ЗАПОРІЗЬКА ОБЛАСНА
УНІВЕРСАЛЬНА НАУКОВА
БІБЛІОТЕКА

УКРАЇНСЬКИЙ ВИБІР:
ВИКЛИКИ ТА ПЕРСПЕКТИВИ

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВІЙНИ

ПРЕС – ДАЙДЖЕСТ

III квартал 2022 р.

КОМУНАЛЬНИЙ ЗАКЛАД
«ЗАПОРІЗЬКА ОБЛАСНА УНІВЕРСАЛЬНА
НАУКОВА БІБЛІОТЕКА»
ЗАПОРІЗЬКОЇ ОБЛАСНОЇ РАДИ

Відділ наукової інформації та бібліографії

Український вибір:
виклики та перспективи

Інформаційна безпека в умовах війни

ПРЕС – ДАЙДЖЕСТ
ІІІ квартал 2022 р.

Запоріжжя
2022

УДК 007:004.056:355.48(048)
Г-52

Інформаційна безпека в умовах війни : прес-дайджест. ІІІ кв. 2022 р. / КЗ «ЗОУНБ» ЗОР, Від. наук. інформації та бібліографії ; [підгот. Ю. Щеглова ; ред. Т. Пішванова]. – Запоріжжя : [ЗОУНБ], 2022. – 24 с. – (Український вибір: виклики та перспективи).

У сучасних умовах пріоритетна роль забезпечення стабільного функціонування інформаційної сфери належить державі. Саме на державу як основний регулятор суспільних процесів покладено важливу місію, що спрямовує та стимулює розвиток інформаційної сфери, не допускає негативних проявів цього розвитку, а навпаки - прискорює перехід України до якісно нової стадії розвитку - інформаційного суспільства. За цих обставин сформувалася залежність національної безпеки держави від забезпечення її інформаційної складової, що зростає в силу розвитку інформаційних технологій і сучасних глобалізаційних процесів. Тому, в умовах посилення зовнішніх загроз і небезпек, особливо після 24 лютого 2022 року, а також соціально-економічної та суспільно-політичної кризи, що спостерігається в Україні, особливої актуальності набувають питання інформаційної безпеки в системі національної безпеки.

Третій спецвипуск прес-дайджеста 2022 року містить публікації, які розглядають актуальні питання захисту вітчизняного інформаційного простору та забезпечення державної безпеки в інформаційній сфері.

Окреслені основні положення сучасної Стратегії інформаційної безпеки України. Деталізовані концептуальні засади державної інформаційної політики в умовах сучасності. Висвітлені типові види загроз зовнішнього інформаційного впливу. Акцентована увага на особливостях проведення спеціальних інформаційних операцій проти України.

Досліджуються наявні підходи до побудови дефініції інформаційної безпеки та характеризується їхня сутність.

Описується виявлення негативних проявів впливу гібридних форм і способів сучасного інформаційного простору на людську психіку та формулюються відповідні пропозиції щодо забезпечення інформаційно-психологічної безпеки особистості.

Розглядається поняття кібербезпеки на основі аналізу чинного національного законодавства, а також описуються найбільш гучні та відомі кіберзагрози під час воєнної агресії РФ.

Аналізується сутність поняття пропаганди. Наводяться приклади використання пропаганди в державній інформаційній політиці та при налагодженні комунікації між різними суб’єктами. З’ясовується значимість пропаганди для інформування членів суспільства в державах з демократичним і тоталітарним політичними режимами.

Шопіна І. М.

Поняття інформаційної безпеки: концептуальні підходи до визначення

Вважається, що одне з перших визначень поняття інформаційної безпеки було сформульовано у 1980 році Л. Дж. Хоффманом. Автор вважав, що інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації. Вказана дефініція, сформульована ще у доцифрову епоху, виявилася надзвичайно стійкою – незважаючи на активний розвиток інформаційного права та його термінологічної бази, сприйняття інформаційної безпеки як стану інформації або стану захищеності цієї інформації є найбільш поширеним з-поміж інших підходів до сутності досліджуваного феномену.

Поняття інформаційної безпеки як стану знайшло своє відображення у чинній Стратегії інформаційної безпеки, відповідно до якої інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Відповідно до ч.4 ст.3 Закону України «Про національну безпеку України», державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. З цього законодавчого положення ми можемо зробити висновок, що інформаційна безпека є видом національної безпеки. Отже, як перше за часом виникнення, так і легальне визначення поняття інформаційної безпеки базуються на **статусному підході,** за якого досліджуваний феномен розуміється як актуальний стан інформації (відомостей,

ресурсів) або актуальний стан захищеності останніх.

Близьким до статусного підходу є **концептуальний підхід,** за якого інформаційна безпека сприймається як рівень захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх та внутрішніх загроз.

Якщо статусний підхід обмежується констатацією певного стану інформаційної безпеки, то сприйняття її як рівня передбачає певне оцінювання, диференціацію. Це дає змогу виокремити **диференційний підхід** до визначення інформаційної безпеки, сутність якого полягає у визначенні її рівнів у певних суб'єктів та у певні проміжки часу.

Досить поширеним у теоретичних джерелах є **підхід**, за якого досліджуване явище розуміється як **суспільні (соціальні) відносини**. Так, Р. Калюжний та В. Цимбалюк вважають, що інформаційна безпека − це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації. О. Крюков формулює визначення інформаційної безпеки як суспільних правовідносин щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їхньої життєдіяльності; суспільних правовідносин, пов'язаних з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави.

