Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВІД ЗОВНІШНІХ ПРОЯВІВ»

Студентки 2 курсу, 7м групи,
спеціальності 281 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» _____ Могір Катерина Адріївна
(підпис студента)

Науковий керівник
канд. екон. наук, доцент _____ Міняйло Олександр Іванович
(підпис керівника)

Гарант освітньої програми д.н. держ.упр., професор _____ Орлова Наталія Сергіївна
(підпис гаранта)

Київ 2019

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ – інформаційна безпека

ІП – інформаційний простір

ЗМІ – засоби масової інформації

ІР – інформаційні ресурси

ІС – інформаційні системи

СЗІ – система захисту інформації

БД – база даних

БІ – безпека інформації

МЗ – механізм захисту

ЗІ – захист інформації

ПЗ – програмне забезпечення

СМ – системи моніторингу

ТХІСМ – технологія побудови системи моніторингу

ВСТУП

Стрімкий розвиток ІТ-інфраструктури підприємств незмінно тягне за собою не контролюємий ріст кількості загроз і уразливості державних інформаційних ресурсів, під якими розуміють взаємопов'язана, устаткована, систематизована, закріплена на матеріальних носіях, інформація, створена і зібрана на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету. В цих умовах оцінювання інформаційних ризиків дає можливість визначити необхідний рівень захисту інформації (ЗІ), здійснити її підтримку і розробити стратегію розвитку інформаційної структури об'єкта захисту. [10]

Згідно потребам Закону України «Про захист інформації в інформаційно-телекомукаційних системах» для забезпечення безпеки Державних інформаційних ресурсів, оброблюваних в автоматизованій системі (АС), необхідно розробляти комплексну систему захисту інформації (КСЗІ).

Найбільшу увагу при формуванні систем інформаційної безпеки в вітчизняних компаніях, підприємствах, установах приділяють, як правило, виконанню вимог нормативно-методичної бази в сфері захисту інформації, визначаючи ці вимоги як першооснову становлення системи інформаційної безпеки, що, однак, само по собі ще не створює гарантій достатнього рівня захисту

Інформаційна безпека молода галузь, яка зараз знаходиться на перетині інформаційних технологій та захисту інформації. Лише комплексний підхід дозволить забезпечити інформаційну безпеку на високому рівні. Це стосується до захисту інформації яка зберігається й оброблюється як в окремому комп'ютері, так і в корпоративній мережі. [53]

Мета і завдання дослідження. Метою є дослідження проблеми гарантування інформаційної безпеки України, захисту національного інформаційного простору з огляду на реальні й потенційні загрози та деструктивні пропагандистсько-маніпулятивні інформаційні впливи.

Об'єктом дослідження є маніпулятивні складові інформаційної безпеки держави та механізми протидії маніпуляції громадською думкою, спрямованої проти України.

Предметом дослідження є інформаційний простір, процеси його захисту.

Практичне значення одержаних результатів. Рекомендації можуть використовуватися для забезпечення належного захисту українському інформаційному простору

Структура роботи відповідає поставленій меті та дослідницьким завданням. Кваліфікаційна робота складається зі вступу, трьох розділів (7 підрозділів), висновків, списку використаних джерел (52 найменування). Повний обсяг роботи становить 49 сторінки (основний текст – 54 сторінок).

Результати дослідження опубліковано в статті «Механізми захисту інформаційного простору від зовнішніх проявів». Публічне управління та адміністрування в умовах суспільних трансформацій. Збірник наукових статтей 2019.-С.470.

Інформативною базою виступили результати наукових і прикладних досліджень українських та зарубіжних вчених, навчальних посібників, монографії, мережа інтернет.

РОЗДІЛ 1. БАЗОВІ ПОНЯТТЯ І СУЧАНИЙ СТАН МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВІД ЗОВНІШНІХ ПРОЯВІВ

1.1. Поняття інформаційного простору.

Сучасний термін "єдиний інформаційний простір" (інформаційна сфера) є результатом еволюції концептуального способу диференціації в загальному геополітичному просторі регіонів, які мають особливості і завдяки цьому потрібно їх розглядати як самостійні простори з власними кордонами, ресурсами, структурою та особливості взаємодії їхньої діяльності, які додають інформаційне забезпечення. [4]

В такому понятті кардинально змінюється зміст цих процесів, як взаємодія їхньої діяльності та конкуренції. Конкуренція найпомітніша внаслідок їхньої боротьби за інформаційну перевагу, за керуванням більш тяжким інформаційним ресурсом, що дає більш кращі можливості щодо управління інформаційним ресурсом супротивника.

Інформаційна сфера – це поняття зібраної інформації, інформаційної інфраструктури, об'єктів, котрі самі генерують, збирають, поширюють та використовують інформацію, і регулюють систему зв'язків з громадськістю. Інформаційна сфера - це відносини, які виникають після: формування а також залучення інформаційних ресурсів на базі генерування, масового збору, оформлення, зберігання, пошуку, розширення та надання історично підтвердженої інформації користувачу; створення та залучення інформаційних інновацій і методів для їх підтримки; захист інформації, можливості суб'єктів, що приймають участь в інформатизації і їх процесах. [2]

Інформаційна сфера це самостійний фактором постіндустріального суспільства, яка сама впливає на економічний стан, політичний, оборонний та на інші складові національної безпеки.

Головними компонентами інформаційного простору є потоки інформації та її поля. Інформаційне поле - це збір усієї можливої інформації в PDO, незважаючи на її форму чи стан, яка відокремлена від об'єкта сприйняття і самого об'єкта.

Шлях інформації в полі відбувається за допомогою спілкування між джерелом та одержувачем інформації, що переходить в інформаційний поток. [3]

Найважливішими функціями, які на даний момент контролює інформаційний простір, є:

1. Інтеграція - виявляє особливі види економічної діяльності в єдине масштабне, інформаційне та культурне середовище;
2. Комунікативний – створює своє середовище для транскордонного, інтерактивного і мобільного зв’язку різних суб’єктів господарювання, де вони можуть обмінюються власною інформацією;
3. Актуалізація – з’єднує інтереси не однакових суб’єктів господарювання які реалізуються завдяки реалізації їх інформаційної політики в інформаційному просторі;
4. Геополітичні - формуються особисті ресурси котрі самі змінюють цінність традиційних ресурсів, створюючи новий простір геополітичних стосунків та їх конкуренції;
5. Інформаційно-соціальний простір перетворює суспільство і замінює характер і суть соціально-економічних відносин у культурних, наукових, політичних, релігійних сферах.

Надшвидкий ріст інформаційних ресурсів в світі і поява нових інформаційних технологій змушують зробити величезні зміни в роботі підприємств і їх процесів. Найбільш важливим стає таке виробництво в галузі

освіти, науки, які сприяють розвитку виробництва завдяки переходу на комп'ютеризацію, інформатизацію, і головне на автоматизацію всіх циклів підприємств. [16]

Об`єктивна необхідність вимагає поступового, але неухильного включення інформаційної сфери України до світового інформаційного простору. Активний розвиток радіомовлення, телебачення, кібернетики та інформатики призвели до появи принципово нових засобів передачі даних.

Отже, головною ознакою сьогодення став процес всеохоплюючої інформатизації суспільства.

Якщо мова йде про інформаційне поле конкретної держави (і кожна держава має його), його кордони зазвичай ототожнюються з її межами, включаючи національну територію, повітряний простір та економіку. У цих областях засоби масової інформації, які спілкуються, тобто спілкуються, зображають, складають уявлення про щось, діють. Але що саме вони говорять, як вони представляють і яке представлення вони складають - це вже частина сфери політики і залежить від інформатора. Наприклад, українське телебачення і радіо та російська мова часто розповідають про одну і ту ж подію по-різному. Ви не повинні дивуватися, і вже точно не так: українське телебачення повинне виражати інтереси української держави, російське телебачення повинне виражати інтереси російської держави, і ці інтереси, як відомо, не відповідають. Але бути здивованим і обуреним, коли іноземне джерело часто використовує засоби масової інформації проти нашої держави є цінним і необхідним. [20]

У статті 4 проекту Закону України "Про інформаційну безпеку та її суверенітет" з 1998 р. Пропонується така версія цієї концепції: "Національний інформаційний простір України - це сфера (об'ємний простір), в якій здійснюються інформаційні процеси та розширюється юрисдикція України". Держава виступає гарантом цілісності нашого національного інформаційного простору на основі: державної політики, визначеної законами, які абсолютно

