незнайомого» об'єкту є аналогом процедури розпізнавання (або впізнавання, коли мова йде про здатність людини).

Використання такої системи дозволяє майже вилучити людський фактор з процедури визначення вразливостей об'єкту. Експерт-людина залишається виключно на етапі збору даних про об'єкт і призначений для складання (бажано якнайбільш об'єктивних) даних, що описують його за такими фрагментами: властивості інформації що циркулює на об'єкті, опис поверхового плану, структуру системи технічного забезпечення, опис прилеглої території, тощо.

Рис. 1 ілюструє не структуру АП, а лише сенс алгоритму процедури користування БД як АП.

Заповнення БД, котра будується на базі АП, часто називають навчанням. Тоді говорять про *АП з навчанням*. Існує декілька відомих алгоритмів навчання. Але, інтуїтивно є природним намагання вилучити обмеження щодо кінцевості списку параметрів та вразливостей. Якщо формувати саме такого проектувальника, то постійне накопичення в БД все більшої кількості нових даних від нових спроектованих об'єктів починає з часом впливати на результати подальшого проектування все з більшою вагою.

Тобто поступово реалізується тактика «забування», згідно з якою накопичення усе більшої кількості нових пред'явлень об'єктів для навчання трансформує БД та взагалі АП так, що старі образи, тобто такі що зустрічаються усе рідше, поступово зникають. Процедурно це виглядає як повільне зменшення ваги зв'язків між вхідною та вихідною БД для окремих комбінацій параметрів об'єкту (образів об'єкту). Система проектування набуває властивості поступової автоматичної адаптації до нових видів об'єктів, нових умов їх існування, нових видів вразливостей. Тобто, в процесі життєдіяльності такий автоматизований проектант залишається відкритим до подальшого «донавчання», тобто розвитку. Він «пам'ятає» історію великої кількості діючих об'єктів і доповнюється властивостями нових об'єктів, котрі він проектує. Саме ці властивості і забезпечують властивості системи автоматичного проектування КСЗІ у вигляді адаптації до умов існування (зміна загальної направленості у методології ЗІ, методичної документації, законодавства, тощо), незалежність від експертів на етапі життєвого циклу, об'єктивну дієвість проектування за рахунок користування БД діючих об'єктів.

IV Висновок

Визначено, що БД проектів КСЗІ ОЗ є структурованою, з спеціальною реалізацією, з закритою спеціалізованою системою керування, реляційна – з ненормалізованою схемою БД, близькою до DKNF. Це означає, що БД КСЗІ є дійсно специфічною і не вкладається повною мірою у будь-яку БД відомого типу за існуючими класифікаторами.

Автоматизація проектування КСЗІ є неможливою без створення такої БД або адаптації деякої існуючої БД до стану, котрий здатний забезпечити зазначені вище властивості. Саме таке завдання наразі вирішується спеціалістами КПІ на кафедрі «Фізико-технічних засобів захисту інформації» факультету «Інформаційної безпеки».

*Список використаної літератури**: 1.** ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології // Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій. **2.** ДСТУ 3396.1-96. Захист інформації // Технічний захист інформації. Порядок проведення робіт. **3.** Луценко В. М. Визначення уразливості об'єктів інформаційної діяльності як складова порядку розробки систем захисту інформації / Луценко В. М., Худяков В. О. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. .-К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. Вип. 2 (21) с. 49–55. **4.** Герасименко В. А. Защита информации в автоматизированных системах обработки даннях / Кн. 1 – М.: Энергоатомиздат, 1994 – 400 с. **5.** IT Baseline Protection Manual. Електронний ресурс: http://www.bsi.bund.de/gshb/English/t/t1000.htm на термін 04.2010 р. **6.** ГОСТ Р ИСО МЭК ТО 10032-2007.*

Віталій Носов, Олександр Манжай
Харківський національний університет внутрішніх справ

УДК 65.012.8+34

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ В УКРАЇНІ

Анотація: **Проаналізовано зміст та структуру інформаційного протиборства, наведено визначення ключових понять у даній сфері, визначено характерні риси та мету інформаційної війни. На підставі**

вивчення літературних джерел та аналітичного матеріалу запропоновано окремі заходи протидії інформаційній війні та інформаційно-психологічному впливу. Наведено конкретні приклади спроб інформаційного впливу, розглянуто структуру відповідних повідомлень та методику їх аналізу. Запропоновано створити центр реагування та проведення спеціальних операцій з метою нейтралізації інформаційних загроз, впровадити в освітній процес заняття з «основ інформаційної безпеки», активізувати наукові пошуки у сфері інформаційного протиборства, активізувати дискусію на міжнародному рівні щодо врегулювання визначення понять та заборони інформаційної агресії й інформаційної зброї.

