
- створення національної системи кібербезпеки.

Останньому було приділено увагу і у затвердженій Указом Президента України «Річній національній програмі співробітництва Україна - НАТО на 2013 рік» - «ужити заходів щодо становлення національної системи кібернетичної безпеки». Серед іншого цей План дій передбачав у 2013 році здійснення цілої низки заходів щодо посилення кібербезпекової компоненти нашої держави [4]:

- провести під егідою Спільної робочої групи Україна - НАТО з питань воєнної реформи консультації експертів Україна - НАТО в рамках робочої підгрупи з питань кібернетичного захисту;

- сприяти розвитку співробітництва з питань кібернетичного захисту між органами державної влади та відповідними компетентними органами Альянсу, а також на двосторонній основі з державами - членами НАТО (США, Сполучене Королівство Великої Британії та Північної Ірландії, Королівство Нідерланди та інші);
- опрацювати питання щодо можливості залучення України до спільних кібернетичних навчань держав - членів Альянсу («Eurocybex» та інші);
- опрацювати питання щодо можливості налагодження співробітництва України з Агентством НАТО з комунікацій та інформації (NCI);
- продовжувати взаємодію з відповідними органами іноземних держав і міжнародними організаціями в режимі реального часу через команду реагування на комп'ютерні надзвичайні події України CERT-UA (Центр реагування на комп'ютерні інциденти).

Крім того, державні органи, до компетенції яких відносяться питання протидії зовнішнім та внутрішнім кібернетичним загрозам в Україні, а також за участі інших зацікавлених державних органів та структур громадянського сектору здійснюють заходи з підготовки узгоджених цілісних пропозицій до національного законодавства, що мають унормувати сферу кібербезпеки та поліпшити реагування на сучасні кіберзагрози.

Серед таких ключових заходів – підготовка в 2013 році Кабінетом Міністрів України пропозицій змін до Закону України «Про основи національної безпеки України». Важливою їх особливістю є те, що ці пропозиції містять погоджений між всіма ключовими відомствами задіяними в сфері захисту національних інтересів в кіберсфері визначення понять «кіберпростір» та «кібербезпека».

Незважаючи на Указ Президента України № 449/2014 "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", нажаль, в Україні все ще відсутній документ, що має на загальнодержавному, стратегічному, рівні визначити основні поняття в сфері кібербезпеки, загрози, принципи та напрями забезпечення кібернетичної безпеки, і особливо – ключові заходи з вдосконалення державного управління та нормативно-правового поля у сфері кібербезпеки та кіберзахисту. Більшість з інформаційно розвинутих країн вирішують проблему концептуального бачення кібербезпекової проблематики через прийняття національних стратегій кібернетичної безпеки.

Питаннями забезпечення інформаційної безпеки України опікуються понад 20 державних органів і центральних органів виконавчої влади. Незважаючи на це, досі не налагоджено ефективної міжвідомчої взаємодії та не визначено єдиного спеціально уповноваженого органу, який займався б комплексним вирішенням усього спектру проблем у зазначеній сфері. Відсутність належної централізації управління та координації діяльності відповідних органів державної влади обумовлює недостатню ефективність системи формування та реалізації державної політики інформаційної безпеки.

Тому пріоритетними напрямками державної політики щодо посилення інформаційної (зокрема кібернетичної) безпеки держави, варто виділити такі:

- реформування нормативно-правових документів, які регулюють як визначення сучасних загроз інформаційній (кібернетичній) безпеці держави, але й механізмів реагування на них
- розроблення Стратегії кібернетичної безпеки України, в якій слід визначити мету, завдання, структуру та режим функціонування національної системи забезпечення кібернетичної безпеки, встановлення дієвого контролю за дотриманням чинного законодавства з питань інформаційного захисту;
- дослідження питань захисту об'єктів критичної інфраструктури від кібератак. З цією метою має бути визначено та класифіковано критичні об'єкти, кібератаки на які можуть завдати значної шкоди державі і створити загрози міжнародним стосункам у кіберпросторі;
- сприяння розробці вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави;
- завершення імплементації положень Конвенції РЄ про кіберзлочинність у національне законодавство;
- оптимізація системи підготовки кадрів у сфері кібербезпеки для потреб Збройних Сил України та інших органів сектору безпеки і оборони України;
- сприяння більш активній політиці державних безпекових інституцій щодо інформування населення про кіберзагрози;
- забезпечення безперервного підвищення кваліфікації військовослужбовців, державних службовців та працівників, що задіяні на ключових об'єктах критичної інфраструктури;
- сприяння недопущенню мілітаризації кіберпростору;
- підтримка як існуючих багатосторонніх навчань з протидії кібернападам на державну інформаційну інфраструктуру, так і ініціювання нових видів таких навчань.

Висновки

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам в кіберпросторі. До таких проблем в першу чергу відносяться: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів.

Пріоритетними напрямками державної політики щодо посилення інформаційної (зокрема кібернетичної) безпеки держави є реформування нормативно-правових документів у галузі інформаційної безпеки, дослідження питань захисту об'єктів критичної інфраструктури, сприяння недопущенню мілітаризації кіберпростору.

Список літератури

1. Горовий В.М. Концептуальні засади створення системи захисту національної інформаційної інфраструктури від кіберзагроз / В.М. Горовий, О.Д. Довгань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 2. – С. 15-21.

2. Климчук О.О. Кібервійна у сучасних умовах / О.О. Климчук, Р.М. Кравченко // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1. – С. 78-84.

3. Погорецький М. Поняття кіберпростору як середовища вчинення злочинів / М. Погорецький, В. Шеломенцев // Інформаційна безпека людини, суспільства, держави. – 2009. – № 2. – С. 77-81.

4. "Сучасні тренди кібербезпекової політики: висновки для України". Аналітична записка. [Электрон. ресурс] – Режим доступа: http://www.nisd.gov.ua /136711.pdf.

5. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю.І. Радковець, О.В. Левченко, О.М. Косогов // Наука і оборона. – 2014. – № 1. – С. 38-41.

6. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с

7. "Стратегія національної безпеки України" (Указ Президента України № 389/2012 від 8 червня 2012 року) [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/9570.html

Надійшла до редколегії 8.07.2014

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НАЦИОНАЛЬНОГО КИБЕРПРОСТРАНСТВА

А.Н. Косогов

На основе анализа нормативно-правового обеспечения информационной безопасности Украины определены проблемы обеспечения безопасности национального киберпространства. Предложены пути решения проблем в области государственной политики Украины в данной сфере.

Ключевые слова: *информационная безопасность государства, киберпространство, кибербезопасность, кибернетические угрозы.*

PRIORITY DIRECTION STATE POLITICIANS ON PROVISION OF NATIONAL KIBERPSPACE SECURITY

O.M. Kosogov

On base of the analysis normative-legal provision to information safety of the Ukraine are determined problems of the provision to security national cyberspace. Offered ways of the decision of the problems in the field of state politicians of the Ukraine in given to sphere.

Keywords: *national information security, cyberspace, cybersecurity, cybernetic threats.*