обов'язкові для всіх учасників інформаційної компанії на національній території, незалежно від їх власників; Зберігання державної власності на основні об’єкти національної території України, використання власної та адекватної бази, економічних важелів для регулюючого впливу на суспільні відносини у сфері інформації; національна система досконалої освіти та майбутніх кваліфікацій для працівників власних засобів масової інформації, експериментальної та наукової діяльності уряду; Забезпечити надійне економічне зростання за цільовими програмами, здійснити необхідні заходи підтримки. [35]

Досліджуючи структуру функцій натиску інформаційного простору, потрібно відокремити три його компоненти:

Розглядаючи зміст функціонального навантаження інформаційного простору, доцільно виділити три його компоненти:

1. Це пов'язано з особливим і конкретним створенням власних елементів;
2. Вони повинні створити сприятливі умови щоб інтегрувати це у масштабний інформаційний простір, використовуючи максимальний розвиток глобальної інформаційної інфраструктури та глобалізації інформаційного простору.
3. Супроводження захисту всіх його власних елементів державного інформаційного простору(безпеки), свобод і прав українських суб'єктів, які працюють у цій галузі, як важливий фактор формування і збереження інформаційного суверенітету України. [45]

Головними ознаками інформаційного простору України є:

1. Єдині принципи та правила з’єднань усіх тем інформаційної діяльності з оптимальним співвідношенням принципів державного регулювання та саморегуляції у формуванні та розвитку державного інформаційного простору

2. Наявність умов для безпечного обміну інформацією між державою, організаціями та громадянами;
3. Найбільш повне задоволення інформаційних потреб держави, організацій та громадян у всій державі;
4. Підтримка балансу інтересів між державою та світовою спільнотою для вступу України до глобального інформаційного простору та збереження нашого інформаційного суверенітету.

Таким чином, єдиний інформаційний простір - це масова сукупність власних баз даних, технологій їх використання та управління, забезпечення інформаційних, телекомунікаційних систем і мереж, що працюють завдяки основам загальних принципів та правил, забезпечуючи інформаційну взаємодію відносин організацій та громадян і задоволення їх необхідних інформаційних потреб. [29]

Другими словами, єдиний інформаційний простір складається з:

1. Інформаційні ресурси (ІС) - бази даних, архіви всіх видів, державні системи зберігання інтелектуальної власності, бібліотеки, музейні склади тощо;
2. Інформаційно-телекомунікаційна інфраструктура;
3. Комп'ютерні та підприємницькі, телекомунікаційні мережі також спеціалізовані системи особливого призначення, канали і мережі передачі між ними даних, способи посередництва і керування територіальним потоком інформації;
4. Інформаційні, комп’ютерні та телекомунікаційні технології - основні, прикладні та підтримуючі бази, системи та їх впровадження;
5. Науковий потенціал та виробничий потенціал у сфері інформатики, телекомунікацій, обчислювальної техніки, зв’язку, розширення доступу до інформації;

6. Організаційні структури, до яких також входить персонал, який забезпечує функціонування та розвиток державної інформаційної інфраструктури;
7. Інформаційні технології, зв'язок, ринок інформації та телекомунікацій, інформаційні послуги, продукти;
8. Способи взаємних дій інформаційного простору України зі відкритими світовими мережами;
9. Інформаційна безпека системи;
10. Медіа-системи;
11. Система інформаційного законодавства. [31]

Інформаційний простір України ще знаходиться на активному етапі створення. Його розвиток характеризується значною нерівністю та відставанням з розвиненими сусідніми країнами, які приділяють значно більше уваги вдосконаленню своєї інформаційної сфери. Характер нашої пострадянської не закріпленої економіки визначає особливості її інформаційного забезпечення, її сутність полягає в:

1. Стара організація інформації про забезпечення економічного розвитку не підходить теперішнім потребам суспільства.
2. Вирішити проблеми світового суспільства неможливо тому копіювання відповідної діяльності інформаційної організації розвинутих країн є неефективним.
3. Структура найоптимальнішої установи, що відповідає умовам суспільства, є невідома, вона виникає тільки в самому процесі життєдіяльності суспільства. [48]

1.2. Види впливу на інформаційний простір.

Основними структурними елементами інформаційного простору суспільства, який має ґрунтуватися на здійсненні державної інформаційної політики, є

інститути, які діють та керують засобами масової інформації (засоби масової інформації та засоби масової комунікації) та установи, які активно оновлюють свої інтереси. В інформаційному просторі, потрібно генерувати змістовні інформаційні потоки по всій громаді. Основними підрозділами управління, які впливають на інформацію про управління є: органи влади та адміністрації (насамперед, структури, які активно спілкуються з громадськістю - служби PR, підрозділи, що реалізують концепцію електронного уряду); державні та недержавні засоби масової інформації та неурядові громадсько-політичні асоціації, інформаційно-комунікаційна діяльність яких відповідає національним інтересам держави. [52] Адміністративні об'єкти в публічному інформаційному просторі для суб'єктів громадського порядку - це, як правило, всі елементи та системи, що існують у цьому просторі. Ступінь та форма впливу залежать від індивідуальних особливостей та характеристик об'єктів управління, а також від їх значущості для цілей та цілей державної інформаційної політики. Значення суспільно-політичних об'єднань, партій та організацій як предмета управління силами та засобами державної інформаційної політики значно зростає за період виборів на рівні центрального та регіонального уряду. [40] При плануванні та здійсненні управлінських впливів на елементи та системи інформаційного простору суспільства в контексті державної інформаційної політики застосовується систематизація об'єктів управління, що дає можливість розподіляти типи, форми, характер і засоби управління. Загалом така систематизація включає:

1. Матеріально-технічні елементи – це всі інформаційно-телекомунікаційні інфраструктури установ. Їх громадська політика до цих засобів досягається, перш за все, методом створення кращих умов, які забезпечуватимуть стабільне функціонування та сприятимуть розвитку цієї інфраструктури, можливість доступу для всього суспільства, і їхня безпосередня інтеграція в інформаційний простір та в професійну і комунікативну діяльність.

2. Віртуальні матеріальні об'єкти – поток інформації, що циркулюється і знаходиться на інформаційних ресурсах в інформаційному просторі суспільства. Управлінська роль національної політики щодо вище перерахованих об'єктів полягає в управлінні інформаційними потоками і процесами, також їхніми інформаційно-правовим регулюванням (це стосується і шляхом регулювання зв'язків з громадськістю для покращення обміну інформацією), для впровадження захисту усієї інформації та її ресурсів, створюють інформаційний фон та створюють інформаційні потоки, структуру і їх характер яких відповідають цілям і вимогам державного сектора і обов’язково державним інтересам з метою покращення і забезпечення політичної, соціальної стабільності інших у громадськості, також до цього відноситься культурний розвиток, розвиток науки і інші соціально необхідні завдання.
3. Об'єкти людської природи - людство і всесвітні спільноти. Керування цими засобами в сфері національної демократичної держави інформаційної політики повинно базуватися на суб'єктивних відносинах, доступної і відкритої інформації та інтерактивної взаємодії на рівних правах.

Особливим об’єктом керуванням державною інформаційною політикою є простір геополітичного конкурента, між яким в вас відбувається відкрите або приховане протистояння інформації. В такому випадку більшість методів керування - це таємні маніпулятивні технології, а використовувані інструменти та технології є арсеналом для ведення інформаційної війни та інформаційних операцій (інформаційні дії та психологічні впливи). В інформаційному суспільстві зі зростаючою залежністю людей від інформації засоби масової інформації та масової комунікації (МК) як одиниця діяльності стають все більш маніпулятивними. [46] Наступні причини (групи причин) є основою цього процесу:

1. Причини, викликані упередженістю та суб’єктивністю людей у сфері масової комунікації, тобто спотвореннями, спричиненими їх індивідуальними психологічними, особистими якостями, політичними пристрастями, симпатіями тощо.
2. Причини, зумовлені політичними, соціально-економічними та організаційними умовами засобів масової інформації, зокрема залежністю ЗМІ та ЗМІ від певних соціальних суб'єктів.
3. Причини, викликані функціонуванням засобів масової інформації. Різні програми дотримуються певних загальних правил або принципів, щоб привернути увагу та охоплення широкого кола засобів масової інформації та засобів масової інформації при доставці матеріалів та підготовці новин. [44]

Потрібно розглянути детальніше актуальні види впливу на інформаційний простір такі як: пропаганда, маніпуляції та дизорієнтація.

Пропаганда - це спеціальне і цілеспрямоване нав’язування думки серед всьіх людей. Цей термін походить ще від латинської мови і перекладається "те, що має бути поширене".