А. Ландіна формулює поняття інформаційної безпеки як об'єкта злочинного посягання – це врегульований нормами права порядок суспільних відносин у частині реалізації інформаційної потреби фізичних та юридичних осіб, суспільства, держави, проти якого спрямоване суспільно небезпечне діяння. **Реляціоналістський** (від англ. relationalism – юридичний реалізм) **підхід** обумовлює сприйняття інформаційної безпеки як виду суспільних правовідносин, що виникають в інформаційній сфері на основі актів інформаційного законодавства з метою приведення об'єктів інформаційної безпеки у бажаний для держави і суспільства стан.

Досить цікавим є **інструментальний підхід**, за якого інформаційна безпека сприймається як сукупність засобів забезпечення інформаційного

суверенітету України, захисту інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз. Додамо, що він також знайшов відображення у правових актах. Так, у Положенні про організацію системи внутрішнього контролю в банках України та банківських групах інформаційна безпека розуміється як комплекс організаційних, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях банку та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності банку або його клієнтів.

У зарубіжних теоретичних джерелах досить розповсюдженим є **протекціоністський підхід**, у межах якого інформаційна безпека ототожнюється із захистом. Так, інформаційна безпека визначається як захист інформації, системи та апаратного забезпечення, які використовують, зберігають і передають інформацію для забезпечення цілісності, конфіденційності та доступності даних, а також захищені операційні процедури. Інформаційна безпека визначається також як ступінь захисту, інтеграції та доступності інформації та засобів її обробки.

Слід також відмітити наявність **збережувально-забезпечувального підходу**, за якого інформаційна безпека визначається як збереження конфіденційності, цілісності та доступності інформації; а також інших її властивостей, таких як автентичність, підзвітність, невідмовність. На думку О. Литвиненка, під інформаційної безпекою слід розуміти єдність трьох елементів: забезпечення захисту інформації; забезпечення захисту й контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності. Збережувально-забезпечувальний підхід формує уявлення про інформаційну безпеку як про збереження і забезпечення істотних властивостей інформації, зокрема, її цілісності, доступності, автентичності, конфіденційності.

Процесуальний підхід представляє інформаційну безпеку як процес або сукупність процесів, які виникають і протікають в інформаційних та соціальних системах і призначені для досягнення цілей публічного управління в інформаційній сфері. О. Шумейко вважає, що інформаційна безпека – це одна з характеристик інформаційної системи, тобто інформаційна система на певний момент часу володіє деяким станом (рівнем) захищеності, а захист інформації – це процес, який повинен

виконуватися неперервно протягом життєвого циклу інформаційної системи.

У межах **діяльнісного підходу** інформаційна безпека ототожнюється з діяльністю або комплексом дій з інформаційними ресурсами або системами. Так, польські дослідники поняття інформаційної безпеки визначають як сукупність дій, методів і процедур, здійснюваних уповноваженими особами і спрямованих на забезпечення цілісності збирання, зберігання та обробки інформаційних ресурсів шляхом їхнього захисту від небажаного, несанкціонованого поширення, модифікації або знищення.

Екзистенційний підхід зосереджує увагу на внутрішньому суб'єктивному сприйнятті інформаційної безпеки, породжуючи поняття «відчутна інформаційна безпека», яка визначається як суб'єктивна ймовірність, з якою споживачі інформації вважають, що їхня особиста інформація не буде переглядатися, зберігатися або змінюватися неналежними сторонами під час транспортування або зберігання у спосіб, що відповідає їхнім впевненим очікуванням.

Отже, серед описаних підходів відсутній нормативний. Слід звернути увагу на міждисциплінарність дослідження проблем інформаційної безпеки, яка, з одного боку, сприяє багатоаспектному її розумінню, але, з іншого боку, не дозволяє спрямувати всі зусилля на створення належного правового та нормативного підґрунтя досліджуваного феномену.

Науково-інформаційний вісник Івано-Франківського університету Права імені Короля Данила Галицького. Серія Право. – 2022. - № 13. – С. 133-140.

Новицький В. Я.

Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах.

З метою адекватного реагування на поширення гібридних загроз в Україні наприкінці 2021 року на державному рівні була схвалена **Стратегія інформаційної безпеки** як фундаментальний документ, який визначає завдання та шляхи діяльності держави з метою недопущення кризових явищ у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових. Очікується, що практичне

впровадження цієї Стратегії має посилити можливості держави щодо забезпечення власної інформаційної безпеки, захисту інформаційного простору. Основною загрозою безпеці України в цьому документі визначена Росія і проведена цією країною інформаційна політика. Стратегію планується реалізувати до 2025 року.

Цим декларативним документом (Стратегія інформаційної безпеки) визначено 7 важливих перспективних цілей. *Перша* передбачає протидію дезінформації та інформаційним операціям, насамперед з боку держави-агресора, спрямованої проти України. *Друга* – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. *Третя* – підвищення рівня медіакультури та медіаграмотності суспільства. *Четверта* – забезпечення дотримання прав особи на збір, зберігання, використання і поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів. *П'ята* – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до всеукраїнського інформаційного простору. *Шоста* – розвиток інформаційного суспільства та підвищення рівня культури діалогу. *Сьома* ціль – створення ефективної системи стратегічних комунікацій.

