Національна безпека

УДК 004.931

Лащів Олексій Володимирович

студент

Навчально-наукового інституту інформаційної безпеки

Національної академії Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ПОНЯТТЯ, ПЕРСПЕКТИВИ РОЗВИТКУ ТА ОСНОВНІ ДЖЕРЕЛА ЗАГРОЗ

Анотація. *Досліджено перспективи розвитку інформаційної безпеки України, зокрема законодавче та практичне регулювання зазначеної сфери суспільних відносин, визначені фактичні загрози та джерела виникнення таких загроз інформаційній безпеці держави, охарактеризовано поняття «інформаційна безпека», надано практичні рекомендації щодо вдосконалення системи інформаційної безпеки України.*

Ключові слова: *інформаційна безпека України, інформаційні загрози, інформаційні операції, національна інформаційна інфраструктура, інформаційний вплив, державна інформаційна політика.*

Аннотация. *Исследованы перспективы развития информационной безопасности Украины, в частности законодательное и практическое регулирование указанной сферы общественных отношений, определены фактические угрозы и источники возникновения таких угроз информационной безопасности государства, охарактеризованы понятия «информационная безопасность», даны практические рекомендации по совершенствованию системы информационной безопасности Украины.*

Ключевые слова: *информационная безопасность Украины, информационные угрозы, информационные операции, национальная информационная инфраструктура, информационное воздействие,*

государственная информационная политика.

Summary. *The prospects of the development of information security of Ukraine, in particular, the legislative and practical regulation of this sphere of public relations were determined, the actual threats and sources of such threats to the information security of the state were determined, the concept of "information security" was described, practical recommendations were given regarding the improvement of the information security system of Ukraine.*

Key words: *information security of Ukraine, information threats, information operations, national information infrastructure, information influence, state information policy.*

В наш час повноцінне життя суспільства будь-якої сучасної країни дуже важко уявити без всебічного проникнення інформатизації в усі сфери взаємовідносин. Розвиненість та популярність інформаційних систем має велике значення для майбутнього переважної більшості людей і є однією з основних складових, що визначають сучасний образ та створює фундаментальну основу для повноцінного існування.

Останні події в історії нашої держави дозволяють стверджувати, що ми вступили у сучасний період інформаційних війн. Зокрема, інформаційна складова становить ключовий елемент гібридної війни проти України, що створює серйозну загрозу для безпеки її існування.

Метою даної статті є визначення основних напрямів розвитку інформаційної безпеки України та визначення основних джерел загроз її функціонуванню.

Інформаційна безпека є об'єктом дослідження для багатьох науковців пострадянського простору, серед яких О.Ю. Борисов, О.О. Левін, О.В. Литвиненко, Ю.Є. Максименко, І.О. Пеньков, Д.В. Сорокін та інші [1].

При детальному аналізі Закону України «Про основи національної безпеки України» розглядаються основні напрямки гарантування безпеки у інформаційній сфері, згідно якої у багатьох випадках розуміють інформаційну безпеку як складову національної безпеки України. В той же час необхідно відмітити, що зазначені поняття не є подібними за змістом. Під інформаційною сферою на рівні змісту розуміється інформація та сфера її обігу. Відповідно, безпека інформації – це стан захищеності інформації, сфер її створення та накопичення, оброблення, зберігання, використання та розповсюдження.

У понятійному змісті інформаційна безпека України, це:

- по-перше, здатність держави, суспільства та соціальних груп (групи) забезпечити інформаційні ресурси достатнім рівнем захищеності, надійності функціонування інформаційних та комунікаційних систем в інтересах повноцінного функціонування та сталого розвитку суспільства;
- по-друге, здатність держави протистояти інформаційним загрозам та небезпекам, негативним інформаційним впливам на індивідуальну та суспільну свідомість, інформаційні структури;
- по-третє, здатність держави підтримувати постійну готовність до адекватних відповідей у інформаційному протиборстві[2].

Отже, підсумовуючи вищезазначене, інформаційна безпека – це здатність держави, суспільства та соціальних груп (групи) забезпечити інформаційні ресурси достатнім рівнем захищеності, надійності функціонування інформаційних та комунікаційних систем та протистояти інформаційним загрозам та небезпекам, негативним інформаційним впливам, підтримуючи постійну готовність до адекватних відповідей у інформаційному протиборстві.