Термін “пропаганда” пов'язаний з посиланням Папи Римського від 22 червня 1622 року. Оригінальна назва цього посилання Congregatio de Propaganda Fide. Там безпосередньо йшлося про формування нової установи спеціально для координації місіонерської роботи, тобто нав’язування або поширення віри. В цьому листі особливо детально було написано про категоричне заборону використання цієї діяльності в політичних цілях. Як не дивно, пропаганда стала одним із найсильніших впливів на людей та невід'ємною частиною політики. [19]

Багато хто, вважає терміни “пропаганда” та “маніпуляція” однаковими, але це не відповідає правді. Завдяки пропаганді замовник має на меті добитись від вас реакції чи якоїсь поведінки: переробляти на виробництві, боротися за релігію або державу, підтримувати потрібну політичну силу. Може бути ще для того, як

мити руки перед обідом або ви не приймаєте ніяких наркотиків. Дивлячись на це, пропаганда може чудово показувати ваші потреби чи інтереси. Но, також це є не завжди нечесно і шкідливо для вас. А ще це не обов'язково має бути брехня. [11]

Цікаво те, що поширення чи нав’язування власної думки як діяльність зародилася задовго до листа Папи Римського. В античності, в часи жорстокої племінної війни, солдати старались стримувати ворогів, для того щоб зміцнити свій дух і самому переконати себе у власній перевазі. Особливі країни досягли стільки, що ми все ще не знаємо про їх агітаційні матеріали. Ми пов’язуємо американських індіанців із їх дитинством із намальованими лицями та їхніми криками. Вікінги спеціально заточували до гостроти собі передні зуби, бо така посмішка в бійці була дуже страшна. Рогаті шоломи - це також спобіс стримувати і домінувати психологічно проти ворога, але це вже не зовсім вікінги. Це колись було «модним» серед вандалів, а вікінгам це приписували літературознавці 19 століття.

Багато представників релігій удосконалювали пропагандистське мистецтво, наприклад: християнство, іслам, буддизм. І це робили для поширення серед людей своїх поглядів. Вони завжди показували неймовірні чудеса, здійснені їхніми провидцями та обіцяли людям довге і щасливе життя а також інші благословення, для тих хто зацікавиться їхньою вірою. Однак така пропаганда була зовсім не мирною. [8]

Маніпуляція - це передача інформації, що створює помилковий погляд на світ у свідомості людей; Показуючи "штучні потреби" (які вам справді не потрібні, але якими ви маніпулюєте, для вас це життєво важливо) діяти в потрібному вам напрямку. Маніпулятор добре знає ваші потреби та слабкі сторони, страхи та комплекси. Він знає, що і як потрібно сказати чи показати, щоб заохотити дії. Він знайде час і місце для цього найбільш ефективно. Насправді пропагандисти часто вдаються до маніпуляцій. Тому ці слова часто вважають синонімами. Перенесення інтересів у віртуальний простір підірвало

традиційне розуміння механізмів узгодження інтересів учасників інформаційних відносин. Як результат, руйнується існуюча межа між такими поняттями, як національна, регіональна та глобальна безпека, і, як наслідок, встановлення нових пріоритетів національної безпеки вимагає відповідного перероблення як систем безпеки, так і методологічних основ їх досліджень. [18]

Процес створення глобального інформаційного суспільства характеризується тенденціями формування єдиного інформаційного простору, який на сьогоднішній день має характеристики масштабної боротьби за масштаби свого впливу на суспільство. З розвитком комунікаційних технологій та розповсюдженням інформаційних ресурсів засоби масової інформації інших країн стають легкодоступними для внутрішньої аудиторії країни. Україна розташована на кордоні між Сходом та Заходом, що вимагає необхідності постійного просторового та часового зрушення стратегічних інтересів окремих держав та визначає поведінкові технології формальних лідерів політичних систем. Отже, іноземні ЗМІ є важливим елементом впливу на думку громадськості щодо процесів у світі та країні. [21]

Маніпулювання інформацією за допомогою різних інформаційних технологій та психологічних ефектів, особливо ЗМІ, стало масовим явищем у світі. Це стосується, зокрема, механізмів здійснення політичного впливу та досягнення політичних цілей. Слід зазначити, що в Україні тема маніпулятивних спецоперацій проти України в закордонних засобах масової інформації, за винятком звинувачень проти Російської Федерації, практично не вивчена, але це переважно газетні видання або телевізійні історії.

До проголошення незалежності України, тобто до 1991 року, питання інформаційної безпеки та боротьби з інформаційним маніпулюванням вчені та експерти вирішували виключно на основі боротьби між класами в рамках захисту ідеологічних переконань та прагнення СРСР. Після здобуття незалежності головна увага приділялася проблемам самовизначення, територіальної цілісності, мовної політики та політичної та економічної

незалежності нації. Інформаційна безпека згадувалася в контексті національної безпеки, але не мала чіткого визначення та формулювання, і тому вона не досліджувалася, хоча й згадувалася. Інформаційна безпека та залежність внутрішнього інформаційного простору від впливу зарубіжної інформації почали розглядатися лише у другій половині 1990-х. Основна увага приділялася інформаційному впливу східного сусіда - Російської Федерації - на Україну. Концепції інформаційної безпеки та маніпулювання інформацією в цей період розглядалися лише в контексті співіснування з Росією: спільні кордони, впровадження двомовності, політична незалежність у прийнятті рішень та національна ідея. На початку XX століття були розроблені методологічні підходи до вивчення інформаційної безпеки та впливу інформації. Інформаційна безпека вийшла на перший план із низкою вчених, які активно працювали над визначенням термінології та досліджували всілякі взаємозв'язки. [32]

Дезінформація – це підтягнутий до високого творчого рівня способу і принципу діяльності іноземної преси, це є один із методів зарубіжної пропаганди. Це показується у продажних журналістами при вилученні політичних фактів чи новин у соціально загострених повідомленнях, у спеціально переробленому тлумаченні структурного змісту головних суспільних подій.

Інформація і дезінформація розташовуються на інших рівнях однієї і тої же властивості, того зміна між ними найчастіше мають тільки умовний характер.

Поширення неправдивої інформації теж є тактикою терору. Мас-медіа - це могутні знаряддя війни. Якщо держава підтримує застосування тактик терору, то, як правило, воно в більшій чи меншій мірі контролює і засоби масової інформації. [23]

У колишньому СРСР і країнах, які перебували під його впливом, все ЗМІ перебували під контролем держави. Неможливо було сказати ні слова проти існуючого режиму. Система агентури і розвідки працювала настільки

злагоджено, що опозиційна ідея, висловлена навіть в інтимній обстановці, могла коштувати людині життя. [9]

Свобода слова і свобода інформації є ключовими поняттями демократичної ідеології, оскільки гарантують народовладдя як основу управління в державі. Контроль над ЗМІ невеликої кількості приватних компаній ставить під загрозу сам принцип демократії. Європейська комісія з прав людини визнала «надмірну концентрацію преси» порушенням прав, гарантованих статтею 19, і закликала держави запобігати подібним порушення.

Іноді буває неясно, де закінчуються правдиві відомості і починається дезінформація. Інформацію часто інтерпретують так, щоб вона відповідала нашому світогляду, впливала на нашу думку або приводила до конкретних результатів.

Щодо інтернету, то він був відносно вільний від політичного контролю і не уявляв комерційного інтересу. Величезна мережа обміну інформацією - незвичайний, інтригуючий противагу концентрованої економічної, політичної і соціальної влади, що надає безмежні варіанти для мобілізації культурної та політичної діяльності. У той же час сьогодні величезний вплив на Інтернет і контроль над ним має глобальний маркетинг, і напевно державні розвідувальні служби не упускають можливості долучитися до шпигують за нами міжнародним корпораціям і хакерам. [28]

Дезінформація пов'язана не тільки з джерелом брехні, неточної інформації і технологій. Інформаційний процес передбачає наявність як відправника, так і адресата. Всі ми цікавимося новинами - вони нас хвилюють, бентежать, здаються нам нудними або позбавляють надії. І якщо суспільство хоче вирішити проблему дезінформації і обговорити роль ЗМІ, то спочатку потрібно подивитися на те, як ми збираємо, сортуємо і використовуємо інформацію.

Мішень дезінформації - наші емоції, обмежена свідомість і нездатність відбирати інформацію, а також схильність вірити всьому, що найбільш відповідає нашому особистому і колективному досвіду, нашим емоційним перевагам. Ця тактика використовує наше бажання зберегти свої привілеї, заради яких ми готові погодитися з чим завгодно.

Дезінформація використовується для того, щоб звести наклеп на активістів і лідерів, дискредитувати громадські та політичні рухи, збуджуючи підозри і ненависть до окремих людей і груп, посилити лояльність, роз'ятрити старі рани і порушити спрагу помсти. [26]

РОЗДІЛ 2. СУЧАСНІ МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

2.1. Моніторинг інформаційного простору.

