МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет правознавства, публічного управління та національної безпеки

Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

ЧЕРНИШ РОМАН ФЕДОРОВИЧ

УДК 659.4:327.88

КВАЛІФІКАЦІЙНА РОБОТА

«ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ПРОВЕДЕННЯ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ ТА «ГІБРИДНОЇ ВІЙНИ»»

281 «Публічне управління та адміністрування»

Подається на здобуття освітнього ступеня «Магістр»

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____Черниш Р.Ф.

Науковий керівник
Литвинчук Ірина Леонідівна
доктор економічних наук, професор

Житомир 2021

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління за результатами попереднього захисту:

_____

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № __ від «___» _____ 202_ р.

Завідувачка кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ В.П. ЯКОБЧУК
(підпис)

«___» _____ 202_ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти Черниш Роман Федорович захистив кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою_____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК _____ Н.С. Пугачова
(підпис)

АНОТАЦІЯ

Черниш Р.Ф. Інформаційна безпека держави в умовах операції об’єднаних сил та «гібридної війни». Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 «Публічне управління та адміністрування». Поліський національний університет, Житомир, 2021.

В реаліях сьогодення інформаційний простір, за умови жорсткої міжнародної конкуренції, використовується державами як арена для боротьби їх різновекторних національних інтересів. Насамперед, це пов’язано з тим, що сучасні інформаційні технології надають змогу реалізувати власні національні інтереси без ведення активних бойових дій. При цьому, значна шкода завдається національній безпеці держави - протагоніста, в якій не функціонує дієва система захисту від деструктивних інформаційних впливів.

Особливої актуальності окреслене питання набуло в контексті реалізації Російською Федерацією різноманітних форм та методів ведення «гібридної війни» по відношенню до України.

Стан забезпечення безпеки інформаційного простору України свідчить про системне залучення фахівців ІТ-галузі, до здійснення актів кіберагресії проти України з використанням спеціального програмного забезпечення шкідливої дії. Поряд з тим, відбувається несанкціоноване втручання в роботу офіційних веб-ресурсів органів державної влади та органів місцевого самоврядування. Вказані протиправні дії призводять до спотворення процесу обробки інформації, її несанкціонованої маршрутизації та, можливого, використання в протиправних цілях (в тому числі й для ведення так званої «гібридної війни»).

Вироблення дієвих організаційних та нормативно-правових способів протидії вказаним протиправним антидержавницьким діям є вкрай нагальним.

Ключові слова: Інтернет, гібридна війна, національна безпека, інформація, акти кіберагресії.

ANNOTATION

Roman Chernysh. State information security in the context of a joint force operation and a «hybrid war». Qualification work on the rights of the manuscript.

Qualification work for a master's degree in specialty 281 «Public Administration». Polissia National University, Zhytomyr, 2021.

In today's realities, the information space, under conditions of fierce international competition, is used by states as an arena for the struggle of their multifaceted national interests. First of all, this is due to the fact that modern information technologies make it possible to realize one's own national interests without conducting active hostilities. At the same time, significant damage is done to the national security of the state - the protagonist, in which there is no effective system of protection against destructive information influences.

The outlined issue became especially relevant in the context of the implementation by the Russian Federation of various forms and methods of conducting a «hybrid war» against Ukraine.

The state of ensuring the security of the information space of Ukraine indicates the systematic involvement of IT professionals in the implementation of acts of cyber-aggression against Ukraine using special malicious software. At the same time, there is unauthorized interference in the work of official web resources of public authorities and local governments. These illegal actions lead to distortion of the information processing process, its unauthorized routing and, possibly, use for illegal purposes (including for the so-called «hybrid war»).

Elaboration of effective organizational and normative-legal ways of counteracting the specified illegal anti-state actions is extremely urgent.

Key words: Internet, hybrid war, national security, information, acts of cyber aggression.

ЗМІСТ

ВСТУП

Актуальність дослідження. 2014-2017 рр. стали найбільш кривавими в історії новітньої України. За даними ООН, у вказаний проміжок часу, через російську агресію з 2014 року на сході держави загинули понад 10 тис. українців. Серед них – близько 3 тис. українських військовослужбовців [34].

Однак, українцям вдалося згуртуватися і дати гідну відсіч ворогу. Зважаючи на викладене, країна-агресор у 2017-2018 рр. почала змінювати формат протистояння: перехід від активних (відкритих) бойових дій, до реалізації нових методів ведення гібридної війни

Зокрема, відмічається активізація хакерських угрупувань, які діють за вказівки спеціальних служб РФ, в напрямку поширення шкідливого програмного забезпечення, яке має можливості доступу до інформації з обмеженим доступом, що циркулює в органах державної влади, місцевого самоврядування, правоохоронних органах, державних підприємствах, установах, організаціях, об’єктах критичної інфраструктури тощо.

Окремі аспекти окресленої проблематики в своїх наукових працях розглядали В. Гребенюк, І. Доронін, М. Кіца, Л. Макаренко, А. Марущак, К. Молодецька, І. Мудра, Е. Паршакова, Г. Почепцов, О. Саприкін, Т. Ткачук, В. Цимбалюк тощо. Однак, зважаючи на динаміку розвитку суспільних відносин в інформаційній сфері, питання інформаційної безпеки держави в умовах проведення операції Об’єднаних сил та «гібридної війни»» потребують подальшої наукової розробки.

Мета і завдання дослідження. *Мета* кваліфікаційної роботи полягає у тому, щоб на підставі критичного аналізу національного законодавства та практичної діяльності відповідних уповноважених суб’єктів та громадських інституцій, зважаючи на необхідність організації дієвої протидії країні-агресору у всіх сферах суспільного життя (насамперед недопущення інформаційного впливу на свідомість громадян, витоку інформації з обмеженим доступом тощо), а також нейтралізації передумов до нанесення шкоди інтересам держав,

запропонувати зацікавленим суб'єктам вжити конкретних упереджувальних заходів.

Для досягнення поставленої мети в роботі вбачається за доцільне виконати наступні *завдання*:

- визначити та охарактеризувати форми та методи ведення представниками спеціальних служб Російської Федерації «гібридної війни» в інформаційній сфері;
- проаналізувати діяльність спеціальних підрозділів інформаційного впливу Російської Федерації;
- дослідити процес протидії сепаратизму в інформаційній сфері, як передумови реалізації євроінтеграційних процесів;
- проаналізувати використання програм віддаленого доступу, як загроз національній безпеці України;
- охарактеризувати механізми поширення шкідливого програмного забезпечення на об'єктах критичної інфраструктури, органах державної влади та місцевого самоврядування;
- визначитися з шляхами протидії маніпулюванню громадською думкою з використанням засобів масової інформації та Інтернет мережі;
- розробити для зацікавлених суб'єктів конкретні пропозиції спрямовані на забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни».

Об'єкт дослідження: сучасний стан забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни».

Предмет дослідження: суспільні відносини, що виникають в процесі забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни».

Методи дослідження. Методологічну основу кваліфікаційної роботи складають відповідні методи наукового дослідження. Завдяки використанню логічного і аналітичного методів вдалося відібрати, систематизувати та проаналізувати інформацію за темою дослідження (розділ 1, 2, 3). В процесі

застосування історично-правового методу вдалося відслідкувати хронологію становлення окремих інституцій (підрозділи 1.2., 1.3.). Для аналізу і характеристики сучасних тенденцій забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни» було використано порівняльно-правовий і описово-аналітичний методи (розділ 1, 2). Формально-юридичний метод дозволив здійснити вивчення змісту правових документів, що регулюють процедуру забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни» в конкретних сферах суспільного життя (розділ 2,3).

Апробація результатів дослідження. Окремі результати та висновки, отримані в ході проведеного дослідження, були предметом обговорення на засіданні кафедри економічної теорії, інтелектуальної власності та публічного управління Поліського національного університету та висвітлені у відповідних науковий публікаціях у вітчизняних фахових виданнях внесених до «Переліку наукових фахових видань України» (всього понад 10), в т.ч. й тих, які індексуються в міжнародних наукометричних базах Scopu та WoS [3, 4, 5]. А також в ході доповідей на відповідних науково-практичних конференціях (всього понад 10).

Практичне значення одержаних результатів полягає в тому, що висновки отримані за результатами кваліфікаційного дослідження можливо використати у: *науково-дослідній сфері* – для подальшого вивчення і дослідження окресленої теми; *нормотворчій діяльності* – у процесі реформування та удосконалення вітчизняного законодавства; *правозастосовній діяльності* – у діяльності відповідних державних органів та громадських організацій.

Структура дипломної роботи: вступ, 3 розділи, сім підрозділів, висновки, список використаних джерел (50 найменувань). Загальний обсяг 48 аркушів.

РОЗДІЛ 1. «ГІБРИДНА ВІЙНА» РФ ПРОТИ УКРАЇНИ: ФОРМИ, МЕТОДИ ТА СИЛИ

1.1. Форми та методи ведення представниками спеціальних служб Російської Федерації «гібридної війни» в інформаційній сфері

Протягом останнього часу продовжують фіксуватися тенденції до зміни курсу РФ по відношенню до України – перехід від відкритого збройного протистояння на сході України до реалізації форм та методів ведення т.зв. «гібридної війни».