Щодо визначення існуючих основних загроз національним інтересам і національній безпеці України, серед яких є також інформаційні загрози,

законодавець визначив вказані фактори у ст.7 Закону України «Про основи національної безпеки України». Їх перелік у вказаній статті класифікований законодавцем за дев'ятьма сферами суспільних відносин: внутрішньополітичні, зовнішньополітичні, воєнні, сфери безпеки, економічні, науково – технологічні, цивільного захисту, екологічні, інформаційні. Конкретизуючи останню сферу, законодавець зазначає такі загрози в інформаційній сфері: прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [3]. Враховуючи, що в даний закон були внесені значні зміни у 2014-2015 роках та виходячи з переліку зазначених загроз у інформаційній сфері, слід зазначити, що в ньому відсутня велика кількість важливих елементів зазначених загроз та не відображено їх повного переліку.

Лише через два роки після внесення змін Закону України «Про основи національної безпеки України» було прийнято рішення Ради національної безпеки та оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», яке введено в дію указом Президента України від 25 лютого 2017 року № 47/2017, основні джерела загроз інформаційній безпеці України поділено у відповідності до ст. 7 Закону України «Про основи національної безпеки України» на внутрішні та зовнішні. До зовнішніх загроз віднесені:

- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території інших держав;

До внутрішніх загроз відносяться:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України;
- інформаційне домінування держави-агресора на тимчасово окупованих територіях;
- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [4].

Отже, аналізуючи вищевказаний перелік інформаційних загроз, визначений рішенням Ради національної безпеки та оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» слід зазначити, що Радою національної безпеки та оборони України було конкретизовано внутрішні та зовнішні загрози інформаційній безпеці України, відображений повний перелік їх основних складових частин в умовах сучасної інформаційної війни. Крім того в Доктрині викладені пріоритети державної політики у інформаційній сфері, а також механізм її реалізації.

Неможливо не помітити, що у сучасному суспільстві інформація набуває все більш важливої ролі. І це змінює правила гри у військовій, політичній та економічній сферах. Новий інструментарій в арсеналі інформаційного протиборства привносить не лише значно дешевші засоби впливу, які досить часто навіть помітити складно, що несе в собі приховану небезпеку, яку необхідно вчасно виявляти та нейтралізовувати в найкоротший термін [5].

В той же час слід відмітити що визначення і конкретизація зазначених загроз, пріоритети державної політики у цій сфері та механізм протидії визначався достатньо повільно, оскільки з початку окупації Російською Федерацією Кримського півострову та гібридної війни проти України на Донбасі пройшло майже три роки, внаслідок чого наша держава зазнала великих людських, територіальних, фінансових втрат. Перш за все слід відзначити, що тимчасова втрата частини території України стала можливою за рахунок успішного ведення інформаційної війни проти України, а саме внаслідок проведення низки руйнівних

інформаційних операцій на нашій території, поєднаних з військовими діями, націленими на позбавлення нашої країни територіальної цілісності.

До основних перешкод на шляху побудови ефективної системи інформаційної безпеки України слід віднести недостатнє фінансування та низькій рівень технічного забезпечення спеціально уповноважених органів державної влади у цій сфері, недостатня кількість кваліфікованих кадрів, незадовільний рівень оплати праці фахівців цього напрямку, низький рівень координації органів державної влади з суміжними повноваженнями, ускладнений порядок обміну інформацією внаслідок недосконалого законодавчого регулювання.

Відповідно до вищенаведеного, задля вдосконалення системи інформаційної безпеки державою повинні бути зроблені певні кроки у цьому напрямі, а саме: здійснення підвищення фінансування та збільшення рівня технічного забезпечення уповноважених державних органів у сфері інформаційної безпеки держави, запровадити та інтенсифікувати існуючі програми навчання та обміну досвідом з відповідними компетентними державними органами країн ЄС та НАТО в сфері інформаційної безпеки, ведення уповноваженими органами та посадовими особами переговорів щодо вирішення питання про надання Україні допомоги в рамках міжнародних програм у галузі інформаційно-технічного співробітництва.

Вирішення державою вищезазначених проблем значно підвищить рівень інформаційної захищеності України та позитивно вплине на загальний рівень стану безпеки.

Література

1. Коротченко Е.Г. Информационно-психологическое противоборство в современных условиях / Военная мысль, 1996. – С. 9.
2. Нарис теорії і практики інформаційно-психологічних операцій / За заг. ред. В.В. Балабіна. – К: ВІТІ НТУУ«КПІ», 2006. – С 178.

3. Про основи національної безпеки України :Закон України від 19.06.2003 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15.
4. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017 [Електронний ресурс]. – Режим доступу: www.president.gov.ua/documents/472017-21374.
5. Сучасні інформаційні війни / Г. Почепцов. – К.: Вид. дім "Києво-Могилянська академія", 2015. – 497 с.