Планується, що успішна реалізація Стратегії інформаційної безпеки матиме такі позитивні наслідки, як: побудований захищений інформаційний простір, гарантування інформаційної безпеки держави та її складових; ефективне функціонування системи стратегічних комунікацій; запровадження механізмів ефективної протидії поширенню незаконного контенту тощо.

В умовах гібридної війни наша держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання держави. Інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на країни, в яких інформаційний простір є незахищеним.

Загалом існує з десяток різних видів інформаційного впливу. Тому потрібно розрізняти пропаганду, спеціальні інформаційні операції, психологічні операції, дезінформацію та інші впливи, оскільки кожен з них має свій алгоритм, форми й методи реалізації. Досвід протидії інформаційним операціям переконливо демонструє, що переважно вони плануються й організовуються з-за кордону, але з опорою на наявні оперативні позиції й можливості в країні, де проводиться така операція. Зазвичай російські інформаційні операції вирізняються тим, що вони плануються й реалізуються у рамках єдиного оперативного задуму та спільного стратегічного наративу, відрізняючись лише формами й методами реалізації, а також вибором цільової аудиторії. Але безпосередні виконавці часто мешкають в Україні, що і надає змогу вітчизняній спецслужбі викривати конкретних осіб, мережі ботоферм чи тролеферм, застосовувати до них відповідні заходи, передбачені чинним законодавством.

Наприклад, тролеферми – більш складна структура, яка має свою ієрархію, де працюють «живі» люди. Найвища ланка – це ті, хто пише пости, виступає з «експертною» думкою, ініціює дискусії й задає напрями обговорення. Як правило, вони особисто пишуть тексти на задану замовником тему, згідно з затвердженими методичними рекомендаціями. Але в них складно знайди спільні фрази і вислови. Можна побачити лише емоційно забарвлені маркери, такі як «тарифний геноцид», «київська влада», «карателі» тощо. Знов-таки демаскуючою ознакою таких тролів є співпадання меседжів і часу порушення того чи іншого питання. Нижче в ієрархії є виконавці, які поширюють дописи перших, долучаючи свої слова й активно відповідаючи на коментарі користувачів, щоб підтримували публікацію у стрічці новин. Найнижчою ланкою є особи, які здійснюють позиційне коментування. Як правило, вони поширюють заздалегідь прописані для них (10–20 варіантів) коментарі і неохоче дискутують. На більш-менш серйозне питання щодо теми, яка коментується, вони неспроможні відповісти.

Головне завдання тролів – ініціювати в мережі інформаційну хвилю на задану тематику (або хвилю «флуду» чи «флейму»), до якої масово приєднаються реальні користувачі, яких на професійному жаргоні росіяни називають «гарматним м’ясом». Але бото- чи тролеферми не є небезпечними самі по собі. Їхню вражаючу ефективність забезпечує те, що майже всі сегменти бото- й тролеферм (якщо ми говоримо про російські) є функціональною складовою російських автоматизованих

комплексів моніторингу мережі Інтернет з прихованими функціями впливу на процеси у середовищі соціальних мереж. Так, у РФ діють системи моніторингу компаній «Крібрум», «Медіалогія», «Квант», «Бастіон», «Brand Analytics» тощо. Кількість автоматизованих бот-акаунтів, які діють у всьому світі, складає понад 100 млн. акаунтів (тільки в системі «Крібрум»). Таке поєднання дає змогу реалізувати небезпечну технологію впливу на користувачів соціальних мереж, так званий «астротурфінг» – імітацію широкої громадської підтримки певних ідей, думок, меседжів, а також осіб чи політичних сил. Астротурфінг дає змогу створити фейкову громадську думку або інтерпретацію події, яку користувачі мережі Інтернет сприйматимуть як справжню. Наявність таких систем дозволяє РФ на основі моніторингу контенту в Інтернеті й аналітичного опрацювання «великих даних» виявляти вразливості противника, планувати, здійснювати й коригувати власні інформаційні атаки, а також відстежувати їхню ефективність і результативність.

За таких умов не можна недооцінювати роль та місце Служби безпеки України у питаннях забезпечення інформаційної безпеки в Україні. Логічно, що у положеннях Стратегії інформаційної безпеки значна роль відводиться діяльності вітчизняної спецслужби, яка у межах своєї компетенції проводить моніторинг завдяки спеціальним методам і способам вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення реальних та потенційних загроз державній безпеці в інформаційній сфері; організовує та забезпечує протидію проведенню проти України спеціальних інформаційних операцій, особливо з боку РФ, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України.

Також слід вказати, що у липні 2021 року при РНБО України створено групу з питань захисту вітчизняного інформаційного простору. Очікується, що напрацювання та результати робочої групи можуть бути використані для ініціювання внесення відповідних нормативних змін з урахуванням досвіду демократичних країн світу щодо забезпечення високого рівня захисту від трансформаційних гібридних загроз.

Інформація і право. – 2022. - № 1 – С. 111-118.

Алещенко В.

Інформаційно-психологічна складова безпеки особистості в умовах гібрібної війни.

Інформаційно-психологічна безпека особистості (ІПБ) – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

Інформаційно-психологічну безпеку визначають і як стан захищеності індивідуальної, групової й суспільної свідомості та соціальних суб'єктів різних рівнів від впливу негативних інформаційних факторів, які викликають дисфункціональні соціальні процеси. Таким чином, ІПБ особистості покликана захистити особистість і суспільство від деструктивного інформаційного впливу.