На нашу думку основними серед них є:

– залучення осіб з «хакерського середовища» (відкрито та «під чужим прапором») до створення шкідливого програмного забезпечення, яке за певних умов після інсталяції на ПЕОМ може призвести до витоку службової інформації, яка на них обробляється.

Зокрема, з початку 2016р. фіксується активізація протиправної діяльності російських «хакерських» угруповань по створенню загроз інформаційній безпеці України шляхом ініціювання кібератак типу APT та несанкціонованих втручань в інформаційні системи та комп'ютерні мережі державних і приватних установ з використанням шкідливого програмного забезпечення (APT 28, «Sofacy», «Potao», ШПЗ «WannaCry», «Petya.A» та «NotPetya»).

Внаслідок реалізованих «атак» в різний період було заблоковано діяльність таких структур, як аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця, Укренерго тощо [39].

Атаки відбувалися під час оновлення програмного забезпечення, в результаті чого здійснювалось внесення змін до системних бібліотек операційної системи «Windows» та створення т.зв. «backdoor».

В результаті проведених маніпуляцій на ПЕОМ відбувалось шифрування файлів та знищення файлової системи.

Згідно наявної інформації, активну участь у проведенні «хакерських» атак, направлених на відповідні українські структури, взяла російська «хакерська» група «Lurk» [1].

При цьому, з урахуванням збільшення популярності т.зв. «майнінгу» (діяльність спрямована на отримання винагороди емітованої валюти і комісійних зборів у різних криптовалютах, зокрема біткойнах), прогнозується реалізація нової серії «хакерських» атак (у т.ч. й на державні органи та установи України) з використанням нових вірусів.

Проблемним питанням виявлення та нейтралізації вказаного вірусу є те, що він не блокує роботу ПЕОМ. Основною його ціллю є втягнення обчислювальної комп'ютерної техніки конкретного користувача чи/та установи у «майнінг». Також вищевказане не виключає можливість копіювання даних щодо персонального комп'ютера та документів, які на ньому містяться, з подальшою передачею на відповідні ftp-сервери.

– реалізація представниками спеціальних служб РФ інформаційних акцій, спрямованих на дискредитацію здійснюваних урядом України реформ та висвітлення в негативному ракурсі соціально-економічного становища в Україні.

Підґрунтям для однієї з них став оприлюднений 29.01.2018р. звіт комісії ООН з продовольчої безпеки на планеті та Продовольчої і сільськогосподарської організації ООН (FAO – «Food and Agriculture Organization of the United Nations»), яка виконує моніторингову місію на території Донецької та Луганської областей, у т.ч. на тимчасово окупованих територіях.

У зазначеному звіті зазначалося, що на окупованих територіях Донецької та Луганської областей (в зоні конфлікту) з населенням у 1,2 млн. осіб 26% з них відчуває обмеження у харчуванні та може перебувати у стані голоду [2]. Однак, вказані дані, шляхом стандартної маніпуляції цифрами та екстраполяції їх на всю територію України, були використані

представниками спеціальних служб РФ для поширення «фейкової» новини про «наслідки реформ діючого уряду в Україні».

Спочатку вищевказані матеріали було розповсюджено на загальноросійських каналах та сайтах антиукраїнської спрямованості «Россия 1» та «TV Звезда». В подальшому «новина» була розтиражована на платформах різнопланової спрямованості (як російських, так і українських).

Водночас, на нашу думку, на увагу у поширені зазначеної «новини» заслуговують канали її розповсюдження (спрямованість сайтів, які були використані з цією метою). Так, поряд із центральними загальноросійськими сайтами відверто антиукраїнської спрямованості використовувались й вітчизняні інтернет-ресурси, у т.ч. регіональні;

– використання регіонального сегменту мережі Інтернет (насамперед соціальних мереж) представниками спеціальних служб РФ, а також підконтрольними їм бойовиками терористичних організацій «ДНР/ЛНР», для впливу на громадян України та формування у них антигромадської позиції, що набуло особливої актуальності на фоні ускладнення соціально-економічної та суспільно-політичної ситуації та погіршення рівня життя населення.

В ході моніторингу Інтернет-мереж соціального спрямування встановлено, що деструктивний інформаційно-психологічний вплив з боку спецслужб РФ та підконтрольних їм терористичних організацій ОРДЛО реалізуються за трьома основними напрямками:

– зрив мобілізації та призовних кампаній до лав ЗС України;

– компрометація діяльності органів державної влади та місцевого самоврядування;

– дискредитація правоохоронних органів та ЗС України.

Так, в соціальній мережі «ВКонтакте» створено спільноту «Житомирская народная республіка». В зазначеній групі розміщувалася інформація антиукраїнського спрямування на підтримку НЗФ в ОРДЛО, а також поширювалися відеоролики за участі бойовиків НЗФ.

Співробітниками СБ України в межах чинного законодавства було вжито необхідних заходів для блокування Інтернет-спільноти фейкової «ЖНР» та припинення її інформаційного наповнення [32].

– поширення (шляхом розсилання на офіційні електронні адреси українських державних установ) шкідливого програмного забезпечення, яке після інсталяції відправляє інформацію, що міститься на ПЕОМ, на сервери, розташовані на території Російської Федерації.

Зокрема, продовжують фіксуватися факти надсилання на офіційні електронні поштові адреси окремих державних та правоохоронних органів, а також військових формувань електронних листів, які містять шкідливі вкладення. Вказані листи надходили з фейкових адрес реальних державних установ.

В подальшому, з використанням спеціалізованого програмного забезпечення, здійснювалася декомпіляцію вкладення в електронний лист.

В результаті встановлено, що вищевказане вкладення спрямоване на отримання російською стороною прихованого доступу до інформації, яка розміщується на ПЕОМ користувача.

Більш детально вказане проблемне питання буде проаналізовано в 2 та 3 розділах роботи;

– спонукання з боку російських структур громадян України (в першу чергу учасників АТО) до працевлаштування на території РФ. Після цього фіксується створення компрометуючих ситуацій, направлених на вчинення ними кримінально-караних діянь (розбій, торгівля наркотичними засобами) з подальшим висвітленням вищевказаного в ЗМІ і позиціювання перед світовою спільнотою захисників України у якості злочинців-рецидивістів [19];

– підтримка самопроголошених «ДНР/ЛНР», автономістських рухів в різних регіонах України тощо.

1.2. Спеціальні підрозділи інформаційного впливу Російської Федерації

В березні 2021р. виповнилось сім роки з моменту анексії Російською Федерацією території АР Крим та розв'язання збройного конфлікту на сході України. На нашу думку, їх реалізація була б неможливою без підтримки військової агресії з боку місцевого населення, яка виникла внаслідок цілеспрямованого впливу на свідомість і підсвідомість громадян (насамперед молоді) та формування у них антигромадської позиції (недовіри до чинної влади, правоохоронних органів тощо), а також спонукання до вчинення актів непокори чи інших протиправних дій [45].

Під час Другої світової війни у збройних силах СРСР існували підрозділи, відповідальні за ведення контрпропаганди, які займалися виготовленням листівок та аудіомовленням, що повинні були впливати на психіку супротивника.

Про необхідність створення інформаційних військ у класичному вигляді в Росії почали говорити з часів конфлікту в Грузії у 2008 році. І це не дивно, адже на нашу думку, наслідки кібернетичної війни можуть бути не менш руйнівними, ніж ядерної. Зазначене обумовлено тим, що в наш час інформатизація впроваджена у всі сфери суспільного життя, а вплинути на стабільну роботу об'єктів критичної інфраструктури можливо з будь-якої точки земної кулі.

З розвитком новітніх технологій, в роботу спеціальних служб РФ почали активно впроваджуватися новітні розробки в інформаційній сфері. Так, з 2010р. у ФСБ РФ почало впроваджуватися програмне забезпечення для моніторингу соціальних мереж та електронних ЗМІ. На перших стадіях воно працювало лише з відкритою інформацією. За умови, якщо користувач обмежив доступ до особистої інформації за допомогою відповідних налаштувань, її неможливо було проаналізувати. Однак, з часом провайдерів зобов'язали встановити обладнання, яке дозволило співробітникам спеціальних служб контролювати веб-трафік (моніторити інформацію на

етапі її опублікування). Однак дані, розміщені на закордонних серверах, залишалися недоступними. Тому, найбільш вагомі соцмережі РФ (Mail.ru, «Одноклассники», «ВКонтакте») в 2012-2013рр. були поглинені бізнес-групами, власників яких російські ЗМІ пов'язують із вищим керівництвом вказаної держави.

У тому ж 2012р., у відповідності до офіційних даних, співробітники Служби зовнішньої розвідки РФ почали моніторити Інтернет - мережі з застосовуванням новітніх інформаційних технології. Так, ними було оголошено три закриті тендери на суму понад 30 мільйон рублів із задекларованою метою вироблення нових методик моніторингу блогосфери (дослідження з кодовими позначеннями «Шторм-12», «Монітор-3» і «Диспут»). Однак, на думку експертів, вже в той час існувала ймовірність використання розробок на отримання персональних даних користувачів в російських та іноземних соціальних мережах [29].

