Строяновський В.В.,
старший викладач Національної академії Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

TOPICAL ISSUES OF IMPROVING SYSTEM CYBER SECURITY OF UKRAINE

Постановка проблеми. Гібридна війна, ключовим елементом якої є інформаційний чинник, формує довгострокові виклики для Української держави. У нещодавно проголошеній "Стратегії реформ – 2020" заявлено про необхідність реформи системи національної безпеки і оборони, одним з ключових пріоритетів якої має стати кібернетична безпека [1].

Ця обставина і визначає ***зв'язок загальної проблеми з найбільш важливими науковими та практичними завданнями*** дослідження проблем теорії та практики забезпечення кібернетичної безпеки України в умовах гібридної війни. Адже недосконаліть правового, інституційного та науково-методичного забезпечення кібернетичної безпеки гальмує реформування системи національної безпеки України загалом.

На підставі аналізу актуальних досліджень і наукових публікацій [2-11] можна зробити висновок про те, що проблеми забезпечення кібернетичної безпеки в сучасних умовах стали предметом дослідження фахівців з національної безпеки, державного управління та правознавців. Проте, незважаючи на значну кількість робіт, в яких досліджуються проблеми забезпечення кібернетичної безпеки України, маємо констатувати, що сьогодні ще обмаль праць в яких би аналізувалися питання відповідності правового забезпечення кібернетичної безпеки України завданням адекватного державного реагування на сучасні виклики та загрози національним інтересам у цій сфері.

Саме тому ***мета статті*** полягає в розгляді актуальних питань удосконалення системи кібернетичної безпеки України.

Виклад основного матеріалу. На даний час Україна фактично воює в умовах "гібридної війни", яка поєднує військові, інформаційні, терористичні та інші агресивні дії.

"Гібридна війна" передбачає 3 стадії:

розхитування ситуації через кризу інспірування внутрішньодержавного конфлікту;

деградація, розорення і розпад країни з перетворення її в "недієздатну державу";

зміна політичної влади на цілком підконтрольну агресору.

Населення України все частіше звертається до Інтернету, як джерела оперативних новин та інформації, яка надходить безпосередньо з місць подій.

Ст. 7 Закону України "Про основи національної безпеки" визначає загрози національним інтересам України в інформаційній сфері однією з яких є намагання маніпулювати суспільною свідомістю, шляхом поширення недостовірної, неповної або упередженої інформації [12].

Водночас, в Стратегії національної безпеки від 2012 року визначено такі стратегічні цілі та основні завдання політики національної безпеки:

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, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

розроблення і впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у т.ч. згідно з вимогами Конвенції про кіберзлочинність;

створення національної системи кібернетичної безпеки [13, с. 136].

Поширення кіберзлочинності є чинником, що загрожує глобальній міжнародній стабільності й негативно позначається на безпеці інформаційного простору України.

Кіберзагрози Україні та суспільству умовно можна розділити на 2 рівні. Перший – "класичні" кіберзлочини, що потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби: хактивізм, кібершпигунство та кібердиверсії. Техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою.

При цьому, низка кіберзлочинів має на меті й може скоюватися для збагачення злочинців. В Україні в повному обсязі присутні всі ключові "класичні" кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз

даних, поширення порнографії, продаж зброї чи наркотиків тощо) і щороку їх кількість зростає [2].

Розглядаючи динаміку кількості кримінальних проваджень, порушених СБ України та МВС України за фактами виявлених кіберзлочинів, прослідковується їх істотне збільшення. Стрімко зростає кількість шахрайств, здійснюваних за допомогою високих інформаційних технологій та злочинів, пов'язаних з незаконними діями з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення.

Загалом можна констатувати, що кількість виявлених злочинів демонструє виразну тенденцію до зростання абсолютно за всіма основними статтями КК України, що стосуються злочинів, здійснюваних із використанням високих інформаційних технологій. У структурі злочинів переважають різноманітні випадки шахрайств, основною жертвою яких є банківський сектор.