На сьогоднішній день в умовах сучасних глобальних, регіональних інформаційних протиборств, деструктивні комунікативні впливи, зіткнення різновекторних інформаційних національних інтересів, також поширення експансії і агресії, захист національного простору а також гарантування національної безпеки все частіше являються завданнями і пріоритетними і стратегічними у сучасних держав у системі глобальних інформаційних відносин.

Збереження державної інформаційної автономії і також сформувати ефективну систему захисту в сфері інформації наразі це актуальна проблема для нашої країни, яка часто є об’єктом зовнішнього інформаційного розповсюдження,

експлуатаційних пропагандистських технологій та інформаційного вторгнення руйнівного характеру.

Саме проблему інформаційного захисту, проблем безпеки національного інформаційного простору досліджували наразі багато науковців. Але у працях фахівців саме інформаційна безпека досліджувалась, радше, як невід'ємна складова національної безпеки. [1]

Проблеми визначення ключових інформаційних загроз, наразі залишилися поза увагою наукових працівників, вивчення їхніх джерел, дослідження технологій щодо ведення інформаційно-психологічних війн і операцій, а ще виявлення та обґрунтування методів протидії інформаційно-психологічним негативним впливам.

Аналіз переліку національних інтересів України в галузі інформації дозволив виявити інтереси, реалізація яких можлива в тій чи іншій формі лише за умов постійної координації, нагляду, управління операціями та інших функціонуючих компонентів (таблиця 1):

Аналіз списку національних інтересів

Таблиця 1

Витяг із переліку національних інтересів України в умовах інформаційної сфери	Для їхньої реалізації з точки зору корпоративного управління
Захист від руйнівної інформації та психологічних впливів	Реалізація вищезазначених положень передбачає їх виявлення та нейтралізацію до моменту, що призводить до негативних наслідків
Захист українського суспільства від агресивних наслідків деструктивної пропаганди	Забезпечує моніторинг інформаційного простору для виявлення загроз та прямих негативних наслідків та

	негайних заходів
Захист українського суспільства від агресивного інформаційного впливу, спрямованого на просування війни, розпалювання етнічної та релігійної ненависті, насильницьку зміну конституційного ладу або порушення суверенітету та територіальної цілісності України	Передбачає моніторинг інформаційного простору щодо виявлення загроз та безпосереднього негативного впливу, вжиття оперативних заходів реагування
Створення системи та механізмів захисту від негативних зовнішньо інформаційних психологічних впливів, зокрема пропагандистської	У світлі міжнародного права передбачає моніторинг інформаційного простору з метою виявлення загроз та негайних негативних наслідків та негайних заходів
Розвиток стратегічної системи зв'язку України	По суті це означає створення активної інформаційно-орієнтованої системи, що включає такі компоненти, як інформаційно-психологічні операції. Ця система втрачає свої властивості, коли немає ефективної підсистеми управління
Забезпечення вільного потоку інформації, якщо інше не встановлено законом	Дозволяє виявляти та реєструвати порушення вільного потоку інформації
Формування позитивного іміджу України у світі, передача міжнародної спільноти	Ключовий елемент у цьому

оперативної, достовірної та об'єктивної інформації про події в Україні	пункті «оперативної»
Розвиток системи іномовлення та забезпечення присутності українського голосового каналу в кабельних мережах та супутникових передачах за межами України	Потрібен незалежний моніторинг продуктивності та ефективності цієї системи
Розвиток та захист національної інформаційної інфраструктури	Потрібно забезпечити адекватний моніторинг реагування на загрози та спроби впливати на функціонування інфраструктури

Аналіз інформаційного простору в областях нашої держави здійснюється за допомогою Державного комітета телебачення та радіомовлення України, всі їхні результати оприлюднюються у мережі Інтернет та містять інформацію щодо діяльності обласних державних адміністрацій, які щоденно моніторять місцеві аудіовізуальні ЗМІ з метою виявлення матеріалів, які закликають до насильницької зміни і повалення конституційного ладу, посягання на територіальну цілісність, пропаганду війни, сепаратизму і тероризму, та реалізують заходи щодо припинення здійснення ретрансляції заборонених російських телеканалів на території областей. [27]

Щодо особистим керуванням інформаційного простору в мережі Інтернет, то детальне вивчення наукових джерел і зарубіжного досвіду дозволяє зробити висновки щодо методів керування простору в мережі Інтернет, до яких належать:

1. Блокування або заборона доступу до сайтів, що містять інформацію, яка порушує чинне в тій чи іншій країні законодавство

2. Фільтрування інформаційного потоку в місцях загального користування (інтернет-кафе, навчальні заклади, підприємства) – це блокує доступу до необхідної інформації на основі "чорних списків" – заблокування доступу до адресів, що містяться в списку (Китай, Російська Федерація) чи "білих списків" – дозволу доступу тільки до конкретних адрес (Північна Корея), а також за ключовими словами;
3. Відстеження активності інтернет-користувачів (Російська Федерація), перлюстрація повідомлень;
4. Авторизація користувачів при доступі в інтернет із застосуванням провайдерами програмних чи апаратних засобів (Білорусь, Алжир, Іран).

Одну з найдосконаліших систем контролю мережі Інтернет має Китай, яка включає як законодавчу базу, що формувалася поступово та у логічній послідовності, так і систему фільтрування трафіку. У цій країні жорсткіше здійснюється політична цензура, ніж блокування сайтів аморальної спрямованості. Регулятивна політика КНР здійснюється в трьох основних напрямах:

1. Регулювання всіх видів потокових відеосайтів (а деяких із них – у режимі реального часу), що можуть розміщувати контент, який би ніколи не вийшов на державному телебаченні;
2. Регулювання поширення відео у пірінгових (торент) мережах, що стосується порнографічних матеріалів;
3. Регулювання сайтів, які функціонують у межах філософії Веб 2.0 ("контент, що створюється користувачами"), – китайські YouTube-клони (www.tudou.com, www.youku.com, www.56.com). [30]

Незважаючи на відсутність точного правового контролю до самого поняття, процедури контролю інформаційного простору (переважно в мережі Інтернет), у статті 11 Закону України від 06.12.1991 № 1932-XII "Про оборону України" серед основних функцій Генерального штабу Збройних Сил України визначено участь в організації використання та контролю за повітряним,

водним і інформаційним простором держави, який здійснюється в особливий період. [34] Указом Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "За заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" передбачалося визначення механізму реалізації повноважень Генерального штабу Збройних Сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період. [35] Доцільно зазначити, що більшість положень цього Указу Президента України до сьогодні залишилися невиконаними.

Таким чином, натепер в Україні відсутній комплексний закон та відповідні підзаконні нормативно-правові акти щодо правового регулювання контролю інформаційного простору в мережі Інтернет, де чітко б визначалися: правовий статус суб'єктів контролю; зміст контрольних відносин; використання встановлених законом способів і методів контролю; правові норми щодо юридичної відповідальності контролюючих та підконтрольних суб'єктів. У такому аспекті доцільно розробити відповідні акти, якими б регулювалися види контролю інформаційного простору в мережі Інтернет, розмежовані за: контролюючими суб'єктами, об'єктами контролю, змістом та методами контролю, етапами (стадіями) контролю, а також за результатами і наслідками контрольної діяльності. Проте, як свідчить досвід Китаю, застосування державою методів контролю мережі Інтернет серйозно шкодить економіці країни, а технологічний сектор залишається без інновацій, такі самі наслідки можливі й в Україні. [22]

2.2. Система оцінки інформаційних загроз.

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до нанесення шкоди інтересам даних суб'єктів.

Класифікація загроз інформаційної безпеки.

Загроза інформаційної безпеки є набором умов і факторів, які представляють ризик порушення інформаційної безпеки.

Загроза інтересам суб'єктів щодо інформаційних відносин означає потенційне подія, процес або явище, яке, впливаючи на інформацію або інші компоненти інформаційної системи, може прямо або побічно завдати шкоди інтересам цих суб'єктів.

Класифікувати загрози інформаційній безпеці.

Загрози інформаційної безпеки можна класифікувати за різними критеріями:

1. Про аспекті захисту інформації від загроз:

А) Загрози конфіденційності (неприпустимий доступ до інформації). Загроза конфіденційності полягає в тому, що інформація стає відомою тим, хто не має доступу до неї. Це відбувається при доступі до деякої обмеженої інформації, що зберігається в комп'ютерній системі чи переданої з однієї системи в іншу. Термін «витік» використовується з міркувань конфіденційності. Такі загрози можуть бути викликані «людським фактором» (таким як ненавмисна передача привілеїв іншому користувачеві іншому користувачеві), несправностями програмного і апаратного забезпечення. Обмежена інформація включає державну таємницю (комерційна таємниця, особиста інформація, професійна таємниця: наркотики, адвокат, банківська справа, бізнес, нотаріальне страхування, розслідування і судова система, листування, телефонні дзвінки, пошта,

телеграф і інша інформація (секретна)). Характер винаходи, корисна модель або дизайн до офіційної публікації (ноу-хау і т. Д.)