Отже, під інформаційно-психологічною безпекою сьогодні прийнято розуміти стан захищеності громадян, їхніх окремих груп і соціальних верств, а також населення в цілому від інформаційно-психологічних впливів, що здійснюються шляхом впровадження деструктивної інформації у свідомість та (або) у підсвідомість людини, що призводить до неадекватного сприйняття ним дійсності.

Сферою активного пізнання в гібридній війні виступає вектор інформаційних впливів на особистість, спрямований на формування деструктивних установок. Це явище отримало назву деструктивний *інформаційно-психологічний вплив (ІПВ)* і трактується як вплив інформації на психіку та свідомість людини, що призводить до неадекватного відображення оточуючої дійсності і як наслідок - зміни поведінки.

Основними суб'єктами у сфері забезпечення інформаційно-психологічної безпеки особистості є: Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, міністерства та інші центральні органи виконавчої влади, Національний банк України, ЗСУ, Служба безпеки України, Служба зовнішньої розвідки України, Державна служба спеціального зв'язку та захисту інформації України тощо.

Враховуючи специфіку діяльності вказаних органів влади, основну мету їхнього створення і чисельність апарату, можна зробити висновок, що вищезазначені органи державного управління можуть ефективно

забезпечувати переважно загальнодержавні ідеологічні та захисні заходи від інформаційних загроз суспільству, державі. Поряд з цим забезпечити належний інформаційно-психологічний захист кожної особистості та підвищення її власних ресурсів шляхом організаційних, соціальних, психологічних, педагогічних та інших заходів вищевказані суб'єкти інформаційної безпеки фізично неспроможні.

Основними суб'єктами ІПВ є: особи, які приймають рішення, і насамперед військово-політичне керівництво держави; окремі індивіди, військовослужбовці та цивільне населення, у тому числі дружніх та нейтральних держав; політичні партії; громадські та релігійні організації, меншини; певні соціальні групи (інтелігенція, підприємці, домогосподарки тощо).

Сучасні теорія та практика визначають, що **до основних об'єктів ІПВ належать:** духовний стан особистості; умови та фактори, що забезпечують розвиток усіх сфер життєдіяльності особистості та суспільства; мовне середовище; соціальні, ідеологічні та політичні орієнтири; соціальні зв'язки; психофізичні фактори, що виявляються у вигляді фізичних, хімічних та інших впливів. природного, антропогенного та техногенного походження; генофонд народів, що населяють державу.

Необхідно чітко розуміти, що інформація, яка несе психологічну загрозу, небезпеку, за своєю сутністю не відповідає моральним нормам і є маніпулятивною, часто викликає в людини стан психічної напруги, тривоги, страху, інформаційно-психологічний стрес, психічний розлад та інші психофізіологічні порушення. Тривалий інформаційний вплив, що перевищує допустиму для конкретної людини межу, спонукає інформаційне перенавантаження психіки та призводить до втоми нервових центрів, послідовних реакцій на подразники. Це призводить до послаблення супротиву організму, порушення нормальних фізіологічних функцій, зниження працездатності, виникнення почуття безпорадності та сугестивності. За «успішного» здійснення ІПВ на індивідуальну та суспільну свідомість досягається головне завдання – зміна світоглядних засад суспільства, його духовних цінностей та моральних орієнтирів. Формуються спотворені уявлення та потреби, одночасно нав'язуються чужі ідеали. Відбувається трансформація психологічної безпеки особистості, що може призвести до психічних розладів. Саме тому психологічна безпека особистості та суспільства має займати особливе місце в державній політиці.

Критеріями ІПБ особистості в суб'єктивному плані виступають її ресурси, рівень захищеності яких від інформаційного впливу залежать від таких внутрішніх факторів:

1) сформованість уявлень про інформаційно-психологічну безпеку (адекватність знань сприяє свідомому формуванню захисних механізмів від інформаційних загроз);

2) рівень критичності мислення (здатність піддавати всебічному аналізу різну інформацію з метою з'ясувати ступінь її логічності та ефективності застосування в цій ситуації);

3) ступінь психологічної стійкості (суб'єктивна готовність не піддаватися і не підкорятися інформаційному впливу).

Виокремлюються такі напрями інформаційно-психологічних атак проти України:

1) широке застосування підконтрольних засобів масової інформації (у теле-, радіо- та Інтернет-просторі), ведення за їхньою допомогою пропаганди та створення необхідного сприятливого інформаційно-психологічного фону на територіїУкраїни, зокрема, з метою здійснення дезінформації, нагнітання обстановки, виправдання агресії, деморалізації патріотично налаштованих кіл українського суспільства;

2) нав'язування думок про неспроможність української влади керувати державою та приймати раціональні рішення; формування негативних суджень щодо воєнно-політичного керівництва України;

3) поширення поглядів про те, що українська армія на сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва;

4) нав'язування думки про те, що Україна не обійдеться без російського газу і сторонам необхідно повернутися до перегляду газових контрактів;

5) виключення з радіо простору на підконтрольних РФ територіях загальнодержавних українських теле- й радіоканалів, взяття під контроль регіональних (місцевих) засобів масової інформації тощо;

6) застосування пропагандистських підрозділів в інформаційних та соціальних мережах (на форумах, у соціальних групах, Інтернет-спільнотах).