В Україні спостерігаються доволі високі показники розкриття кіберзлочинів у банківській сфері [3]. Водночас, при оцінюванні рівня розкриваності фінансових кіберзлочинів варто зважати на високий рівень їх латентності – банківським установам переважно вигідніше закрити очі на вкрадені кошти й тихо компенсувати їх із власних ресурсів, ніж заявляти про це у правоохоронні органи [4].

Державі стає відомо лише про 5 % злочинів у кіберпросторі, а значна кількість потерпілих від них можуть тривалий час і не знати про те, що їх атакували. Іноді на виявлення факту "зламу" витрачаються місяці (якщо це спрямований "злам", здійснений фахівцями, – роки) [5].

Таким чином можна констатувати, що далеко не завжди держава реально обізнана з масштабами кіберзлочинності. І ця проблема наявна у всіх державах, де кіберзлочинність набирає обертів. Зростають масштаби більш складних кіберзлочинів.

Якщо говорити про злочини, віднесені до групи геополітичних, чи міждержавних, механізмів боротьби (кібершпигунство та кібердиверсії), то Україна в окремих випадках стає об'єктом кібершпигунських акцій.

У Всесвітній мережі (а також соціальних мережах) активно поширювалися інструкції про те, як саме можна здійснювати *DDoS*-атаки.

Крім пересічних користувачів, які брали участь в атаці, в мережі було запущено спеціальний проект "Низькоорбітальна іонна гармата" (*Low Orbit Ion Cannon*), який мав полегшити проведення *DDoS*-атак.

Водночас кримінальних проваджень чи інших процесуальних дій за результатами цих атак так і не було порушено [6], оскільки, по-перше, до правоохоронних органів із відповідними заявами ніхто з постраждалих так

і не звернувся, а по-друге, особливістю *DDoS*-атак щодо урядових ресурсів є те, що прямого економічного збитку державні органи від них не зазнають.

Масштабною хактивістською кампанією стало політичне протистояння в жовтні 2013 року – лютому 2014 року довкола підписання/непідписання тодішньою владою Угоди про асоціацію між Україною та ЄС (події Євромайдану). Це протистояння активно відбувалося в соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану невідомі особи почали масово використовувати нет-боти з метою засмічення інформаційного поля, введення людей в оману та поширення чуток [7].

Загалом відбулася прицільна атака на ресурси та інструменти, які забезпечують комунікацію політиків із громадськістю та ЗМІ через інтернет. Використовувалися механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків), що унеможливило використання їхніх мобільних телефонів у роботі.

Постраждали й електронні ЗМІ, які були головними інформаційними майданчиками, а заразом і рушійними силами акцій протесту. Кілька днів поспіль хакерських атак зазнавав сайт "Української правди" та "Главкому".

Це змусило зазначені ЗМІ переносити свою активність до соцмереж, тобто розміщувати новини у соціальних мережах [8].

Загострились українсько-російські відносини, що частково є наслідком суспільно-політичної кризи, яка охопила українське суспільство протягом грудня 2013 року – лютого 2014 року. В результаті протистояння було сформовано загони хактивістів, які йменують себе "Кіберберкутом" (*Cyberberkut* – віртуальна структура, що не визнає української влади, яка сформувалася після лютого 2014 р.) та "Кіберсотнею Майдану", "Анонімусами" з російською або українською "пропискою" тощо.

"Кіберберкут" здійснив атаки на сайти структур НАТО: на офіційний сайт НАТО, а також на сайти Центру кіберзахисту НАТО в м. Таллінні та Парламентської асамблеї НАТО. Він здійснював також й дефейси, розміщуючи на атакованих ними сайтах карту України, де західні області помічені нацистською свастикою, а з Криму виходять стріли напрямів "фронтових ударів" на Південь і Схід України.

Найбільш масованою атакою "Кіберберкуту" на урядові інтернет-ресурси була атака, від 3 березня 2014 року, в результаті чого складнощі в роботі відчули понад 100 урядових та різноманітних інтернет-ЗМІ сайтів.