06.11.2012р. на посаду Міністра оборони РФ було призначено С. Шойгу. Відразу після призначення він почав активно лобіювати тематику «створення російських кібервійськ». При цьому, останній порівнював кібератаки зі зброєю масового ураження, за допомогою якої можна здобути будь-яку інформацію [30].

Врешті, у 2013р. в Міністерстві оборони (МО) РФ було прийнято офіційне рішення про необхідність створення кібервійськ [11]. Основні їх завдання полягатимуть у централізованому проведенні операцій кібервійни, управлінні і захисті військових комп'ютерних мереж Росії, захисті російських військових систем управління і зв'язку від кібертероризму та надійне закриття інформації, що обробляється у них, від ймовірного противника. Війська здійснюватимуть координацію та інтеграцію операцій, що проводяться кіберпідрозділами ЗС Росії, експертизу кібернетичного потенціалу Міноборони Росії та розширення можливості його дій в кібернетичному просторі.

14.01.2014р. С. Шойгу підписав наказ про створення в складі Генерального штабу ЗС Росії кібернетичного командування, основне завдання якого полягає в захисті від несанкціонованого втручання в електронні системи управління Росії [13].

Навесні 2014р. в Міноборони з'явилися «війська інформаційних операцій». Їх основним завданням стало кібернетичне протиборство з ймовірним противником та, відповідно, порушення належного функціонування його інформаційних мереж. До складу військ увійшли частини і підрозділи у військових округах та на флотах, укомплектовані висококваліфікованими фахівцями: математиками, програмістами, інженерами, криптографами, зв'язківцями, офіцерами радіоелектронної боротьби, перекладачами тощо [12].

При цьому, на базі відповідних профільних вищих навчальних закладів РФ почали посилено готувати відповідних фахівців. Так, у вересні 2015р. на базі Військової академії зв'язку РФ відкрилася кадетська школа ІТ-технологій, а в грудні цього ж року зазначений ВНЗ закінчили перші випускники наукової роти «спецназу інформаційної безпеки» [30].

22.02.2017р., виступаючи в Державній думі, міністр оборони РФ С. Шойгу офіційно відмітив, що в Збройних силах РФ створені війська інформаційних операцій [28], основним завданням яких став захист інтересів національної оборони РФ.

Вказана інформація стала першим прямим підтвердження з боку МО факту існування інформаційних військ на території РФ.

На думку екс-начальника Аналітичного управління КДБ СРСР В. Рубанова, їх чисельний склад може сягати тисячі осіб [10], а розмір фінансування становить близько $ 300 млн в рік. Щодо їх структури, то інформація є засекреченою. У відповідності до офіційних даних, розміщених на сайті МО РФ, в структурі відомства існує кілька підрозділів, в зону відповідальності яких можуть входити інформаційні операції. В першу чергу це Головне розвідувальне управління, Головне управління розвитку

інформаційних і телекомунікаційних технологій під керівництвом полковника Максима Беца, а також Управління прес-служби і інформації. Ймовірно, до вказаної діяльності причетна й 6-а наукова рота Восьмого управління Генштабу [31].

За оцінками аналітиків (експертів компанії Zecurion Analytics), станом на початок 2017р. за рівнем розвитку кібервійськ Росія входить у топ-5 держав світу після США, Китаю, Великобританії та Південної Кореї [28].

Аналізуючи відкриті джерела інформації, можливо прийти до висновку, що на офіційному рівні існування кібервійськ визнано лише частиною країн у світі (США, Ірак, Великобританія, РФ тощо), однак реально вони функціонують майже в кожній розвиненій державі. Зважаючи на викладене, беручи до уваги участь збройних сил РФ у збройному конфлікті на сході України, вважається, що першочергові зусилля вищого керівництва держави у вказаній сфері повинні бути спрямовані на формування в Україні професійних кібервійськ, в тому числі з використанням потенціалу волонтерських інформаційних груп (Cyberhunta, Inform Napalm та ін.).

1.3. Протидії сепаратизму в інформаційній сфері, як передумова реалізації євроінтеграційних процесів

Матеріали вказаного підрозділу роботи було обговорено в ході міжнародної науково-практичної конференції в м. Запоріжжя [42]. Зокрема, увагу присутніх було акцентовано на тому, що прихильники т.зв. «ДНР/ЛНР» активно використовують інформаційний простір з метою впливу на свідомість громадян, що проживають на тимчасово підконтрольній бойовикам території України, як у власному «медійному ресурсі», так і у засобах масової інформації Російської Федерації.

Зокрема, ними систематично поширюються тенденційні матеріали пропагандистського характеру. Основна тематика: негативна економічна ситуації в Україні, відсутність узгодженості в діяльності вищих органів державної влади, заборгованість із виплатою заробітної платні, «переддефолтний» стан економіки, непослідовність реформ, які проводяться в державі тощо. В якості експертів, які аналізують зазначені проблемні питання, запрошуються фахівців-економістів (з РФ і ті, що проживають на підконтрольних бойовиках територіях) та викладачі Донецьких «вищих учбових закладів».

Поряд з тим, вищевказаними суб’єктами, з метою прихованого психологічного, політичного, комерційного та фізичного примусу, викривлення сприйняття реальності в Інтернет-просторі широко застосовуються маніпулятивні технології. Серед способів та технологій, які використовуються з вищевказаною метою, виділяються наступні: пряме підтасовування фактів; замовчування невигідної інформації; упередженість інтерпретації фактів; надання сфальсифікованої інформації; навішування ярликів для компрометації політиків; використання групових інтересів та ін [50].

З метою доведення вигідної інформації до суспільства, перевага, як правило, надається електронним засобам масової інформації (Інтернет-

видання), які використовують новітні інформаційні технології для розповсюдження новин.

Окремою технологією маніпулювання можна виділити т.зв. маніпулювання на форумах.

Даний вид технології полягає в коментуванні, в т.ч. анонімному, тієї чи іншої проблематики та ситуації різними користувачами Інтернет-ресурсу, що є ознакою демократизму і плюралізму Інтернету. Водночас, зацікавлені особи можуть активно втручатися у форуми, коментуючи, начебто й неупереджено, ті чи ті події. Насправді ж «голос народу» виявляється звичайним пропагандистським засобом, іноді провокативним, але завжди дієвим, бо здається об'єктивним. Маніпулювання на Інтернет-форумах соціально шкідливе, оскільки розповсюдження неправдивої інформації дискредитує сам інститут громадської думки, робить його вразливим та недієздатним [24].

На думку фахівців, сепаратистами і в подальшому активно використовуватимуться інформаційні ресурси з метою впливу на свідомість громадян (в першу чергу молоді), які проживають на сході України (насамперед на територіях, підконтрольних «ДНР/ЛНР»), що негативно впливатиме на безпеку нашої держави на фоні відсутності на вищевказаних територіях повноцінної україномовної сітки мовлення.

Зважаючи на викладене, з метою протидії інформаційній агресії, фахівцями пропонується створення єдиного комунікаційного центру, аналогічного за функціями та завданнями структурного підрозділу НАТО.

У 2014р. в Латвії було створено Центр стратегічних комунікацій НАТО (NATO Strategic Communications Centre of Excellence), серед завдань якого – забезпечити адекватну відповідь на спроби інших країн вплинути на інформаційний простір членів НАТО. Центр має опікуватися питаннями «гібридної війни» [15].

Поряд з тим, ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної

співпраці волонтерів. Волонтерський рух в мережі Інтернет, як інструмент протидії інформаційній агресії або для здійснення аналогічних атак на інформаційне поле супротивника, став одним із засобів протидії російській агресії проти України.

Серед українських волонтерських проектів, які діють як допоміжні віртуальні ресурси в інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами, можливо виділити Inform Napalm та «Інформаційний спротив», центр «Миротворець». Зазначені мережеві проекти є яскравим прикладом того, як за допомогою належним чином розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та результативно супроводжувати офлайн-процеси.

Практично всі вище згадані проекти діють за схемою роботи так званої OSINT (Open Source Intelligence) - розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отриманої з відкритих джерел.

Важливою складовою такої роботи є системний аналіз наявної інформації з відповідною оцінкою та висновками, що дозволяють зрозуміти логіку та передбачити дії противника. Одним із базових правил такої практики є те, що близько 90% необхідної для аналізу та прийняття відповідних рішень інформації перебуває у відкритих джерелах.

До таких джерел відносять: традиційні ЗМІ (газети, журнали, радіо, телебачення); інтернет-видання, що відносяться до ЗМІ (новинні сайти та портали, інтернет-ресурси профільних структур); акаунти та віртуальні майданчики у соціальних мережах; офіційні звіти державних структур; публічні заяви політиків та держслужбовців; спостереження — радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth); професійні та академічні звіти, конференції, доповіді, статті; звіти та виступи в ЗМІ окремих незалежних експертів та експертних груп [22].

Окремим негативними моментом протидії інформаційній експансії є те, що чинні законодавчі акти у сфері інформаційної безпеки здебільшого

перебувають на стадії розробки або доопрацювання, внаслідок чого ускладнюється процедура правового реагування та впливу на діяльність суб'єктів інформаційного поля держави.