Б) Загроза цілісності (незаконна зміна даних). Ризик порушення цілісності - це ризик, пов'язаний з ймовірністю зміни інформації, що зберігається в інформаційній системі. Порушення цілісності можуть бути викликані різними факторами - від навмисних дій персоналу до відмови обладнання.

В) Загроза доступності (вжиття заходів щодо запобігання або запобігання доступу до ресурсів інформаційної системи). Порушення доступу - це створення умов, при яких доступ до послуги або інформації або блокується, або дозволяється на певний період часу, щоб уникнути досягнення певних бізнес-цілей.

2. За місцем знаходження джерела загрози:

А) внутрішні (джерела загроз знаходяться в системі);

Б) зовнішні (джерела загрози знаходяться поза системою).

3. Стосовно заподіяної шкоди:

А) загальний (пошкодження всього охоронного об'єкта, значної шкоди);

Б) локальні (пошкодження окремих частин об'єкту, що охороняється);

В) приватний (який пошкоджує певні функції функції безпеки).

4. За ступенем впливу на інформаційну систему:

А) Пасивний (структура і зміст системи не змінюються)

Б) Активний (структура і зміст системи можуть відрізнятися)

5. За типом події:

А) Природний (об'єктивний) - викликається реакцією об'єктивних природних явищ або процесів на інформаційне середовище і не залежить від власної волі.

Б) Штучне (суб'єктивне) - викликано реакцією на інформаційну сферу у людини. Штучні загрози включають в себе:

- ненавмисні (випадкові) загрози, помилки співробітників або програмного забезпечення, несправності системи, несправності комп'ютерного обладнання і пристроїв зв'язку;

- умисні загрози неприпустиме втручання в інформацію, створення спеціалізованого програмного забезпечення для отримання несанкціонованого доступу, створення і поширення шкідливих програм.

Навмисні загрози викликані діями людини. Основні проблеми національної безпеки також пов'язані з умисними погрозами, оскільки вони є основною причиною крадіжок і злочинів. [14]

На думку експертів з безпеки, більше 65% збитків інформаційних ресурсів відбувається через ненавмисних помилок. Це одна з причин, щоб зосередитися на більш ефективної постачання систем комп'ютерної безпеки. З цієї причини Національний інститут стратегічних досліджень запропонував програму «Електронна Україна». Служби безпеки, які поширюють інформацію для громадськості, тепер по якоїсь причини уразливі для доступу до конфіденційної інформації.

Загрози є джерелами загроз інформаційної безпеки. Суб'єкти (особи), а також такі дії, як політичні конкуренти, корумповані чиновники, злочинці і адміністративні органи, також можуть бути джерелами загроз. У той же час джерела загроз виконують такі завдання: знання конфіденційної інформації, зміна особистої вигоди і знищення. [25]

РОЗДІЛ 3. МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВІД ЗОВНІШНІХ ПРОЯВІВ

3.1. Український інформаційний простір.

Історично склалося так, що інформаційний простір(ІП) володіє національно-специфічними способами побудови. Тому в контексті нашої держави застосовується категорія Національного інформаційного простору України. Законодавче визначення його обґрунтовується так: Національний інформаційний простір України — сфера, де виконуються процеси і яка входить до юрисдикції України. Відзначимо, що існування державного ІП часто є особливою (але безпомилковою) ознакою національної ідентифікації. Основні характеристики:

1. Територія, де безпосередньо, чи опосередковано поширюється інформація. Межі інформаційного застосування мають збігатися з її державними кордонами. Де діють усі складові ІП: радіо, преса, телебачення;
2. Структурованість ІП.

ІП є утворенням, що розширюється та конкретизується згідно із розвитком нашого суспільства. Це обмін повідомленнями структурами інформаційного простору. До ЗМІ, і до інформаційних потоків можна зарахувати такі сфери людської зайнятості, як туризм, міграцію, освітні, культурні обміни, конференції, змагання та інші. ІП представляють собою циркуляцію інформації, окреслюють напрями і форми, які спричиняють зміни на різних рівнях і в різних системах, а саме: зміни в природі, ресурсах, управлінні, культурних і національних системах. Отже, узагальнимо властивості національного інформаційного простору: де йдеться мова конкретно про ІП країни, де його робота ототожнюються з кордонами держави. [52] На всій території конкретної держави базуються ЗМІ, що інформують, аргументують і повідомляють, створюють про щось уявлення. В той час, особисті потоки інформації, де інтенсивність і циркуляція системами інформаційного простору межує із сферою управління національною політикою й залежить від людини

інформатора. Таким чином, наші мас-медіа та російські часто висвітлюють одні і ті ж події по-різному. У західних ЗМІ дають власну оцінку подіям. Ця ситуація обумовлена тим, що національні мас-медіа мають обґрунтовувати інтереси національних країн, а ці інтереси, звичайно ж, не однакові. Підсумовуючи "Національного інформаційного простору" — це досить тяжкий і потужний комплекс. До складу якого входять його суб'єкти, все матеріально-технічне обладнання, а також вся інтелектуально інформаційна власність. [41]

Традиційні ЗМІ беруть участь у формуванні українського національного інформаційного простору, і навіть сьогодні важливу роль відіграють новітні електронні ЗМІ, серед яких найважливіші - сучасні дослідники.

1. Кабельне телебачення, де телевізори певної області (регіону) підключені до певного радіомовного центру через кабельне з'єднання. Кабельне телебачення в основному призначене для розповсюдження розважальних програм, але може мати і суспільно-політичний характер.

2. Відеомагнітофони - пристрої для запису та відтворення аудіовізуальних програм та інших журналістських матеріалів. Інформація для них поширюється на касетах і має в основному культурний та розважальний характер, що не заважає ЗМІ поширювати всі інші види інформації. Швидке зростання продажів відеореєстраторів у світі почалося в 1983 році. З нами це в дев'яностих роках. Відеореєстратори часто використовуються в рекламних цілях.

3. Телефонні конференції (телевізійні програми, телефони тощо) - встановлення супутникового зв'язку між двома точками земної кулі, незалежно від відстані та регіону, для спілкування між групами людей, для участі в обговоренні важливих соціальних питань тощо.

В даний час майже кожен новинний перегляд може використовувати телевізійний прийом. Це можна обговорити, коли прямий репортер повідомляє

або коментує подію на своєму телеканалі. Це явище стало поширеним і всюдисущим у нашому інформаційному просторі.

Останнім часом термін «конференційний дзвінок» вживається в іншому значенні. Це назва колективного методу спілкування в Інтернеті. У цьому сенсі телеконференція - це свого роду «дошка оголошень», де кожен охочий може прочитати необхідну інформацію або надіслати повідомлення зацікавленим сторонам.

4. Електронна пошта - це спосіб надсилання кореспонденції між двома віддаленими місцями через міжнародну систему комп'ютерного зв'язку. Дозволяє зберігати повідомлення в пам'яті комп’ютера, поки абонент не прочитає текст і не відправить команду знищити його. Цей спосіб передачі інформації вигідний не тільки для швидкості прийому повідомлень, але і для того, що синхронізація учасників процесу спілкування не потрібна.

5. Електронні таблиці - це великі комп’ютери, які зберігають різну інформацію, доступну для підключених до них абонентів через комп'ютерну систему. Банківські (економічні, професійні тощо) Дані генеруються шляхом зберігання певних типів інформації в пам'яті комп'ютера, де вона зберігається і поширюється на вимогу осіб або організацій. [42]

6. Лазерний прес - це випуск газети чи журналу (або іншої друкованої інформації) за допомогою лазерних принтерів. Він працює дуже швидко і друкує тексти зі швидкістю копіювання. Оскільки прискорення виробництва друкованої журналістики за допомогою лазерного принтера значно скоротило час, необхідний для передачі інформації від джерела до споживача, це також значно вплинуло на стан інформаційного простору в напрямку його активації для повного задоволення інформаційних потреб Населення. [13]

Особливе місце в сучасному світі поклало інформаційний простір комп’ютерної мережі Інтернет. Насправді, деякі новітні ЗМІ (телефонні конференції, електронна пошта, відео, газети) працюють лише завдяки всесвітньо відомій системі комп'ютерних комунікацій. Як результат, вони розмовляють окремо через Інтернет, і це зазвичай сприймається як новий вид журналістики. Корисно висловити думку авторів підручника «Основи масової інформаційної діяльності».