В інтернет-протистоянні Росії з Україною проти України вперше було застосовано троянські програми (віруси). З одного боку, завданням вірусів було формування бот-мережі із заражених комп'ютерів та

отримання повноцінного доступу до їх наповнення, а з іншого – викрадення інформації з цих комп'ютерів. Основним мотивом ініціатора кібератаки було бажання встановити прихований контроль за визначеними об'єктами для подальшого спостереження за інформаційним обміном із власної території.

Останнім часом майже в 2 рази зросла кількість шахрайств, здійснюваних за допомогою високих інформаційних технологій та злочинів, пов'язаних з незаконними діями з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення.

Під час "революції гідності" "зламувались" електронна пошта та аккаунти відомих політиків, після чого масово розсилаються фейкові (підроблені) повідомлення, спрямовані на дезінформування суспільства. Відбувалися кібератаки на ресурси та інструменти, які забезпечують комунікацію політиків із громадськістю та ЗМІ через інтернет.

Велике значення має кваліфікація вітчизняних журналістів, які висвітлюють події в АТО в Інтернет просторі. Адже нині в Україні працює понад 35 тис. журналістів, а лише 40 % з них мають базову професійну освіту. На жаль, не всі журналісти у своїй роботі спираються на відповідні інформаційні документи, кодекси професійної етики, інші документи, в результаті чого вони можуть поширювати необ'єктивну та недостовірну інформацію, що призводить до образи честі та гідності, ділової репутації.

Сьогодні нашому суспільству потрібні, соціальна відповідальність журналістів за свою діяльність, паритетні відносини ЗМІ та влади, ЗМІ та вітчизняного судочинства.

Основним джерелом журналістських етичних вимог повинен бути кодифікований Кодекс журналістської етики, який регулюватиме моральні відносини громадськості, окремих осіб, організацій, установ, фірм, підприємств тощо з журналістами, редакціями. Тобто він поширюватиме дію на неетичні відносини юридичних, фізичних осіб, які займаються творчою, технічною журналістською діяльністю. Роль саморегулювання етичних проблем особливо зростає у перехідний до демократії період, що зумовлює актуальність і значення кодифікованого Кодексу журналістської етики.

Потреба у новому кодифікованому Кодексі етики журналіста України зумовлена багатьма чинниками. В Кодексі, повинні відтворюватися суттєві зміни в державі, наприклад наявність державних, комерційних, приватних, незалежних ЗМІ й існування нових моральних взаємин журналіста й читача, не передбачено відповідальності журналіста

за шкоду, завдану аморальною поведінкою журналіста підчас виконання своїх обов'язків.

Крім того, у чинному українському Кодексі немає статей, що засуджували б приховану рекламу, регулювали мораль журналіста у кіберпросторі, визначали статус самого Кодексу.

Щодо форми, то чинний Кодекс журналістської стики містить в одній статті поєднання кількох вимог, що формально не відповідає вимогам до кодексів і, крім того, є логічною помилкою. Сучасною формою Кодексу журналістської етики повинен бути кодифікований Кодекс, що конкретно визначав би моральні проступки журналістів і встановлював би за них відповідальність на прикладі етичних кодексів журналістів та інших документів Австралії, Австрії, Великої Британії, Німеччини, Іспанії, Канади, Нідерландів, Норвегії, Росії, США, Франції, Швеції.

На сьогодні, правова основа, міжнародний досвід, етичні принципи висвітлення антитерористичної операції містяться в рекомендаціях СБ України, які визначають правові засади, основні принципи й загальні цілі інформування громадськості про антитерористичну операцію, порядок взаємодії оперативного штабу із засобами масової інформації з урахуванням визначених законодавством обмежень на поширення інформації в ході проведення антитерористичної операції.

При цьому особливу увагу звертає на себе аналіз активності користувачів, які перебувають в зоні АТО.