Так, відсутність низки законодавчо-закріплених понять у вказаній сфері негативно впливає на прийняття рішень слідчими при кваліфікації відповідних протиправних діянь.

Зокрема, диспозиція ст. 111 Кримінального кодексу України (далі КК України) передбачає відповідальність за діяння, умисно вчинене громадянином України, в т.ч. на шкоду інформаційній безпеці, хоча в національному законодавстві відсутнє тлумачення терміну «інформаційна безпека» (в окремих коментарях до ст.111 КК України також вживається поняття «інформаційної експансії»), що створює підґрунтя для правих маніпуляцій з боку зацікавлених сторін кримінального процесу (зазначений термін розуміється ними на власний розсуд через призму суб'єктивності) [42].

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

Отже, виходячи з викладеного вище, можна зробити наступні висновки до першого розділу роботи:

1. Основними є такі форми та методи ведення т.зв. «гібридної війни»:

– залучення осіб з «хакерського середовища» (відкрито та «під чужим прапором») до створення шкідливого програмного забезпечення, яке за певних умов після інсталяції на ПЕОМ може призвести до витоку службової інформації, яка на них обробляється;

– реалізація представниками спеціальних служб РФ інформаційних акцій, спрямованих на дискредитацію здійснюваних урядом України реформ та висвітлення в негативному ракурсі соціально-економічного становища в Україні;

– використання регіонального сегменту мережі Інтернет (насамперед соціальних мереж) представниками спеціальних служб РФ, а також підконтрольними їм бойовиками терористичних організацій «ДНР/ЛНР», для впливу на громадян України та формування у них антигромадської позиції, що набуло особливої актуальності на фоні ускладнення соціально-економічної та суспільно-політичної ситуації та погіршення рівня життя населення;

– поширення (шляхом розсилання на офіційні електронні адреси українських державних установ) шкідливого програмного забезпечення, яке після інсталяції відправляє інформацію, що міститься на ПЕОМ, на сервери, розташовані на території Російської Федерації;

– спонукання з боку російських структур громадян України (в першу чергу учасників АТО) до працевлаштування на території РФ. Після цього фіксується створення компрометуючих ситуацій, направлених на вчинення ними кримінально-караних діянь (розбій, торгівля наркотичними засобами) з подальшим висвітленням вищевказаного в ЗМІ і позиціювання перед світовою спільнотою захисників України у якості злочинців-рецидивістів;

– підтримка самопроголошених «ДНР/ЛНР», автономістських рухів в різних регіонах України тощо.

2. Про необхідність створення інформаційних військ у класичному вигляді в РФ почали говорити з часів конфлікту в Грузії у 2008 році. З розвитком новітніх технологій, в роботу спеціальних служб РФ почали активно впроваджуватися новітні розробки в інформаційній сфері. Так, з 2010р. у ФСБ РФ почало впроваджуватися програмне забезпечення для моніторингу соціальних мереж та електронних ЗМІ. У 2012р., у відповідності до офіційних даних, співробітники Служби зовнішньої розвідки РФ почали моніторити Інтернет - мережі з застосовуванням новітніх інформаційних технології. У 2013р. в Міністерстві оборони (МО) РФ було прийнято офіційне рішення про необхідність створення кібервійськ.

3. З метою реалізації євроінтеграційних процесів, вважається, що протидію сепаратизму в інформаційній сфері повинен забезпечувати та координувати єдиний комунікаційний центр, аналогічний за функціями та завданнями відповідним структурним підрозділам НАТО.

РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА СТРАТЕГІЧНО ВАЖЛИВИХ ОБ'ЄКТАХ

2.1. Використання програм віддаленого доступу, як одна із загроз національній безпеці України

Аналіз поширених у засобам масової інформації даних свідчить про стрімке зростання кількості фактів несанкціонованого втручання в сталу роботу офіційних веб-ресурсів органів державної влади та органів місцевого самоврядування [18], об'єктів критичної інфраструктури [21], правоохоронних органів [23] тощо, що призводить до спотворення процесу обробки інформації, її несанкціонованої маршрутизації та, можливо, використання в протиправних цілях (в тому числі й на шкоду національній безпеці України).

На нашу думку, вищевказане обумовлено як об'єктивними (відсутність належного фінансування, застарілість обладнання та програмного забезпечення тощо), так і суб'єктивними чинниками (призначення на посади осіб, відповідальних за технічну безпеку, без досвіду роботи та належного фахового рівня, нехтування положеннями чинних нормативно-правових актів у інформаційній сфері тощо).

Зазначені фактори призводять до того, що, подекуди, відповідальні особи, в першу чергу, органів влади та управління, а також об'єктів критичної інфраструктури звертаються за допомогою для оптимізації роботи ПЕОМ, налаштування відповідних програмних продуктів тощо до сторонніх суб'єктів, як здійснюють вказані дії як безпосередньо у відповідних службових приміщеннях, так і шляхом віддаленої підтримки (використовуючи можливості програм віддаленого доступу («TeamViewer», «AnyDesk», «Microsoft Remote Desktop» тощо)).

Однак, вказані дії суперечать положенням діючих нормативно-правових актів у частині обов'язкової автентифікації та ідентифікації

користувача, захисту інформації, яка належить до державних інформаційних ресурсів, характеризує діяльність суб'єктів владних повноважень, військових формувань та оприлюднюється в мережі Інтернет, або передається через телекомунікаційні мережі.

Відповідно до ст. 5 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затверджених постановою Кабінету Міністрів України від 29.03.2006 №373 (далі Правила): «Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Автентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора; ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою» [26].

Водночас, відповідно до ст. 4 Правил, захисту в системі підлягає: «…відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами» [26].

Тобто, у разі використання можливостей зазначених програм, сторонні особи отримують віддалений доступ до інформаційної системи органів державної влади чи об'єктів критичної інфраструктури, усього масиву даних, який знаходиться на ПЕОМ, з можливістю її зміни та модифікації.

За свідченням фахівців, на увагу заслуговує той факт, що вказані програмні продукти розробляються на території іноземних держав або ж іноземні спеціальні служби (в т.ч. й РФ), зважаючи на норми власного національного законодавства, мають доступ до відповідних масивів даних.

Так, на прикладі дослідження роботи програмного забезпечення «TeamViewer» нами було встановлено, що Інтернет-, Хостинг провайдери та Data-центри, які залучені до маршрутизації та роботи згаданого софту частину серверів розміщують на території Російської Федерації.

Таким чином, аналіз вказаної інформації дає можливість стверджувати, що вся діяльність Інтернет-, Хостинг-провайдерів та Data-центрів на території РФ ліцензується та регулюється ФСБ, яка має безперешкодний доступ до інформації, що циркулює в них. З урахування непоодиноких випадків використання в органах державної влади та місцевого самоврядування, на об’єктах критичної інфраструктури України програмного забезпечення для віддаленого доступу, існує реальна можливість з боку спецслужб РФ отримати доступ до інформації, яка циркулює у інформаційних системах зазначених об’єктів з подальшим її використанням в протиправних цілях.

З урахуванням викладеного, з метою належного захисту офіційних електронних ресурсів органів державної влади та органів місцевого самоврядування регіону, унеможливлення спотворення процесу обробки інформації, її несанкціонованої маршрутизації та ймовірного використання в протиправних цілях співробітниками спеціальних служб країни-агресора, вважається за доцільне на рівні Кабінету Міністрів України закріпити виключний перелік програмних засобів, які дозволено інсталювати на відповідні службові ПЕОМ.

2.2. Механізми поширення шкідливого програмного забезпечення на об’єктах критичної інфраструктури, органах державної влади та місцевого самоврядування

Матеріали вказаного підрозділу роботи було обговорено в ході постійно діючого науково-практичного семінару в м. Харкові [48]. Зокрема, увагу присутніх було акцентовано на тому, що аналіз забезпечення безпеки інформаційного простору України свідчить про активне залучення іноземних фахівців галузі ІТ-технологій, зокрема РФ, спецслужбами іноземних країн до здійснення актів кіберагресії проти України з використанням спеціального програмного забезпечення шкідливої дії (далі ШПЗ).

Вказані спеціалісти залучаються до розробки програмного забезпечення, призначеного для отримання інформації, яка передається відкритими каналами зв’язку з використанням комунікативних можливостей електронних поштових сервісів, а також побудови дієвої системи їх розповсюдження, збереження масиву отриманих даних.

Фіксуються спроби втручання в роботу ПЕОМ працівників органів державної влади і місцевого самоврядування шляхом розповсюдження вірусного програмного забезпечення через електронні поштові сервіси.

За результатами узагальнення отриманої нами інформації можливо прийти до висновку про те, в умовах ведення т.зв. «гібридної війни» акти кіберагресії, в переважній більшості, спрямовані на державний сектор (органи державної влади та місцевого самоврядування, правоохоронного блоку тощо).

В результаті вказаних маніпуляцій (розсилка шкідливого ШПЗ) встановлюється доступ до поштових скриньок, інформації, яка надсилається та отримується поштовим сервісом, та прихований доступ до ПЕОМ, на якому було інстальовано шкідливе програмне забезпечення, що, в свою чергу, може призвести до витоку службової інформації, персональних даних тощо.