"Пишуть вони, за допомогою всесвітньої павутини, світ переживає народження нового типу ЗМІ, яке займе особливе місце у 21 столітті серед традиційних засобів масової інформації, таких як телебачення, преса, радіо та розвиток". Технологія пропонує безпрецедентні можливості. Інтернет - найбільша у світі комп'ютерна мережа, створена для збору, обміну та швидкого розповсюдження інформації. [24]

3.2. Існуючі проблеми захисту інформаційного простору.

Поки в Україні не існує єдиного органу, який би мав єдине право регулювати роботу телеканалів. Тому юридичне забезпечення інформаційної сфери потребує значного вдосконалення та орієнтації на найкращі досягнення демократичних країн. Варто зазначити, що таке ставлення органів державної влади до інформаційної політики потрібно якнайшвидше змінити.

Ми також не повинні забувати, що ми живемо у світі, сформованому процесами глобалізації, геополітичних перетворень та віртуалізації інформаційного простору. З часу здобуття Україною незалежності зовнішня інформаційна активність зросла в десятки разів. Чинне законодавство відкриває широким можливостям осіб без громадянства та громадян інших країн для створення засобів масової інформації в нашій країні. Виконавчій владі все ще позбавлено права здійснювати регуляторні функції в цій галузі. Зокрема, немає реальних

важелів регулювання мовної ситуації. Ось чому російськомовна преса в Україні є найбільшою частиною загальної кількості друкованих ЗМІ. [6]

На жаль, на тлі втручання іноземних ЗМІ виникає недовіра до вітчизняного продукту. Це неприпустимо, оскільки держава повинна забезпечити суверенітет національного інформаційного простору. Фактично наш інформаційний простір не був захищений від зовнішньої інформації. Сьогодні це одна з найважливіших стратегічних загроз подальшому всебічному розвитку суспільства та держави. Тому необхідно, щоб Україна була представлена за кордоном. Необхідні двосторонні міжурядові угоди, зокрема з сусідніми країнами, щодо транскордонних радіо- і телевізійних передач, а також необхідно поглибити співпрацю між українськими та зарубіжними ЗМІ. У багатьох випадках необхідно встановити договірну базу з зарубіжними країнами і, перш за все, з Росією (яка переважно представлена в українському інформаційному просторі) щодо розповсюдження і, в деяких випадках, офіційного перерозподілу інформаційного простору. Цей підхід до управління інформацією зараз застосовується, зокрема, в Італії, Великобританії, США, Грузії, Австралії, Канаді та інших країнах. [17]

Гібридний інформаційно-медійний характер російської агресії вже станом на 2014 рік повною мірою виявив неприпустимо слабкі позиції України в забезпеченні власної інформаційної безпеки, зокрема:

1. Критична кількість медіа, які перебуваючи в інформаційному просторі України, порушують її закони та загрожують її національній безпеці;

2. Недостатньо захищений від неліцензованих трансляцій вітчизняний телерадіопростір, стабільне технічне покриття якого й досі значно меншим за територію держави (навіть без урахування окупованих районів);

3. Неадекватна вимогам часу система норматив-но-правового та інституційного забезпечення розвитку інформаційної сфери, зокрема, відсутність концептуальної державної політики інформаційної безпеки;

4. Недостатньо фахова, слабко організована й надто залежна від власників ЗМІ журналістська спільнота;

Брак дієвих інституцій та механізмів оперативного реагування на інформаційні загрози як технічного, так і психологічного характеру. Все це свідчить, що станом на кінець 2013 року в Україні практично не було цілісної системи захисту національного медійного і, зокрема, теле радіо інформаційного простору. Серед іншого, це призводило до створення умов для масової та безперешкодної трансляції аудіовізуального продукту, зміст якого прямо порушував законодавство України у сфері інформаційної безпеки. [38]

3.3. Можливі механізми та рекомендації щодо захисту інформаційного простору від зовнішніх проявів.

Проблема захисту інформаційного простору України є досить актуальною на сьогоднішній день, українські вчені провели власне дослідження і не один раз пропонували шляхи вирішення та заходи, які були б спрямовані на ефективну реалізацію державної політики в інформаційному просторі. На думку Н. Войцих, обов’язково потрібно зробити такі головні умови:

1. В системі органів державної влади повинна бути сформована одна і єдина структура, завданням якої є проведення і контроль за державною інформаційною політикою. Ця структура повинна має охопити всі підрозділи державної влади і описуватись як спеціалізовані органи влади в цій темі, що забезпечують регулювання інформаційної сфери, так і підрозділу в інших органах влади, відповідальні за інформаційні аспекти діяльності в сфері їх компетенції;

2. Державне управління інформаційною сферою має бути планомірно забезпечене фінансовими і матеріальними ресурсами за рахунок бюджетного фінансування — природно, виходячи з реальних можливостей держави за статтею витрат на державне керування;

3. Застосування національної інформаційної політики має проводитись разом із єдиним центром і тільки на рівні вищого керівництва країни при обов'язковій відповідальності одного з вищих посадових осіб держави за вирішення конкретного завдання [7].

Слід зазначити, що запровадження визначених заходів тільки сприятиме підвищенню державної політики в інформаційному просторі України. Аналіз показує, на даний момент ніяка з означених вимог у саму практику не впроваджена. Така позиція, щодо регулювання інформаційної сфери сприяє негативні наслідки, які відображаються на можливості держави надавати належну, аргументовану відсіч провокаціям в інформаційному просторі. Отже, стан національного інформаційного простору України на даний момент є незадовільним.

Зовнішня агресія, сильна антиукраїнська пропаганда і пов'язані з нею проблеми національної безпеки, особливо на рівні інформації та психології, спонукали державу приділяти особливу увагу питанням інформаційної безпеки Безліч соціальних, економічних і політичних проблем, які створили ці проблеми, хоча і є актуальними як мінімум на 15 років, нарешті увійшли в суспільну дискусію і політичний порядок денний. [39]

Серед досягнень державної політики:

Через низку обмежувальних урядових рішень громадяни рідше використовують російський пропагандистський інформаційний продукт.

1. Ініціювати процеси для створення стійких механізмів, які полегшили б виробництво великих обсягів вітчизняної кінопродукції;

2. Є певні досягнення в забезпеченні українського телевізійного висвітлення прикордонних, окупаційних і прикордонних територій.

3. Перші кроки були зроблені для забезпечення прозорості власності ЗМІ в Україні. [37]

Зазначу, що прогресивний характер та доцільність державних заходів, котрі спричинили до заявлених результатів це заборона (російського кіно, телеканалів, закон про прозорість власник ЗМІ), на жаль, цього недостатньо щоб були відчутні зміни. Ми можемо бачити це як старт правильних дії в вирішенні проблем. Фактична дія нового законодавства на єдину прозорість права власності на ЗМІ залежить від дальшого покращення законодавчої бази та її застосування. Підтримка кінотеатру від держави знаходиться лише в стадії проекту, і наслідки цієї підтримки можуть не бути реалізованими протягом деяких років. Але, потрібні не лише кінофільми, а ще й інші інформаційні продукти, де Україна втрачає конкуренцію, необхідна державна підтримка: ЗМІ і інтернету. Лише стосовно першого пункту (заборони на російські телеканали та кінопродукти) можна сказати за їх дійний вплив на формат споживання інформації громадян.

Проблеми, які ми так і не змогли вирішити:

1. Відсутність узгодженої політики уряду та запланованого підходу до ІБ;

2. Відсутність ефективного підрозділа який би реагував на інформаційно-психологічні загрози та належне управління в цій галузі.

Держава не мала доктринального документа, котрий послужив би основою для створення системи захисту інформації. Цей наявний проект концепції захисту інформації не може бути надійним шляхом вирішення проблеми і він також не може стати таким документом. Також не було ефективних урядових механізмів для моніторингу загроз, розробки та реалізації рішень щодо інформаційної безпеки та регулювання впливу різних підрозділів у цьому процесі.

Міністерство інформаційної політики тільки є допоміжним елементом непослідовної системи та повноважень. Таким чином, збільшення спроможності держави правильно реагувати і діяти на проблеми національної безпеки на рівні інформації не відбулося. [12]

Проблеми, які залишиються без уваги уряду:

1. Олігархічне медіа-середовище в Україні;
2. Низька медіаграмотність людей.

Також, не було вжито жодних кроків для спроби вирішення цих проблем.