Особливого значення проблеми інформаційно-психологічної безпеки особистості набувають в умовах виконання обов'язків військової служби. Об'єктом особливого інформаційно-психологічного впливу залишаються свідомість і психіка особового складу ЗС України. Військовослужбовець,

будучи повноправним членом суспільства, піддається тим самим деструктивним інформаційно-психологічним впливам, як і кожна людина. Проте специфіка виконуваних завдань визначає значущість питань захисту військовослужбовців від ІПВ, оскільки така дія може суттєво підірвати всю систему військової безпеки держави. Негативними наслідками ІПВ на особовий склад ЗС України в умовах гібридної війни слідв важати:

• розмивання відчуття гордості за свою державу, належності до її збройних сил, підриву переконаності військовослужбовців у необхідності виконувати свій конституційний обов'язок по захисту Українського народу, своєї землі;

• зниження морально-психологічного стану, створення обстановки невпевненості, сумнівів особового складу щодо власного майбутнього, майбутнього збройних сил і держави, послаблення волі до проведення конструктивних реформ, а у воєнний час - до збройного опору;

• розкол військових колективів за політичними, релігійними, етнічними, службовими та іншими мотивами, протиставлення солдатського й офіцерського складу;

• погіршення боєздатності частині підрозділів за рахунок зниження службової активності, дезертирства, симуляції хвороби, ухилення від виконання наказів командирів, зради, коливань і сумнівів у надійності зброї, у придушенні волі, створення спотвореної картини бойових дій, бойової обстановки;

• невірне сприйняття військовослужбовцями наявних загроз національній безпеці, дійсних планів і намірів противника.

Ефективними способами протистояння негативному впливу інформаційних потоків є:

• моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері;

• розвиток і функціонування системи стратегічних комунікацій сил оборони;

• здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційно-психологічної безпеки, у тому числі захисту єдиного інформаційного середовища сил оборони, зокрема, в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів ЗСУ, інших військових формувань, утворених відповідно до законів України;

• зв'язки з українськими та іноземними засобами масової інформації

щодо висвітлення ситуації в районах здійснення заходів із забезпечення національної безпеки й оборони, відсічі та стримування збройної агресії РФ;

• протидію інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти ЗСУ та інших військових формувань, утворених відповідно до законів України;

• донесення достовірної інформації до військовослужбовців ЗСУ, інших складових сил оборони;

• визначення та розробка як один з основних індикаторів (показників) стану національної безпеки такого інтегрованого критерію, як морально-психологічний стан громадян країни (об'єктивно відображає рівень підтримки громадянами державної політики чинної влади), і показників його оцінки (рівень деструктивного зовнішнього та внутрішнього інформаційного впливу);

• підготовки фахівців у сфері інформаційно-психологічного протиборства, розвиток міждисциплінарних наукових і навчальних програм за профілем соціальних комунікацій та інформаційно-психологічної безпеки.

Вісник КНУ ім Т. Шевченка. Військово-спеціальні науки. – 2022. - № 1. – С. 13-21.

Мальцева І. Р., Черниш Ю. О., Штонда Р. М.

Аналіз деяких кіберзагроз в умовах війни.

В наш час вплив в кіберпросторі може з неймовірною швидкістю розгорнути ситуацію в суспільстві в напрямі, потрібному нашому ворогу.

З 2018 року при Службі безпеки України працює Ситуаційний центр забезпечення кібербезпеки. Ця структура створювалася за допомогою Північноатлантичного альянсу - технічне обладнання та програмне забезпечення для роботи Центру було надано в рамках виконання першого етапу Угоди про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки. На базі Ситуаційного центру функціонує система управління подіями інформаційної безпеки, яка моніторить події у режимі реального часу і дозволяє аналізувати стан інформаційної безпеки. І це дає змогу оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі. В середньому, за статистикою

Держслужби спеціального зв'язку та захисту інформації (Держспецзв'язку), щонеділі в Україні блокувалось до 50 тисяч кібератак на державні інформаційні ресурси.

Як показують останні події, війна в інформаційному просторі завдає не меншої шкоди, аніж війна на полі бою. І це без жодних перебільшень. Розуміючи це все, у перші два місяці воєнних дій парламент оперативно та одноголосно оптимізував кримінальне та кримінально-процесуальне законодавство. Удосконалив також підстави та самі процесуальні механізми щодо притягнення до кримінальної відповідальності всіх кіберзлочинців. Зміни зосереджені у двох даних законах:

1. «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 року;

2. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 року.

Від самого початку війни стало відомо про величезну кількість кібератак на українські ресурси. Напад російських хакерів на Україну розпочався буквально за кілька хвилин до повномасштабного вторгнення армії. За даними агентства Reuters, США, Великобританія та Європейський Союз офіційно звинуватили РФ у великомасштабному кібернападі, який порушив роботу супутникового інтернет-сервісу Viasat за годину до початку війни, 24 лютого 2022 року. Це спричинило до знищення «десятків тисяч» супутникових терміналів. Активно зазначається, що дана атака торкнулася також європейських інтернет-користувачів та деяких вітрових електростанцій. А ще під хвилю потрапили українські військові та декілька сотень цивільних клієнтів.