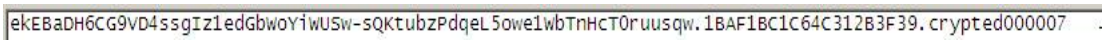
Крім того, використання в ході підготовки вказаної розсилки реальних даних співробітників правоохоронних органів може свідчити про отримання представниками хакерських угруповань або іноспецслужб доступу до окремих інформаційних ресурсів правоохоронних та державних органів.

Також, фіксується поширення через електронні засоби комунікації шкідливого програмного забезпечення - шифрувальника «Troldesh/Shade».

З початку 2019р. відмічається масова розсилка на електронні адреси державних органів та установ регіону електронних листів нібито від імені фінансових установ із вкладеннями у вигляді архіву «info.zip».

У вказаному архів наявний файл «Інформація.js» або інший файл з розширенням «.js». У разі запуску останнього, на ПЕОМ починає працювати алгоритм «javascript» (полягає у використанні різного роду алгоритмів шифрування, які використовується при кодуванні назви файлів і даних, та інформації, яка перебуває на ураженій машині), який при виконанні завантажує файл «ssj.jpg» у тимчасову директорію. При цьому, прикріплений архів «info.zip» може бути потрійним, тобто «info.zip» -> «info.zip» -> «inf.zip» -> «Інформація.js».

У разі шифрування файли отримують нове розширення «.crypted000007».



В кожній директорії з кодованими файлами створюється файл “readme” з реквізитами щодо оплати для їх подальшого розблокування.

Після завершення шифрування на моніторі ПЕОМ відкривається повідомлення російською та англійською мовами.

У тому випадку, коли уражена ПЕОМ під’єднана до цілісної мережі, шкідливе програмне забезпечення інсталюється й на інші комп’ютери (використовуючи SMB протокол). При цьому, окрім фізичного блокування (шифрування) інформації, у зловмисників, за певних умов, може з’явитися можливість віддаленої маршрутизації даних.

Наразі відсутні ефективні способи боротьби з вищезазначеними проявами кіберагресії, оскільки впровадження шкідливого програмного забезпечення на ПЕОМ залежить виключно від особистої компетентності конкретного користувача («людський фактор»).

На нашу думку, відсутність дієвих заходів протидій, окрім іншого, пов’язана і з наявністю колізійних норм в чинному законодавстві, яке регулює суспільні відносини у вказаній сфері та визначає винність діянь [48].

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

Виходячи з викладеного вище, можна зробити наступні висновки до другого розділу роботи:

1. Як свідчить практика, подекуди, відповідальні особи, в першу чергу, органів влади та управління, а також об’єктів критичної інфраструктури звертаються за допомогою для оптимізації роботи ПЕОМ, налаштування відповідних програмних продуктів тощо до сторонніх суб’єктів, як здійснюють вказані дії як безпосередньо у відповідних службових приміщеннях, так і шляхом віддаленої підтримки (використовуючи можливості програм віддаленого доступу («TeamViewer», «AnyDesk», «Microsoft Remote Desktop» тощо)).

Однак, вказані дії суперечать положенням діючих нормативно-правових актів у частині обов’язкової автентифікації та ідентифікації користувача, захисту інформації, яка належить до державних інформаційних ресурсів, характеризує діяльність суб’єктів владних повноважень, військових формувань та оприлюднюється в мережі Інтернет, або передається через телекомунікаційні мережі.

2. Фіксується системне залучення співробітниками спецслужб іноземних країн (в першу чергу РФ), фахівців ІТ-галузі до здійснення актів кіберагресії проти України з використанням спеціального програмного забезпечення шкідливої дії.

Вказані спеціалісти залучаються до розробки програмного забезпечення, призначеного для отримання інформації, яка передається відкритими каналами зв’язку з використанням комунікативних можливостей. Зокрема, документуються намагання втрутитися в сталу роботу ПЕОМ органів державної влади і місцевого самоврядування, об’єктів критичної інфраструктури, правоохоронних органів тощо шляхом поширення шкідливого програмного забезпечення за допомогою електронних поштових сервісів.

РОЗДІЛ 3. ОРГАНІЗАЦІЙНІ ОСНОВИ ПРОТИДІЇ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ В УКРАЇНІ: ШЛЯХИ УДОСКОНАЛЕННЯ

3.1. Шляхи протидії маніпулюванню громадською думкою з використанням засобів масової інформації.

Реалії сьогодення свідчать про сталі намагання функціонерів іноземних неурядових організацій використати окремих українських журналістів та правозахисників для поширення тенденційної інформації щодо суспільно-політичних процесів, які відбуваються в Україні, у тому числі й можливого кримінального переслідування владою політичних опонентів, з метою її подальшого доведення до світової спільноти та формування негативного імідж України.

Зокрема, в ході протидії військово-політичній агресії РФ та висвітлення в засобах масової інформації (далі – ЗМІ) результатів діяльності правоохоронної системи з протидії злочинам проти основ національної безпеки України, насамперед із боку пособників незаконних воєнізованих формувань ОРДЛО та спеціальних служб Російської Федерації, суттєво активізується діяльність окремих груп та осіб, спрямована на надання політичного забарвлення виявленим кримінально-караним проявам та їх подальшого використання для здійснення інформаційного впливу на судову систему та органи влади України. За ініціативи та фінансової підтримки окремих іноземних неурядових організацій, у т.ч. проросійського спрямування, ініціюються обговорення зазначених питань на засіданнях впливових міжнародних структур, насамперед Європейського парламенту та Ради Європи.

Водночас, фіксуються спроби використати конфліктні питання в інформаційній сфері для підготовки матеріалів деструктивного характеру, які

в подальшому використовуються при проведенні іноземною стороною спеціальних інформаційних операцій проти України.

Слід відзначити, що фінансова підтримка іноземних неурядових структур діяльності українських журналістів, насамперед спрямованої на тенденційне висвітлення суспільно-політичної ситуації в Україні, дає можливість останнім не лише отримати додаткові заробітки у вигляді грантів, а і підвищити власні рейтинги за рахунок виходу на міжнародний рівень.

Окремі українські журналісти, намагаючись отримати вищі рейтинги та значні заробітки, виконуючи замовлення іноземної сторони, не завжди усвідомлюють можливість настання негативних наслідків, які несуть загрозу національним інтересам України. Зазначене створює реальні передумови до використання останніх іноземними спецслужбами для проведення підривної діяльності проти нашої держави.

На нашу думку, відсутність ефективної державної підтримки українських засобів масової інформації збільшує кількість журналістів, негативно настроєних до чинної влади України, а також бажаючих отримати світове визнання та додаткові джерела доходів, сприяє їх потраплянню в поле зору іноземних неурядових структур, у т.ч. ймовірно підконтрольних іноземним спеціальним службам, та створює реальні передумови для їх використання на шкоду національній безпеці України.

У зв’язку з цим, іноземною стороною, шляхом втягування журналістів та «правозахисників» у фінансову залежність (гранти, можливість публікуватися у міжнародних виданнях тощо), здійснюється діяльність, спрямована на використання представників українських мас-медіа для збору тенденційної інформації з метою її подальшого оприлюднення в світовому інформаційному просторі. Зазначене негативно відображається на міжнародному іміджі України та створює додаткові важелі впливу на органи влади держави.

3.2. Оптимізації механізму блокування сепаратистських інтернет-ресурсів, як одна із складових забезпечення національної безпеки України в інформаційній сфері

В XXI столітті, зважаючи на розвиток телекомунікаційних систем, все більше часу люди проводять у «віртуальному світі». Щоденно мільйони користувачів викладають інформацію (в тому числі й персонального характеру), яку в будь-який проміжок часу можливо використати проти них, або ж навіть, за певних умов, на шкоду державним інтересам. Значної актуальності для України вказане питання набуло в умовах сьогодення - фактичного перебування у стані «гібридної війни».

Протягом минулих років на рівні керівництва держави було прийнято ряд нормативно-правових актів, спрямованих на обмеження вільного доступу громадян до електронних ресурсів, які використовуються для антиукраїнської діяльності та адмініструються з території Російської Федерації (РФ). В першу чергу вищевказане стосується соціальних мереж «ВКонтакте» та «Одноклассники».

Дійсно, вищевказані заходи були на часі. Адже, у відповідності до офіційної статистики, Vk.com. займав третє місце у рейтингу ТОП 15 сайтів з найбільшою аудиторією в Україні (соцмережа № 1 за поширенням в Україні), а «Одноклассники» (ok.ru) – десяте (третє місце серед соціальних мереж після Facebook.com). В цілому, у вказаному ТОПі було розташовано 4 електронних Інтернет-ресурсів, які мають пряме чи опосередковане відношення до РФ (окрім зазначених: Yandex.ua – 5 та Mail.ru. – 6 місця) [37].

При цьому, у відповідності до офіційної статистики СБ України, в соціальних мережах, які адмініструвалися з території РФ, було зареєстровано і активно діяло на шкоду національним інтересам близько 800 антиукраїнських груп [33].