Не було досягнуто ніякого прогресу у проблемах, пов'язаних з інформаційним простором громадян України, які на даний момент проживають на окупованих територіях. Існуючі урядові рішення щодо інформаційної безпеки можуть впливати лише на територію, яку контролює український уряд. [32]
Проаналізувавши всю інформацію про поточний стан та існуючі проблеми інформаційного простору, я склав таблицю, що визначає проблеми та представляє можливості рішень:

Існуючі проблеми та шлях її вирішення

Таблиця 2

Проблема	**Шляхи вирішення**
Недовіра до телебачення збоку громадян України	Створення нового державного канала, який також буде транслюватися у Донецькій та Луганській областях.
Психологічні проблеми і процеси всередині українського суспільства, не сумісні з українською державністю та демократичним ладом	Організація підтримки власного виробника ІП, покращення місцевих ЗМІ, впровадження однакових умов і шляхів для імпорту інформації з Росії та інших країн
Олігархічне медіа-середовище, і	Посилити або створити нову

власність ЗМІ в державі нечітка, що дозволяє проросійським компаніям пропагувати пропагандистський дискурс в Україні в шкоду нашим національним інтересам	відповідальну структуру, яка буде займатись моніторингом і аналізувати загрози та буде формулювати рішення щодо політики на основі цих спостережень
Громадяни нашої держави мають доступ до російського телебачення через супутник та інтернет На не підконтрольних територіях поширюється аналоговий і цифровий широкомовний ефірний сигнал російського телебачення	Подання позову про те, що ці російські телеканали не сумісні із законодавством України та Європейською конвенцією про транскордонне телебачення та що їх передача на території України заборонена.
Національна рада з питань телебачення і радіомовлення й Державне агентство України з питань кіно	Ці недоліки слід враховувати для дальнішого покращення законодавчої бази. Також, важливо створити штрафну процедуру щодо порушення цього закону, яку повинен зробити Держкіно. У разі виявлення телерадіомовленнями доказів порушень закону Національна рада повинна надати відповідну інформацію Державному кінотеатру. У той же час, тільки Держкіно має дозвіл накладати санкції
Транслювання російського кінопродукту	Мінімізувати час в ефірі. Забезпечити, щоб було створено достатньо вітчизняного контенту, щоб заповнити вакуум замість забороненої російської інформації.

	Крім того, це не означає, що громадянам України не дозволяється отримати доступ до забороненої кінопродукції повністю, оскільки вона залишається безпосередньо в на ефірах російських телеканалів та в Інтернеті

Найважливішою безпосередньою проблемою були і є соціально-психологічні процеси в українському суспільстві, несумісні з нашою демократичною системою. Соціологічні дані, що свідчать про те, що погляди були і залишаються поширеними в нашому суспільстві, засновані на світосприйнятті через призму негативних факторів і стереотипів які несумісні з демократичним розвитком, єдністю суспільства та повним демократичним діалогом. [43]

Слід зазначити, що інформаційний вплив Росії не був би таким ефективним без поєднання трьох інших факторів:

1. Невдача нашої національної політики ідентичності;
2. Російський стратегічний підхід до впровадження інформаційно-психологічних наслідків в нашій державі за останні 15 років
3. Низька медіаграмотність та культура споживання ЗМІ в Україні.

Слід також зазначити, що російські мовники зникли лише з кабельних мереж та радіопрограм (тобто більше не поширюються через ретранслятори в зоні, контрольованій українським урядом), але громадяни все ще мають доступ до російського телебачення через супутник та Інтернет. Крім того, аналоговий та цифровий мовний сигнал російського телебачення поширюється на прикордонні райони з Росією та Молдовою та на прифронтові зони. Так, за даними хроніки та КМІС, 31% населення південних та східних регіонів мали доступ до російських телеканалів. [50]

Ще одним кроком до зменшення частки російської пропагандистської продукції в структурі споживання вітчизняних ЗМІ став Закон про внесення змін до деяких законів України про захист інформаційного телебачення і радіопростору, прийнятих Верховною Радою в Україні 5 лютого (вступив в силу 4 червня) 2015 року. [36]

Цей закон фактично забороняє:

1. Поширення та демонстрацію кіно в Україні, які демонструють популяризацію чи пропаганду влади держави-агресора (Російська Федерація) та їх окремі дії, а також добрий імідж робітників Росії, робітників органів державної безпеки Радянського Союзу. Виправдовують чи визнають окупацію території України після 1 серпня 1991 року як законну;
2. Трансляцію (екранізація каналів мовлення) фільмів, вироблених 1 січня 2014 року особами Росії;
3. Трансляція телепрограм, що транслюються після 1 серпня 1991 р., Які містять популяризацію чи пропаганду Росії і також її окремі дії та обґрунтовують законність визнання окупації території України;

Тобто закон забороняє будь-який пропагандистський телевізійний продукт (як фільми, так і телевізійні програми) та будь-які фільми російського походження, зняті за останні два роки. Державне кіноагентство має право відмовити у видачі прокатних посвідчень або скасувати будь-які видані посвідченя для всіх фільмів, що підпадають під дію закону. [33]

Тож можна зробити висновок, що сьогодні існує багато проблем, які потрібно вирішувати, саме в інформаційному просторі.

ВИСНОВКИ

Проаналізувавши більшість важливих для України проблем в області інформаційного простору, ми можемо зробити висновок, що в даний час ця область потребує значних змін і інновацій.

На жаль, в контексті втручань іноземних ЗМІ існує недовіра до внутрішнього продукту. Це неприпустимо, оскільки держава повинна виступати гарантом суверенітету національного інформаційного простору. Насправді наш інформаційний простір не захищений від зовнішньої інформації. Сьогодні це одна з найважливіших стратегічних загроз подальшому всебічному розвитку суспільства і держави. Отже, необхідно, щоб Україна була інформативно представлена за кордоном. Нам потрібні двосторонні міжурядові угоди, особливо з сусідніми країнами, про транскордонні радіо та телемовлення, і співпраця між українськими та зарубіжними ЗМІ має покращуватись. У багатьох випадках необхідно встановити договірну основу із зарубіжними країнами і, перш за все, з Росією (яка переважно представлена в українському інформаційному просторі) відповідно до розподілу і, в деяких випадках, офіційним перерозподілом інформаційного простору. Цей підхід до

управління інформацією в даний час застосовується, зокрема, в Італії, Великобританії, США, Грузії, Австралії, Канаді та інших країнах.

На мій погляд, існує гостра необхідність у розвитку і вдосконаленні української системи національної безпеки та інформаційної безпеки: моніторинг загроз інформаційній безпеці України як усередині країни, так і на міжнародному рівні; Збереження національних інтересів, цілей і цінностей України в глобальному інформаційному просторі і системи протидії цим загрозам.

На жаль, національний інформаційний простір України схильний до значних загроз, викликів, які ставлять під загрозу функціонування держави, його політичний та економічний розвиток і його інтеграцію в європейські і євроатлантичні структури. Загроза національній безпеці України в інформаційному секторі являє собою сукупність умов і факторів, що становлять загрозу життєво важливим інтересам держави, суспільства і громадськості, оскільки існує також можливість негативного інформаційного впливу на проінформованість і поведінку громадян.

Як правило, питання регулювання (моніторингу, контролю) інформаційного простору викликають бурхливі дискусії в масовій свідомості і сприймаються громадянами як посягання на сферу їх прав і можливостей. Визнавши ці попередження як виправдані, давайте зосередимося на одному аспекті, який, на мій погляд, піднімає питання про роль держави в інституціоналізації інформаційного середовища від категоріальної до дискусійної області. Аргументом для державного регулювання інформаційної діяльності є, зокрема, впровадження, підтримка і подальший розвиток стандартів. Останні забезпечують стабільність і надійність інформаційних систем і довіряють їм. І хоча компанії в масштабах Apple, Google і Facebook намагаються впровадити свої власні стандарти безпеки, звітності, аутентифікації і, можливо, навіть

монетарні стандарти, держава може дистанціюватися від цих систем з невеликими втратами.

Ефективність структури моніторингу багато в чому полягає від якості її конструкції, від розробки технології та її створення. Очевидно, що неможливо створити єдиний стандарт для проектування або проектування систем моніторингу для різних критеріїв класифікації. Тому технології створення локальних, простих і розподілених систем моніторингу не можуть бути однаковими, так як вони різняться по своїм функціям, завданням і цілям. Побудова системи моніторингу має творчий характер. У той же час існують загальні вимоги до проектування систем моніторингу, які повинні дотримуватися при побудові конкретної системи.

Загроза інформаційної безпеки - сукупність факторів та умов, як погрожують порушенням інформаційної безпеки.