За конкретними даними MIT Technology Review, напад російських хакерів на платформу Viasat - це найбільший відомий та болючий злам під час війни. Про це наголошував Хуан Андрес Герреро-Сааде. Це відомий дослідник кіберзагроз із SentinelOne. Даний злам - один із перших живих прикладів того, як кібератаки можуть бути направлені та конкретно розраховані за часом для посилення ворожих збройних сил на нашій планеті, шляхом порушень та навіть цілковитого знищення розвинутих технологій. В ході цієї кібератаки 24 лютого 2022 року запустили дуже шкідливе програмне забезпечення AcidRain. Воно стерло всі дані модемів та маршрутизаторів Viasat, і в результаті чого вони всі

відключилися. Таким чином, на знищення пішли тисячі терміналів. Попереднє програмне забезпечення російських хакерів було вузько спрямованим та сильно шкідливим для системи. Та все ж AcidRaid є скоріше універсальною зброєю.

Не так давно Держспецзв'язок повідомив про масове отримання українськими користувачами нового напливу небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання шахраями повного контролю над вашим пристроєм, а точніше - ноутбуками та комп'ютерами, що загрожує крадіжкою та пошкодженнями комп'ютерних даних.

Наступним потрібно згадати незграбну спробу атаки хакерського угруповування Strontium. Вони намагалися зосередити всі свої зусилля на отриманні доступу до всіх комп'ютерних мереж в Україні, США та ЄС. Цими нищівними діями вони планували забезпечити підтримку фізичного вторгнення Росії в Україну на тактичному рівні, викрасти та знешкодити всю конфіденційну інформацію.

Є інформація, що 23 березня 2022 року ворог намагався здійснити потужну кібератаку на наші державні установи з використанням шкідливих та мало знайомих нашій системі програм, одна з них - Cobalt Strike Beacon. Вона сильно та безповоротно вражає всю систему у випадку її відкриття.

4 квітня 2022 року Держспецзв'язок дав екстрене попередження про масове розповсюдження електронних листів, що носило назву «Військові злочинці РФ.htm». Їхнє відкриття призводить до того, що хакери отримують віддалений доступ до комп'ютерів жертв.

Постійно під прицілами знаходяться об'єкти критичної інфраструктури. Відомий український провайдер Укртелеком потрапив під потужну атаку 28 березня 2022 року, під час якої зловмисники намагалися зламати та проаналізувати, як влаштована ІТ-інфраструктура. В їхні плани входило вивести з ладу обладнання та різні сервіси. Також вони намагалися отримати контроль над мережею та обладнанням даної компанії.

Це приклади лише масованих атак. Ймовірно, про атаки менших масштабів та окремі випадки персональних зламів просто мало що відомо і про них не інформують у суспільстві.

Також важливим фактом є те, що ще до початку воєнних дій, після славнозвісної кібератаки 14 січня 2021 року на сайти державних органів влади, відчувалася конкретна необхідність запровадження невідкладних

змін на рівні українського законодавства, для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо).

На сьогодні ІТ-спільнота вже легко зможе легально тестувати всі необхідні державні інформаційні системи на наявність вразливого місця, а сама держава отримає невідкладні інструменти для значного підвищення ступеня захисту саме таких систем.

Слід зазначити, що від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові - так звана «КіберАрмія». Звичайні люди, поряд із професіоналами сфери ІТ, наносять нищівний удар, атакуючи ворога у кіберпросторі, завдають йому збитків та зривають плани.

Кожному під час воєнного стану варто звернути увагу на дані точки контролю: 1. Старатися вивчати та активно аналізувати слабкі місця вашого кіберзахисту, щоб щоденно укріплювати їх. Хакери завжди здійснюють багато розвідувальних операцій в Україні. Таким чином вони знаходять найслабші місця в захисті наших компаній та, скориставшись цим, атакують, б'ючи по них. Ніколи не існувало та не існує на 100% захищених систем. Варто зазначити, чим менше вартуватиме шахраям злам будь-якої системи, то вищою буде їхня мотивація. 2. Тим, хто перебуває в зоні кіберризику, варто безупинно слідкувати за відповідними повідомленнями на різних офіційних ресурсах Держспецзв'язку та CERT-UA. Ці органи першими публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати їхні ризики. 3. Потрібно завжди пам'ятати про безпеку системи, яка залежить конкретно та абсолютно точно від кожного працівника. Хакери здатні напасти на компанію або ж установу і через робітників різних фірм та установ, викравши їхні дані. В особливій небезпеці знаходяться військові, а також всі державні діячі. Ці категорії людей мають абсолютно точно звикнути до кібергігієни та прийняти її за норму повсякденного життя, щоб не боротися з важкими наслідками в разі атак. 4. Для тих хакерів, хто проводить небезпечні та щоденні кібератаки на ворогів та займається багхантингом з чітким планом удосконалення та зміцнення української кібербезпеки в умовах воєнного часу, задля повного уникнення невирішених проблем із службою правоохоронних органів потрібно бути повністю готовими довести відповідність своєї діяльності інтересам України.

Кібербезпека: освіта, наука, техніка. – 2022. - № 4. – С. 37-44.

Васильєва Н. В.

Пропаганда як складова інформаційно-комунікативної політики і загроза національній безпеці.