Співробітниками СБ України було припинено протиправну діяльність адміністраторів, які підтримували антиукраїнські спільноти у заборонених в

Україні соціальних мережах «Вконтакте» та «Одноклассники» і здійснювали свою протиправну діяльність на територіях Київської, Львівської, Черкаської, Хмельницької, Харківської, Чернігівської, Івано-Франківської, Дніпропетровської та Сумської областей. Ними було створено десятки веб-сторінок та спільнот у соцмережах, де активно поширювалися сепаратистські матеріали. Зокрема, публікувалися антидержавницькі заклики спрямовані на повалення конституційного ладу та порушення територіальної цілісності.

Загалом протягом трьох років Службою безпеки зареєстровано 72 кримінальні провадження, за матеріалами досудових розслідувань слідчих СБ України винесено понад 60 вироків особам, які здійснювали антиукраїнську пропаганду в російських соцмережах. Оперативники спецслужби також припинили функціонування 70 Інтернет-спільнот фейкових псевдонародних «республік» у різних регіонах України [33].

Однак, як свідчать реалії сьогодення, переважна кількість користувачів з метою обходу блокування використовують VPN-сервіси (віртуальні персональні мережі) та анонімайзери. Вищевказані програмні засоби замінюють геолокацію користувача.

За різними оцінками, 20-30% користувачів «Яндекса», «ВКонтакте», «Одноклассники» і Mail.ru встановили собі зазначені сервіси (насамперед на мобільних пристроях).

Виходячи з положень чинного законодавства, пересічні громадяни не вчиняють жодного протиправного діяння. Вищевказане обумовлено тим, що положеннями відповідних нормативно-правових актів передбачено обов’язок провайдерам забезпечити блокування доступу користувачів (абонентів) до ресурсів/сервісів, що належать групам компаній «Яндекс» та «Mail.Ru Group» тощо.

Однак, на нашу думку, окрім правового аспекту є й інші. Зокрема, в першу чергу вищевказане стосується використання інструментів обходу блокування російських сервісів працівниками органів державної влади та

місцевого самоврядування, військовослужбовцями в районі проведення АТО тощо.

Останні, зважаючи на специфіку функціонування протоколу VPN та аномінайзерів (підміняють реальний IP на закордонний), свідомо чи несвідомо відкривають доступ до особистої інформації. В тому числі й для ІТ-фахіців – співробітників спеціальних служб РФ.

Адже, в той час, коли відбувається під'єднання пристрою (мобільного терміналу, ноутбука тощо) до домашньої, корпоративної чи службової (державної) мережі, останній продовжує зашифроване з'єднання з VPN-сервером, відправляючи на нього дані про користувача та мережу. Зважаючи на технічні характеристики, пристрої мають змогу накопичувати інформацію про локальну мережу та відправляти її будь-куди, в тому числі з використанням камери чи мікрофону.

У ЗМІ та Інтернет-мережі неодноразово фіксувалися випадки поширення відомостей щодо дислокації, розгортання та переміщення підрозділів Збройних Сил України та інших правоохоронних органів, стану бойової та мобілізаційної готовності; технічного стану військових засобів ураження, військової та спеціальної техніки; рівня матеріального забезпечення та морально-психологічного стану військовослужбовців та співробітників правоохоронних органів; специфіки виконання робіт підприємствами оборонно-промислового комплексу по розробці, виготовленню, ремонту та модернізації озброєнь та військової техніки тощо та іншої інформації, яка ставить під загрозу успішне проведення антитерористичної операції на сході України. Також, доволі часто військовослужбовці розміщують у соціальних мережах свої особисті фото з району проведення АТО, зроблені на фоні місцевості, в якій дислокується підрозділ.

На увагу заслуговує той факт, що після того, як українські провайдери почали блокувати окремі інтернет-ресурси, спецслужби різних країн, зокрема

й РФ, стали поширювати в мережі Інтернеті власні VPN-сервери, таким чином отримуючи доступ до необхідної їм інформації.

До небезпечних браузерів телеком-експерти віднесли яндекс.браузер, новий браузер FreeU (створений ФСБ), підозри повинні викликати також будь-які нові сервіси, які тільки вийшли на український ринок [38].

Зазначене, окрім можливого несанкціонованого доступу до відомостей, що становлять державну чи службову таємницю (дислокація підрозділів, кількісний чи якісний склад, наявність на озброєнні військових засобів ураження тощо), як свідчать реалії сьогодення, призводить, на жаль, і до більш негативних наслідків – загибелі особового складу на сході України [40].

Вводячи персональні спеціальні економічні та обмежувальні заходи (санкції), керівництво держави переслідувало мету обмежити вплив на свідомість і підсвідомість громадян України (в першу чергу молоді). Однак, проаналізувавши динаміку використання російських соціальних мереж «ВКонтакте» та «Одноклассники», можливо визнати, що вона залишається досить сталою.

На думку фахівців у сфері кібербезпеки, досить важко знайти особу, «яка перестала б заходити в російські соціальні мережі тільки тому, що вона не вміє цього робити. Таких, мабуть, немає. Школярі за 3 секунди навчились це робити» [14].

При цьому, відмічаються тенденції до перереєстрації та створення нових сепаратистських спільнот в соціальній мережі «Facebook».

Вищевказане обумовлено тим, що за даними компанії «Gemius», тижнева українська аудиторія мережі Facebook до заборони російських ресурсів становила 5,3 мільйона користувачів, а після блокування зросла на 2,2 мільйона [20].

На нашу думку є декілька шляхів вирішення окресленого проблемного питання:

– удосконалення системи заходів правового регулювання доступу до персональної інформації в соціальних мережах шляхом чіткої регламентації права та обов'язків власників, адміністрації та технічного персоналу соціальних мереж, які функціонують на території України, щодо використання, зберігання та захисту персональної інформації;

– проведення відповідної роз'яснювальної роботи серед пересічних користувачів, насамперед молоді;

– залучення до розробки систем захисту персональних даних, відповідного програмного забезпечення вітчизняних ІТ фахівців;

– вироблення єдиного підходу до формування і закріплення на відповідному рівні обмежень щодо використання соціальних мереж деякими спеціальними категоріями громадян (військовослужбовці, співробітники правоохоронних органів тощо) [45].

Поряд з тим, зважаючи на необхідність організації дієвої протидії всім формам гібридної війни, які реалізуються спеціальними службами РФ на території України, в тому числі й в інформаційній сфері, не потрібно повністю відхиляти можливість повної заборони (хоча б на час проведення операції Об'єднаних сил) використання громадянами протоколів VPN та можливостей анонімайзерів.

Вказаним шляхом, наприклад, пішла країна-агресор – РФ, прийнявши закон про блокування VPN і анонімайзерів, які не забезпечують обмеження доступу до сторінок з реєстру сайтів, які заборонив Роскомнадзор.

Також, аналогічний механізм впроваджено на території Китайської Народної Республіки. У вказаній країні, сегмент Інтернету повністю відокремлений від «зовнішнього» світу. Наявний єдиний канал зв'язку, який контролюється урядом (Великий китайський файрвол).

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

1. З метою мінімізації негативного впливу на інформаційній простір України, недопущення використання іноземною стороною представників українських ЗМІ та правозахисних структур для проведення інформаційної війни проти нашої держави, на нашу думку доцільно запровадити програму підтримки українських друкованих та електронних засобів масової інформації, що дасть можливість зменшити ризики використання журналістського середовища іноземною стороною, а також сприятиме запровадженню державного регулювання в інформаційній сфері. Поряд з тим, запровадити механізм нормативно-правового регулювання діяльності т.зв. електронних засобів масової інформації (на даний час відсутнє законодавче визначення, а також умови їх діяльності в українському сегменті Інтернет простору), насамперед інформаційних Інтернет-ресурсів (сайти новин, портали, спільноти тощо), а також співпраці вказаних ЗМІ в цілому та українських журналістів зокрема з іноземними неурядовими та державними структурами.

2. З метою мінімізації негативного впливу в Інтернет мережі необхідно вжити заходів направлених на:

– удосконалення системи заходів правового регулювання доступу до персональної інформації в соціальних мережах шляхом чіткої регламентації права та обов’язків власників, адміністрації та технічного персоналу соціальних мереж, які функціонують на території України, щодо використання, зберігання та захисту персональної інформації;

– проведення відповідної роз’яснювальної роботи серед пересічних користувачів, насамперед молоді;

– залучення до розробки систем захисту персональних даних, відповідного програмного забезпечення вітчизняних ІТ фахівців тощо.

ВИСНОВКИ

Відповідно до мети та поставлених завдань у даній роботі було: визначено та охарактеризовано форми та методи ведення представниками спеціальних служб Російської Федерації «гібридної війни» в інформаційній сфері; проаналізовано діяльність спеціальних підрозділів інформаційного впливу Російської Федерації; досліджено процес протидії сепаратизму в інформаційній сфері, як передумови реалізації євроінтеграційних процесів; проаналізовано використання програм віддаленого доступу, як загроз національній безпеці України; охарактеризовано механізми поширення шкідливого програмного забезпечення на об'єктах критичної інфраструктури, органах державної влади та місцевого самоврядування; визначено шляхи протидії маніпулюванню громадською думкою з використанням засобів масової інформації та Інтернет мережі; розроблено для зацікавлених суб'єктів конкретні пропозиції спрямовані на забезпечення інформаційної безпеки держави в умовах проведення операції Об'єднаних сил та «гібридної війни».