Дослідження особливостей користування мережею в Донецькій та Луганській областях, які опинилися в епіцентрі бойових, соціально-економічних, соціально-політичних потрясінь за даними соціологічного дослідження Інституту соціології НАН України, у 2014 році засвідчили певні відмінності інтернет-активності мешканців Донбасу порівняно з іншими регіонами країни.

Дослідження засвідчило особливості використання інтернет-мережі в кризових умовах, в умовах АТО. Як загальну основну тенденцію реалізації інтернет-активності користувачів у 2014 році можна означити збільшення потреби в отриманні новин в мережі. А значна активізація використання певних можливостей мережі мешканцями Донбасу засвідчує важливу роль Інтернету у вирішенні багатьох питань та проблем, які виникають в кризових умовах життя.

Проте суттєво збільшилась порівняно з іншими регіонами інтернет-активність мешканців Донбасу, пов’язана з можливостями спілкування в мережі, як безпосереднього за допомогою спеціальних програм (Скап, Сіпнет тощо), так і опосередкована – через соціальні мережі, форуми, чати тощо.

Таке спілкування допомагає дізнатись про останні новини безпосередньо від очевидців та учасників подій; відшукати однодумців, партнерів для реалізації певних ініціатив; знайти співчуття, підтримку та допомогу. Спілкування в соціальних мережах стає чи не єдиною можливістю для рідних дізнатися про те, що відбувається з їх родичами у зоні АТО.

При цьому, через можливості Інтернет-ресурсу в рамках "Гібридної війни" здійснюється "Інформаційна війна" шляхом нагнітання масової істерії і спротиву законній владі у населення.

При цьому, через Інтернет здійснюється інформаційний вплив на населення Донбасу, в результаті чого виникають випадки паніки та антивоєнні настрої у прилеглих до зони АТО районах (м.м. Маріуполь, Артемівськ, Северодонецьк тощо), що в цілому спрямоване на зрив мобілізації в Україні.

Загалом через Інтернет відбувається спонукання громадян до зради власної держави, підтримки агресора та руйнування морального стану військовослужбовців і цивільного населення нашої держави. Одночасно журналісти російських каналів формують "правильну картинку" як на каналах телебачення так і в мережі Інтернет.

Фактично на непідконтрольних української влади територіях представниками спецслужб РФ здійснюється:

інформаційно-психологічні операції шляхом інформаційного впливу на масову свідомість громадян України та дезінформування суб'єктів прийняття управлінських рішень;

негативний вплив на свідомість громадян та формування потрібного інформаційного впливу поза межами АТО;

поширення чуток через активних осіб, російське ТБ, інформаційні повідомлення в друкованій пресі, листівках, місцевих кабельних операторів та всеукраїнських Інтернет ЗМІ.

При цьому, як показує правовий аналіз змісту виступів, статей та публікацій антидержавної та антиукраїнської спрямованості, які надходять до СБ України, вони не містять ознак статей 111 "Державна зрада", 161 "Порушення рівноправності громадян залежно від їх національної належності та за іншими ознаками", 436 "Пропаганда війни" КК України.

Зазначене викликано неефективною роботою органів державної влади та правоохоронних органів у сфері протидії розповсюдженню через ЗМІ та інші сфери публічної комунікації панічних та завідомо неправдивих даних.

Законодавством України передбачена цивільно-правова відповідальність за поширення недостовірної інформації, однак такий

механізм не є дієвим в умовах загострення суспільно-політичного конфлікту в Україні, проведення бойових дій та ведення агресивної "інформаційної війни".

Висновки. Відсутність юридичної кваліфікації діянь – "операцій інформаційної війни" *(дезінформування, маніпулювання, пропаганди, дестабілізації, прихованого керування та негативного впливу на свідомість громадян)* не дозволяє використовувати кримінальне та кримінально-процесуальне законодавство з метою їх припинення.