Ступінь розвиненості громадянського суспільства визначається здатністю населення та влади одночасно співіснувати, поєднувати і розмежовувати індивідуальне й колективне, приватне і публічне, забезпечувати рівність прав та обов'язків, соціальну справедливість; наявністю суспільних інститутів, здатних представляти інтереси всіх суб'єктів публічного управління, та залученням громадян до процесів прийняття й реалізації управлінських рішень; забезпеченням балансу у розвитку матеріальної й нематеріальної (духовної) сфер життя, що позначається на нормах моралі та цінностях членів такого суспільства. Вищезазначене можливе лише за наявності демократичного, а не тоталітарного політичного режиму, що концептуально позначається і на формуванні інформаційного суспільства, в якому вирішальну роль відіграють інформаційно-комунікаційні технології.

В інформаційному суспільстві відбувається фактологічна інформованість громадян, на підставі чого формуються їхні світоглядні позиції, та надається аналітична оцінка процесам безпеки як всередині держави, так і в світі; створюються умови для розумового й духовного збагачення, нарощування людського капіталу як основи розвитку соціально-економічної, гуманітарної, культурної й інших сфер суспільного життя, підвищення рівня добробуту громадян, зміцнення державності тощо.

Сьогодні будь-яка держава завдяки інформаційним технологіям може:

– розширювати взаємодію між людьми, розповсюджувати масову інформацію, інтелектуалізувати працю, розвивати освіту, науку, охорону здоров'я, культуру тощо;

– реалізувати власні інтереси без застосування воєнної сили, послабити чи завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів;

– загрожувати інформаційним ресурсам та інфраструктурі іншої країни;

– впливати на суспільну свідомість і нав'язувати власну систему цінностей, інтересів і державно-управлінських рішень у важливих сферах

життєдіяльності та подальшого розвитку.

Дієвою формою комунікації, за якої масово поширюються світоглядні ідеї, аргументи тощо, формується суспільна думка на користь конкретної політичної позиції для досягнення необхідного результату, є пропаганда. Оскільки на постіндустріальному етапі політичний, соціально-економічний, культурний (духовний) розвиток держави відбувається завдяки розвиненості інформаційного суспільства, тому інформаційно-комунікаційна політика за умови демократії спрямована на зміцнення громадянського суспільства, задоволення інтересів його суб'єктів, захист прав і свобод, а за тоталітарного режиму – поширює ідеологію політичного центру.

В Україні державна інформаційна політика сприяє входженню країни до світового інформаційного співтовариства; у Росії до мирного населення (як в середині своєї країни, так і за її межами) влада активно застосовує, насамперед через ЗМІ, методи чорної (спеціалізованої) пропаганди, які дозволяють викликати почуття ненависті, зокрема такі:

– «гнилий оселедець» – публічно обговорюється особа, яку звинувачують у здійснені злочину (наприклад, крадіжка, розтління дітей, вбивство та інше), але не для того, щоб встановити факти реального здійснення цього злочину. В аудиторії створюються групи: «прихильники», «противники», «експерти», «обвинувачі» і «захисники», які під час дискусії постійно поєднують ім'я обвинуваченої особи з обвинуваченням. Таким чином, сам злочин не доведено, але «аромат» скоєння слідує за обговорюваною особою при кожній згадці про неї. На нашу думку, такий метод створює міфи, у т.ч. про історичні постаті або організації, наприклад, про І. Мазепу, С. Бандеру, полк «Азов» тощо;

– «великої брехні» – аудиторії впевнено повідомляють про жахливу глобальну брехню, в яку неможливо повірити, наприклад, обговорення розроблення ворожою стороною бактеріологічної/хімічної/ядерної зброї, що дозволяє створити «шоковий ефект» (емоційну травму, почуття страху), який у подальшому тривалий час визначає погляди на ситуацію, всупереч будь-яким доводам логіки та розуму. Такий метод також створює міфи про непереможність Росії і могутність другої за чисельністю армії у світі;

– «абсолютної очевидності» передбачає систематичне надання аудиторії інформації так, щоб вона сприймалась як само собою зрозуміле, і забезпечувала підтримку більшості без потреби доказувати її правдивість. Автоматичне реагування людської психіки на домінуючу

точку зору та безумовне погодження з нею забезпечує «ефект приєднання». Наприклад, результати соціологічних опитувань і референдумів, які демонструють абсолютну підтримку суспільства з певного питання, при цьому такі дані можуть нічого не мати спільного з реальною ситуацією. Такий метод також створює міфи про російські імперські «аксіоми», як «руський мир» – істинне православ'я та монархію – єдину «дану Богом» владу;

– «невідомого героя» - полягає у героїзації власної армії та воєнної кампанії. З метою виправдання жорстокості, аморальності та безглуздості війни, долання опору людської психіки щодо її проведення, через страх особи за себе і своїх близьких, аудиторії розповідають про армію визволителів, а не загарбників, рятівників, а не окупантів. Таким чином, створюється ілюзія боротьби за високі моральні цінності, викривляючи інформацію про дії, які відбуваються насправді. Прикладом є «спецоперація», яку Росія проводить в Україні;

– «40 на 60» полягає у поданні ЗМІ 60% своєї інформації в інтересах супротивника, забезпечивши його довіру, а 40% використовують для надзвичайно ефективної, завдяки цій довірі, дезінформації. Наприклад, українські канали, які надавали свою інформацію в інтересах держави-агресора.

Інформаційна політика Російської Федерації загрожує національній безпеці України, оскільки свідомо впливає на морально-психологічний стан і поведінку людей, формуючи їхні погляди й настрої щодо негативного сприйняття України як суверенної держави, її права на самостійне існування й історію, самоідентифікацію української нації тощо для задоволення імперських амбіцій, і веде до прийняття відповідних політичних рішень з реалізацією у коротко- й довготривалій перспективі.