На підставі критичного аналізу зроблено наступні висновки:

1. Основними є такі форми та методи ведення т.зв. «гібридної війни»:

– залучення осіб з «хакерського середовища» (відкрито та «під чужим прапором») до створення шкідливого програмного забезпечення, яке за певних умов після інсталяції на ПЕОМ може призвести до витоку службової інформації, яка на них обробляється;

– реалізація представниками спеціальних служб РФ інформаційних акцій, спрямованих на дискредитацію здійснюваних урядом України реформ та висвітлення в негативному ракурсі соціально-економічного становища в Україні;

– використання регіонального сегменту мережі Інтернет (насамперед соціальних мереж) представниками спеціальних служб РФ, а також підконтрольними їм бойовиками терористичних організацій «ДНР/ЛНР», для впливу на громадян України та формування у них антигромадської позиції,

що набуло особливої актуальності на фоні ускладнення соціально-економічної та суспільно-політичної ситуації та погіршення рівня життя населення;

– поширення (шляхом розсилання на офіційні електронні адреси українських державних установ) шкідливого програмного забезпечення, яке після інсталяції відправляє інформацію, що міститься на ПЕОМ, на сервери, розташовані на території Російської Федерації;

– спонукання з боку російських структур громадян України (в першу чергу учасників АТО) до працевлаштування на території РФ. Після цього фіксується створення компрометуючих ситуацій, направлених на вчинення ними кримінально-караних діянь (розбій, торгівля наркотичними засобами) з подальшим висвітленням вищевказаного в ЗМІ і позиціювання перед світовою спільнотою захисників України у якості злочинців-рецидивістів;

– підтримка самопроголошених «ДНР/ЛНР», автономістських рухів в різних регіонах України тощо.

2. Про необхідність створення інформаційних військ у класичному вигляді в РФ почали говорити з часів конфлікту в Грузії у 2008 році. З розвитком новітніх технологій, в роботу спеціальних служб РФ почали активно впроваджуватися новітні розробки в інформаційній сфері. Так, з 2010р. у ФСБ РФ почало впроваджуватися програмне забезпечення для моніторингу соціальних мереж та електронних ЗМІ. У 2012р., у відповідності до офіційних даних, співробітники Служби зовнішньої розвідки РФ почали моніторити Інтернет - мережі з застосовуванням новітніх інформаційних технології. У 2013р. в Міністерстві оборони (МО) РФ було прийнято офіційне рішення про необхідність створення кібервійськ.

3. З метою реалізації євроінтеграційних процесів, вважається, що протидію сепаратизму в інформаційній сфері повинен забезпечувати та координувати єдиний комунікаційний центр, аналогічний за функціями та завданнями відповідним структурним підрозділам НАТО.

4. Як свідчить практика, подекуди, відповідальні особи, в першу чергу, органів влади та управління, а також об’єктів критичної інфраструктури звертаються за допомогою для оптимізації роботи ПЕОМ, налаштування відповідних програмних продуктів тощо до сторонніх суб’єктів, як здійснюють вказані дії як безпосередньо у відповідних службових приміщеннях, так і шляхом віддаленої підтримки (використовуючи можливості програм віддаленого доступу («TeamViewer», «AnyDesk», «Microsoft Remote Desktop» тощо)).

Однак, вказані дії суперечать положенням діючих нормативно-правових актів у частині обов’язкової автентифікації та ідентифікації користувача, захисту інформації, яка належить до державних інформаційних ресурсів, характеризує діяльність суб’єктів владних повноважень, військових формувань та оприлюднюється в мережі Інтернет, або передається через телекомунікаційні мережі.

5. Фіксується системне залучення співробітниками спецслужб іноземних країн (в першу чергу РФ), фахівців ІТ-галузі до здійснення актів кіберагресії проти України з використанням спеціального програмного забезпечення шкідливої дії.

Вказані спеціалісти залучаються до розробки програмного забезпечення, призначеного для отримання інформації, яка передається відкритими каналами зв’язку з використанням комунікативних можливостей. Зокрема, документуються намагання втрутитися в сталу роботу ПЕОМ органів державної влади і місцевого самоврядування, об’єктів критичної інфраструктури, правоохоронних органів тощо шляхом поширення шкідливого програмного забезпечення за допомогою електронних поштових сервісів.

6. З метою мінімізації негативного впливу на інформаційній простір України, недопущення використання іноземною стороною представників українських ЗМІ та правозахисних структур для проведення інформаційної війни проти нашої держави, на нашу думку доцільно запровадити програму

підтримки українських друкованих та електронних засобів масової інформації, що дасть можливість зменшити ризики використання журналістського середовища іноземною стороною, а також сприятиме запровадженню державного регулювання в інформаційній сфері. Поряд з тим, запровадити механізм нормативно-правового регулювання діяльності т.зв. електронних засобів масової інформації (на даний час відсутнє законодавче визначення, а також умови їх діяльності в українському сегменті Інтернет простору), насамперед інформаційних Інтернет-ресурсів (сайти новин, портали, спільноти тощо), а також співпраці вказаних ЗМІ в цілому та українських журналістів зокрема з іноземними неурядовими та державними структурами.

Також потребують вдосконалення заходи правового регулювання механізму доступу до персональної інформації в соціальних мережах. Зокрема, необхідна чітка регламентація права та обов'язків власників та персоналу соціальних мереж, які зберігають персональні дані українців України, щодо алгоритмів роботи із зазначеними масивами даних;

7. Зважаючи на посилення російською стороною активності в напрямку реалізації механізму здійснення деструктивного впливу на інформаційний простір держави, в т.ч. із використанням відповідних тематичних соціальних спільнот, вважається за доцільне вжити ряд наступних упереджувальних заходів:

– на законодавчому рівні врегулювати питання щодо фактичного, а не формального закриття чи обмеження доступу громадян до розміщених за кордоном веб-ресурсів, які містять інформацію, заборонену законодавством України. Поряд з тим, необхідно розробити зміни до чинних нормативно-правових актів, якими регламентуються правовідносини в інформаційній сфері, з метою усунення наявних у національному законодавстві правових колізій;

– з використанням можливостей Міністерства культури та інформаційної політики забезпечити ефективне проведення

контрпропагандистських заходів, спрямованих на нівелювання можливих негативних наслідків деструктивної діяльності країни-агресора в кіберпросторі;

– вдосконалити нормативно-правове забезпечення у сфері інформаційної безпеки, у т.ч. шляхом внесення змін до статей 111 і 258^3 КК України (розширення поняття підривної діяльності доповненнями, що охоплюють сферу інформаційної діяльності (Інтернет, ЗМІ, соцмережі, галузь інформатизації тощо) та виокремлення інформаційного сприяння терористичній діяльності), що дозволить виробити єдиний підхід до кваліфікації злочинів у вищевказаній сфері, а також ефективно протидіяти намаганням іноземних спецслужб, організацій, окремих груп та осіб використовувати громадян України для створення важелів інформаційного тиску на нашу державу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. «Лабораторія Касперського» надала звіт про групу, яка створила експлоіт кит angler. URL: https://xakep.ru/2016/08/31/all-about-lurk/.

2. Hunger in conflict zones continues to intensify. URL: http://www.fao.org/news/story/en/item/1099260/icode/.

3. Roman Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval, Olha S. Paramonova. Development of Internet communication and social networking in modern conditions: institutional and legal aspects. *Revista San Gregorio* (special issues Nov). Url: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/;

4. Roman F. Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval and Olha S. Paramonova. Formation and application of communication strategies through social networks: legal and organizational aspects. *International Journal of Management*. Volume 11. Issue 06. June 2020. pp. 476-488. Article ID: IJM_11_06_041 Available online at http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=11&IType=6 Journal Impact Factor (2020): 10.1471 (Calculated by GISI) www.jifactor.com. ISSN Print: 0976-6502 and ISSN Online: 0976-6510. DOI: 10.34218/IJM.11.6.2020.041;

5. Sviatun Olena, Goncharuk Olga, Roman Chernysh, Kuzmenko Olena, Kozych Ihor. Combating cybercrime: economic and legal aspects. *International Journal of Supply and Operations Management* (IJSOM), Special issues, February 2021.

6. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. К. : Видавничий дім «СофтПрес», 2005. 316 с.

7. Бєляков К. Інформатизація організаційно-правової сфери суспільної діяльності. *Право України*. 2004. № 6. С. 88-92.

8. Бондаренко В.О. Інформаційні впливи і операції. *Стратег. панорама*. 1999. № 4. С. 134-140.

9. Брижко В.М., Щвець М.Я., Цимбалюк В.С. Е – боротьба в інформаційних війнах та інформаційне право: Монографія. 2007 р. 234 с.