У зв'язку з чим, доцільно розглянути питання щодо встановлення в особливий період, в умовах проведення антитерористичної операції, військового стану, бойової обстановки, режиму НС кримінальної відповідальності щодо:

умисного публічного розповсюдження завідомо неправдивої інформації вчиненого з метою поширення тривоги, паніки та страху в суспільстві, підбурювання до насильства, ненависті чи дискримінації, закликів до підриву та невиконання законних вимог службових осіб органів державної влади, правоохоронних органів та військових формувань у зв'язку з виконанням ними службових обов'язків, за відсутності ознак більш тяжкого злочину;

екстремістської діяльності – виготовлення, зберігання з метою збуту чи розповсюдження, а також збут, розповсюдження екстремістських матеріалів, публічні висловлювання чи заклики екстремістського характеру, за відсутності ознак більш тяжкого злочину;

поширення завідомо неправдивої інформації, що ганьбить честь, гідність та репутацію особи, вчинене у зв'язку з виконанням нею службових, громадських та інших обов'язків у вищевказаних умовах.

Список використаної літератури

1. Стратегія розвитку України – 2020: [Електронний ресурс] / Офіційний веб-портал Президента України. – Режим доступу:http://www.president.gov.ua. – Назва з екрана.

2. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/?q=system/files/sites/default/files/images/dop.doc. – Назва з екрана.

3. Літвінов М. Об'єднавши зусилля, ми досягнемо високих результатів у боротьбі з кіберзлочинністю / М. Літвінов [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/915190. – Назва з екрана.

4. Банкам выгоднее закрывать глаза на украденные деньги, чем сообщать о кибератаках на их ресурсы [Електронний ресурс]. – Режим доступу: http://112.ua/politika/bankamvygodnee-zakryvat-glaza-na-ukradennye-dengichem-soobschat-o-kiberatakah-na-ih-resursyekspert-20442.html. – Назва з екрана.

5. Інфографіка: злами інформаційних систем, а також час виявлення та реагування на них [Електронний ресурс]. – Режим доступу: https://scontent-a.xx.fbcdn.net/hphotos-prn1/t1.0-1604423_617599488319664_1554722890_n.jpg. – Назва з екрана.

6. Криміналу за фактом хакерських атак на сайт МВС не буде [Електронний ресурс]. − Режим доступу: http://24tv.ua/home/showSingleNews.do?kriminalu_za_faktom_hakerskih_atak_na_sayt_mvs_ne_bude&objectId=185800. – Назва з екрана.

7. Боти намагаються засмічувати інформаційне поле Євромайдана – як з цим боротись [Електронний ресурс]. – Режим доступу: http://v-n-zb.livejournal.com/6379558.html. – Назва з екрана.

8. Саваневський М. Євромайдан: українська цифрова революція та останній шанс аналоговим політикам стати цифровими / М. Саваневський [Електронний ресурс]. – Режим доступу:http://watcher.com.ua/2013/11/yevromaydan-ukrayinska-syfrovarevolyutsiya-ta-ostanniy-shans-analohovym-politykam-staty-tsyfrovymy/. – Назва з екрана.

9. Зараження вірусом Uroburos [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?p=344. – Назва з екрана.

10. Demchak Chris *C.* Rise of a cybered westphalian age / Chris C. Demchak, Peter Dombrowski // Strategic Studies Quarterly. – 2011. – №5(1). – P. 32–61.

11. Maher K. The New Westphalian Web Web / Katherine Ma her // Foreign Policy [Електронний ресурс]. – Режим доступу: http://www.foreignpolicy.com/articles/2013/02/25/the_new_westphalian_web. – Назва з екрана.

12. Про основи національної безпеки України: закон України від 19.06.2003 № 964-IV [Електронний ресурс] Верховна Рада України. − Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15.− Назва з екрана.

13. Нормативно-правова база в галузі безпеки і оборони України: видання друге, доповнене / А. Гриценко, М. Кожієл, А. Єрмолаєв, Ф. Флурі. – К.: Центр дослідження армії, конверсії та роззброєння, 2012. – 820 с.