Впливовим учасником інформаційної політики є Церква, яка змінює свідомість своїх парафіян. Так, в Україні з 2000-х років з метою «збереження духовної, мовної і культурної ідентичності» російською православною церквою через храми Московського патріархату проводилась потужна інформаційно-пропагандистська кампанія, за якої «руський мир» вважався спільним для трьох братських народів: Росії, України та Білорусі - наднаціональним проєктом, що дозволяло Росії підготувати «сприятливий ґрунт» для подальшої експансії. Запровадження спільного святкування Дня Хрещення Русі та боротьба з різними сучасними суспільними рухами завуальовували діяльність

церковників щодо знищення української етнічної та громадянської ідентичності, і значна кількість вітчизняних політичних діячів і державних посадовців не вважали її деструктивною і загрозливою національній безпеці країни. В той же час «руський мир» з духовного ідеалу перетворився на завойовницьку імперську доктрину, яка не має нічого спільного з православ'ям. Зазначимо, що «багаторічне протистояння проукраїнських і проросійських політичних і церковних сил в Україні і за її межами, боротьба прихильників і противників церковної незалежності», з одного боку, «завершилася створенням автокефальної православної церкви України», а з іншого - призвела до повномасштабної військової ескалації з боку Росії.

Крім того, формування уявлення про історичні й сучасні події відбувається під впливом кінематографу. Тому влада через державне замовлення на виробництво фільмів може «переписувати» історичні факти і створювати міфи, виправдовувати внутрішню і зовнішню політику, ідеалізувати політичний режим, у т.ч. поширювати ідеї ксенофобії, расизму і нетерпимості (наприклад, той же шовінізм), обґрунтовуючи переваги свого народу (нації) над іншим (и) і права їх дискримінувати або пригнічувати тощо.

Незважаючи на те, що Україна у воєнному конфлікті з Росією перебуває з 2014 року, складовою якого є введення «гібридної війни» з використанням різних інформаційно-комунікаційних технологій і наявні втрати людей, територій, інформаційного простору, економічних активів тощо, однак «феномен національної безпеки» в державі не був до кінця усвідомлений, що й призвело до ще більших людських і матеріальних втрат у повномасштабній війні 2022 року. В умовах введення «гібридної війни» військові дії відбуваються з використанням спеціального озброєння, що дозволяє, з одного боку, фізично знищити ворога (його людську силу), а з іншого - здійснити комплекс маніпулятивних заходів з формування певних установок, стереотипів і зміни масової свідомості задля розколу й дискредитації політичної еліти в очах власного народу, світового співтовариства тощо.

Пропаганда є зброєю масового ураження, оскільки впливає на свідомість населення і формує суспільне ставлення. У повоєнний період питання гарантування національної, зокрема інформаційної, безпеки має стати головним пріоритетом при формуванні державної інформаційної політики, а також при налагодженні комунікації із населенням, у першу чергу територій, які з 2014 року перебували під окупацією Росії. І тут

багато уваги потрібно приділити соціально-психологічній складовій консолідації громадян України:

1. На рівні дитячих садочків і шкіл запровадження в обов'язковому порядку національно-патріотичного виховання та проведення культурно-просвітницьких заходів із відвідуванням історичних, культурних і природних пам'яток, музеїв, театрів, тематичних виставок тощо (із закладенням коштів у місцеві бюджети), що сприятиме згуртованості дітей та молоді, а також зміні в суспільстві ставлення до української мови й культури, розуміння історичних і сучасних подій, виховує повагу й бережливе ставлення до всього вітчизняного (за походженням) та природи (ліси, парки, сквери).

2. У засобах масової інформації більше уваги приділяти не політичним ток-шоу, де відбувається «з'ясування відносин», а реальним позитивним досягненням України й українців (шляхом застосування «білої», конструктивної пропаганди) в економіці та міжнародних відносинах, культурним надбанням в сфері музики, спорту, видавництва, кінематографії та інших, популяризуванню українського продукту на вітчизняному і світовому ринках. Єдина умова - інформація має бути правдивою, без «ідеологізації».

3. Поширення безоплатних навчальних курсів для різних верств населення, які покращать знання й навички з питань інформаційної та медіаграмотності, кібербезпеки, протидії пропаганді тощо.

Таврійський науковий вісник. Серія: Публічне управління та адміністрування. – 2022. - № 2.- С. 34-41.

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВІЙНИ

Прес – дайджест
ІІІ квартал 2022 р.

Підготувала: *Ю. Щеглова*
Редактор: *Т. Пішванова*

Наклад 10 прим.
Віддруковано у Запорізькій ОУНБ
просп. Соборний, 142, Запоріжжя, 69095

Відділ наукової інформації та бібліографії
Телефон: (061) 787-53-57
Ел. пошта: bibliograf.zounb@gmail.com, bibliograf@zounb.zp.ua

ЗАПОРІЖЖЯ
ПР. СОБОРНИЙ, 142
061 787 53 57

BIBLIOGRAF.ZOUNB@UKR.NET
BIBLIOGRAF@ZOUNB.ZP.UA

FACEBOOK.COM/BIBLIOGRAF.ZOUNB
YOUTUBE.COM/BIBLIOGRZOUNB

ZOUNB.ZP.UA