10. Бывший начальник Аналитического управления КГБ СССР Владимир Рубанов — об угрозах мнимых и реальных. URL: http://kyrgyztoday.org/ru/news_ru/byvshij-nachalnik-analiticheskogo-upravleniya-kgb-sssr-vladimir-rubanov-ob-ugrozah-mnimyh-i-realnyh/.

11. В 2013 году России появятся свои кибервойска. URL: https://rg.ru/2013/07/05/cyberwar-site-anons.html.

12. В Вооруженных силах РФ созданы войска информационных операций. URL: https://www.opentown.org/news/44318/.

13. В России появятся кибернетические войска. URL: http://mirnov.ru/obshchestvo/v-rossii-pojavjatsja-kiberneticheskie-voiska.html.

14. Війна онлайн: у чому полягає небезпека обходу блокування російських соцмереж. URL: http://24tv.ua/viyna_onlayn_u_chomu_polyagaye_nebezpeka_obhodu_blokuvannya_rosiyskih_sotsmerezh_n849627.

15. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. URL: http://gazeta.dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html.

16. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: моногр. / НАПрН України, НДІІП. Київ: Видавничий дім «АртЕк», 2017. 107 с. Розділи 3, 4. С. 45-103.

17. Доронін І.М. Національна безпека України в інформаційну епоху: правові аспекти: моногр. Київ: ТОВ Видавничий дім «АртЕк», 2019. 434 с.

18. Експерт розповів, як уникнути повторення кібератак на сайти держустанов. URL: https://www.unian.ua/science/kiberataki-v-ukrajini-hakerski-ataki-na-derzhavni-sayti-novini-11158679.html.

19. Житомирян, заохочуючи високою зарплатою, завербували в наркоторгівлю в Росії (ВІДЕО). URL:

http://zhitomir.today/news/society/zhitomiryan_zaohochuyuchi_visokoyu_zarplatoyu_zaverbuvali_v_narkotorgivlyu_v_rosiyi_video-id21811.html.

20. Життя без «Вконтакте»: наскільки безпечне «VPN-з'єднання». URL: https://ar.volyn.ua/2017/06/16/kantaktik-vso-paka/.

21. Кібератака**.** URL: https://www.ukrinform.ua/tag-kiberataka.

22. Курбан О. Гібридна війна: сили спецоперацій та соціальні мережі. URL: http://ua.racurs.ua/1064-gibrydna-viyna-syly-specoperaciy-ta-socialni-mereji?articlevolist_page=339.

23. Масштабні хакерські атаки: невідомі зламали сайти нацполіції в кількох областях. URL: https://www.5.ua/suspilstvo/masshtabni-khakerski-ataky-nevidomi-zlamaly-saity-natspolitsii-v-kilkokh-oblastiakh-224726.html.

24. Могилко С. В., Зражевська Н. І. Техніка і методи маніпуляції в інтернет-виданнях (на прикладі інтернет-газет «Прес-Центр», «Антенна»). URL: http://journlib.univ.kiev.ua/index.php?act=article&article=2293.

25. Наказ Міністерства зв'язку та масових комунікацій РФ. «Про затвердження правил застосування обладнання систем комунікації, враховуючи програмне забезпечення, що забезпечує виконання встановлених дій при проведенні оперативно-розшукових заходів» // №86 від 27.02.2018. URL: https://digital.gov.ru/ru/documents/6006/.

26. Постанова Кабінету Міністрів України від 29.03.2006 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

27. Постанова Уряду РФ «Про затвердження Правил взаємодії операторів зв'язку з уповноваженими державними органами, які проводять оперативно-розшукову діяльність» (зі змінами та доповненнями) // № 538 від 27 серпня 2005р. URL: http://base.garant.ru/12141783/.

28. Російські збройні кибersилы. Як Росія створює військові загони хакерів. URL: http://ukrpost.biz/ros%D1%96isk%D1%96-zbroin%D1%96-kibersily-iak-ros%D1%96ia-st/.

29. Російські соціальні мережі та їх небезпека. URL: http://navkolonas.com/archives/16028.

30. Российские вооруженные киберсилы Как государство создает военные отряды хакеров. URL: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

31. Россия ввела войска в интернет. URL: https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml#page4.

32. СБУ заблокувала фейкову спробу популяризації так званої «Житомирської народної республіки». URL: https://ssu.gov.ua/ua/news/1/category/2/view/4522#.eG1SdBII.dpbs.

33. СБУ припинила діяльність «диванних» сепаратистів з соцмереж «ВКонтакте» і «Одноклассники». URL: https://www.unian.ua/incidents/2103219-sbu-pripinila-diyalnist-divannih-separatistiv-z-sotsmerej-vkontakte-i-odnoklassniki-video.html.

34. Скільки загинуло українців за час війни на Донбасі: моторошна статистика. URL: https://24tv.ua/skilki_zaginulo_ukrayintsiv_za_chas_viyni_na_donbasi_motoroshna_statistika_n895325.

35. Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України / Пилипчук В. Г., Компанцева Л. Ф., Кудінов С. С., Доронін І. М., Дзьобань О. П., Акульшин О. В., Заруба О. Г.; за заг. ред. В. Г. Пилипчука: моногр. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 272 с. Підрозд. 3.1. С. 178-192.

36. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. ... д-ра юрид. наук. Київ, 2018. 487 с.

37. Топ-15 популярних сайтів України. URL: https://mozok.net/najpopuljarnishi-sajti-ukrajini.

38. Українців зламують через VPN. Як обійти блокування сайтів без ризику для даних. URL: http://news.finance.ua/ua/news/-/403397/ukrayintsiv-zlamuyut-cherez-vpn-yak-obijty-blokuvannya-sajtiv-bez-ryzyku-dlya-danyh

39. Хакерські атаки на Україну. URL: https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D1%96_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83_(2017).

40. Черниш Р.Ф. Міжнародно-правовий досвід використання соціальних мереж військовослужбовцями збройних сил та співробітниками правоохоронних органів. *Порівняльно-аналітичне право – електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2016. Вип. 6. URL: http://pap.in.ua/6_2016/64.pdf.

41. Черниш Р.Ф. Нові форми протиправного доступу співробітників спеціальних служб країни-агресора до інформаційних ресурсів об'єктів критичної інфраструктури. *Сучасні тенденції розбудови правової держави в Україні та світі* : Зб. наук. ст. за матеріалами 6 Міжнар. наук.-практ. конф. (Житомир, 19 квітня 2018 р.) / Мін-во освіти і науки України ; Жит. нац. агроекологічний ун-т. Житомир, 2018. с. 258-260.

42. Черниш Р.Ф. Окремі кроки протидії сепаратизму в інформаційній сфері, як передумова реалізації євроінтеграційних процесів. *Актуальні проблеми державно-правового розвитку України в контексті євроінтеграційних процесів* : матеріали Міжнародної науково-практичної конференції. присвяченої 20-річчю Конституції України. м. Запоріжжя. Запоріжжя : «Просвіта». 2016. С. 278-282.

43. Черниш Р.Ф. Окремі механізми доступу представників спеціальних служб до інформації, яка циркулює в державних органах в умовах ведення гібридної війни. *International scientific and practical conference «Legal practice in EU countries and Ukraine at the modern stage»* : Conference proceedings, January 25-26, 2019. Arad: Izdevnieciba «Baltija Publishing», p. 439-442.

44. Черниш Р.Ф. Протидія недотриманню положень окремих нормативно-правових актів в інформаційні сфері. *Наукові читання – 2018* :

Матеріали науково-практичної конференції професорсько-викладацького складу науково-інноваційного інституту екології та лісу, 1 березня 2018 р. Житомир : ЖНАЕУ, 2018. с. 181-185.

45. Черниш Р.Ф. Соціальні мережі, як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності* : зб. наук. праць. 2017. Вип. 136. с. 205-214.

46. Черниш Р.Ф. Спеціальні підрозділи інформаційного впливу Російської Федерації. *Вплив євроінтеграції на розвиток юридичної науки в Україні*: Матеріали І всеукраїнської заочної науково-практичної конференції (м.Рівне, 27-28 квітня 2017 р.). Рівне : Національний університет водного господарства та природокористування. 2017. с. 219-223.

47. Черниш Р.Ф., Осауленко І.М. Щодо питання протидії формам та методам ведення представниками спеціальних служб Російської Федерації гібридної війни в інформаційній сфері. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : матеріали постійно діючого наук.-практ. семінару (м. Харків, 25 трав. 2018 р.). Харків : Право, 2018. Вип. 9. с.97-102.

48. Черниш Р.Ф., Осауленко І.М., Микитюк Д.В. Механізми поширення шкідливого програмного забезпечення та правові способи протидії. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : матеріали постійно діючого наук.-практ. семінару, м. Харків, 23 трав. 2019 р. Право, 2019. Вип. 10. с.70-74.

49. Швець М.Я. Основи інформаційного права та концепція формування системи інформаційного законодавства України URL: http://www.library.ukma.kiev.ua/e-ib/NZ/NZV19_2001_Spets/43_shvets_mya.pdf.

50. Штоквиш О.А. Історична свідомість як об’єкт маніпулятивних технологій. URL: http://www.stattionline.org.ua/histori/107/19992-istorichna-svidomist-yak-ob-yekt-manipulyativnix-texnologij.html.