Загроза інтересам суб'єктів інформаційних відносин розуміється як потенційний процес, явище або подія, які, впливаючи на інформацію чи інші другі компоненти інформаційної системи, прямо або побічно завдає шкоди інтересам цих суб'єктів.

Актуальність теми безперечна і вимагає ретельного розслідування. Перспективи подальших наукових досліджень: аналіз закордонного досвіду боротьби з пропагандистсько-маніпулятивним інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ананьїн В.О., Пучков О.О. Інформаційна безпека як складова національної безпеки України / В.О. Ананьїн, О.О. Пучков / Гілея: науковий вісник. – 2014. – Вип. 85. – 195–198 с.
2. Біловус Л. Український інформаційний простір: сьогодення та перспективи / Л. Біловус [Електронний ресурс]. – Режим доступу : http:// ijimv.knukim.edu.ua/zbirnyk/1_1/bilovus_l_i_ ukrayinskyy_informatsiynyy_prostir.pdf.
3. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm
4. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія / О. Бусол [Електронний ресурс]. – Режим доступу : http://nbuviap.gov.ua/ index.php? option=com_content&view=article& id=2961:osnovni-risi-kontrolyu-za-

natsionalniminformatsijnim-prostorom-korolivstva-velikabritaniya&catid=8&Itemid=350.

5. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь : ВТФ “Перун”, 2005. – 1728 с.
6. Воронин А. Нелинейная схема компромиссов в многокритериальных задачах / А. Воронин. // Artificial Intelligence and Decision Making. International Book Series “Information Science & Computing”. – 2008. – № 7. – 7985 с.
7. Воронин А. Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации / А. Воронин, Ю. Зиатдинов. // Кибернетика и системный анализ. – 2009. – № 4. –106–114 с.
8. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. – Режим доступу: http://www.visnyk.academy. gov.ua/wpcontent/uploads/2015/04/20.pdf
9. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: http://www.osvita. mediasapiens.ua/material/34281
10. Грищук Р. Основи кібернетичної безпеки / Р. Грищук, Ю. Даник. – Житомир : ЖНАЕУ, 2016. – 636 с.
11. Грищук Р. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень, 1st ed / Р. Грищук. – Житомир : Рута, 2010. – 280 с.
12. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/ show/514/2009
13. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: http://www.mego.info/матеріал/23-захист-інформаційноїбезпеки-як-функція-держави
14. Ільницька Уляна Інформаційна Безпеки України: Сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним

впливам. / Уляна Ільницька – Національний університет “Львівська політехніка”

15. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: http://www.w1 . c1.rada.gov.ua/pls/zweb2/webproc4_1
16. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України [Текст] : монографія / Б. А. Кормич. – Одеса : Юридична література, 2007.– 471 с.
17. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К. : КНТ, 2006.
18. Ліхтман Б. Правительства берут интернет под контроль / Б. Лихтман, А. Сидельников [Електронний ресурс]. – Режим доступу : http:// www.infosecurity.ru/_gazeta/content/091225/art2. shtml.
19. Манойло А. Государственная информационная политика в особых условиях: монография / А. Манойло. – М. : МИФИ, 2003. – 388 с.
20. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: http://www.dsaua.org/index. php? option=com_content&view=article&id=198%3A2014-0813-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90&lang=uk;
21. Медвідь Ф. Інформаційна безпека України: виклики та загрози [Електронний ресурс] / Ф. Медвідь. – Режим доступу: http://www.nato.ru. if.ua/journal/2009-2-28.pdf.
22. Молодецька К. Соціальні інтернет-сервіси як суб’єкт інформаційної безпеки держави / К. Молодецька. // Information technology and security. – 2016. – № 1. –13–20 с.
23. Молодецька К. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернетсервісах / К. Молодецька. // Проблеми інформаційних технологій. – 2016. – № 20. – 84–93 с.

24. Молодецька К. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. Молодецька // Защита информации. – 2016. – № 23. –75–87 с.
25. Молодецька-Гринчук К. Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. Молодецька-Гринчук. // Актуальні питання забезпечення кібербезпеки та захисту інформації. – 2017. – 121–122 с.
26. Молодецька-Гринчук К. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. Молодецька-Гринчук. // Інформаційна безпека. – 2016. – № 24. – 80–92 с.
27. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. / К. Молодецька-Гринчук. // Інформаційна безпека [Електронний ресурс]. – Режим доступу: http://atbp.onaft.edu.ua/
28. Молодецька-Гринчук К. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. Молодецька-Гринчук. // Інформаційна безпека. – 2017. – № 26. – 104–110 с.
29. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: http://www.ua.textreferat.com/referat-7471.html
30. Онищенко О. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства / О. Онищенко, В. Горовий, В. Попик. – Київ : НАН України, Нац. б-ка України ім. В. І. Вернадського, 2014. – 295 с.
31. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222
32. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2015. – 497 с.
33. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України Рішення Ради

національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14.

34. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – 351 с. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – 116 с.
35. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19 [Електронний ресурс]. – Режим доступу : http:// zakon0.rada.gov.ua/laws/show/2163-viii.
36. Про реалізацію і моніторинг ефективності персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Проект Постанови Кабінету Міністрів України [Електронний ресурс]. – Режим доступу: http://195.78.68.84/dsszzi/ control/uk/publish/article? showHidden=1&art_ id=280657&cat_id=38837&ctime=1503913672346.
37. Пузиренко О. Математична модель загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення / О. Пузиренко // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – № 3. – 129–133 с.
38. Російська гібридна війна: в Литві запустили "фейк" про згвалтування школярки солдатами бундесверу, щоб підірвати довіру до НАТО [Електронний ресурс]. – Режим доступа: http://ua.censor.net.ua/news/428466/rosiyiska_gibrydna_viyina_v_lytvi_zapustyly_feyik_pro_zvaltuvannya_shkolyarky_soldatamy_bundesveru_schob. – Загл. с экрана.
39. Російський сценарій. Усе, що потрібно знати про тотальне стеження за інтернет-користувачами в Україні [Електронний ресурс]. – Режим доступу : https://nv.ua/ukr/techno/it-industry/ rosijskij-stsenarij-use-shcho-potribno-znati-prototalne-stezhennja-za-internet-koristuvachami-vukrajini-2454611.html.

40. Семенов А. Захист національного інформаційного простору Великої Британії / А. Семенов // Матеріали міжнародної конференції «Політична праксеологія: безпека, технології, комунікації» / за ред. В. Бебика. – Київ : ВАПН, 2016. – 117 с.
41. Толубка. В. Б. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник – К. : НАОУ, 2004. – 315 с.
42. Фінансова енциклопедія / О. П. Орлюк, Л. К. Воронова, І. Б. Заверуха [та ін.] ; за заг. ред. О. П. Орлюк. – К. : Юрінком Інтер, 2008. – 472 с.
43. "Фридом Хаус" опасается, что в Украине может усилиться цензура в интернете [Електронний ресурс]. – Режим доступу : https://strana.ua/ news/127317-freedom-house-opasaetsja-chto-vukraine-mozhet-usilitsja-tsenzura-v-internete.html.
44. Хмелевський Р. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р. Хмелевський. // Сучасний захист інформації. – 2016. – № 4. – 65–70 с.
45. Чайка І.Ю. Інформаційна єдність світової спільноти: теоретико-методологічний аналіз: дис. … док. філос. наук: 09.00.03 / Чайка Ірина Юріївна. – К., 2015. – 448 с.
46. Черниш В. Методика оцінки інформаційних ризиків з використанням методу аналізу ієрархій / В. Черниш. // Радіоелектронні і комп'ютерні системи. – 2012. – № 1. – 46–50 с.
47. Ягодзізнський С. М. Державне регулювання та моніторинг інформаційного простору: соціокультурний аспект / С. М. Ягодзінський доцент кафедри філософії Національного авіаційного університету, доктор філософських наук, доцент.
48. Cybersecurity Engineering | The CERT Division [Electronic resource]. – Access mode: http://www.cert.org/cybersecurity-engineering/ – Title from the screen.
49. Einsatz in Litauen: Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr – SPIEGEL ONLINE – Politik [Electronic resource]. –

Access mode: http://www.spiegel.de/politik/ausland/bundeswehr-fake-news-attackegegen-deutsche-soldaten-in-litauen-a-1134925.html. – Title from the screen.

50. M. Fuller. First Software Studies Workshop [Електронний ресурс] /
51. M. Fuller. – Режим доступу: http://pzwart.wdka.hro. nl/mdr/seminars2.
52. NCSI – National Cyber Security Index [Electronic resource]. – Access mode: http://ncsi.ega.ee – Title from the screen.