Summary: **In this paper maintenance and structure of the information confrontation are analysed, the definitions of key concepts in this sphere are presented, the personal touches and aim of infowar are defined. On the basis of study of literary sources and analytical materials the separate measures of combating infowar and information psychological influence are offered. The specific examples of attempts of information influence are presented, the structure of the proper messages and method of their analysis are considered. It is suggested to create the center of reacting and conducting of the special operations with the purpose of neutralization of information threats, to inculcate training of «Basics of Information Security» in an educational process, to activate scientific searches in the field of the information confrontation, to activate a discussion at an international level in relation to the settlement of definition of concepts and prohibition of information aggression and information weapon.**

Ключові слова: **Інформаційна війна, інформаційна безпека, україна, заходи протидії.**

I Вступ

У ст. 17 Конституції України відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу [1]. Сьогодні це твердження не є якимось абстрактним, а все більше набуває конкретних рис у рамках протидії з боку України зовнішній агресії. Невипадково на державному рівні почали розробляти вже давно потрібну концепцію інформаційної безпеки України.

Пріоритетними напрямами інформаційної безпеки мають бути забезпечення наступальності і вживання дієвих асиметричних заходів проти всіх форм і проявів інформаційної агресії. Потрібна і побудова ефективної сучасної системи кібербезпеки, зауважує секретар РНБО О. В. Турчинов [2].

Під час дослідження автори зіткнулися з проблемою суттєвої заангажованості та тенденційності багатьох дослідників системи та структури інформаційного протиборства. Це деякою мірою ускладнює процес дослідження, натомість дозволяє більш прискіпливо підійти до вивчення означеної проблематики.

Проблеми інформаційного протиборства досліджували багато дослідників. Серед них потрібно виділити таких зарубіжних фахівців як А. Александров, В. Вепринцев, С. Базан, У. Бернхардт, М. Лейті, В. Лефевр, В. Медсен, Н. Монро, І. Панарін, Р. Роджерс, С. Саад, А. Тесфа, Т. Томас, Дж. Трауб, а також вітчизняних дослідників О. М. Гузька, М. О. Кондратюка, Ю. Ф. Кучеренка, В. К. Медведєва, С. П. Смольца та багатьох інших авторів.

Мета даної статті – розглянути структуру та зміст окремих елементів інформаційної війни, а також деякі методи протидії цьому явищу.

II Зміст інформаційної війни

Однією з концепцій постіндустріального суспільства є концепція так званого «інформаційного суспільства», яка передбачає перенесення значної частини виробництва до інформаційного сектору економіки. Таким чином, відбувається перехід більшої частини робочої сили в цей сектор, побудова розгалуженої інформаційної інфраструктури, однією зі складових частин якої є мережа Інтернет; поступова інтеграція економік розвинених країн. Очевидно, що з впровадженням даної концепції у життя активізується й інформаційне протиборство країн.

Інформаційне протиборство – це форма боротьби сторін з використанням спеціальних (політичних, економічних, дипломатичних, воєнних тощо) методів, способів та засобів для впливу на інформаційне середовище протилежної сторони та захисту власного середовища в інтересах досягнення поставлених цілей [3, с. 172].

Інформаційну війну можна розглядати як найбільш агресивну форму вказаного протиборства. На сьогодні єдиного визначення поняття «інформаційна війна» не існує.

До числа перших офіційних документів з цієї проблеми належить директива Міністерства оборони США Т 3600.1 «Інформаційна війна» від 21.12.1992. У 1997 р. було надано офіційне визначення *інформаційної війни*, під якою розумілися дії, вжиті для досягнення інформаційної переваги в інтересах національної стратегії і які реалізуються шляхом впливу на інформацію й інформаційні системи противника з одночасним захистом власної інформації та власних інформаційних систем.

Існують й інші визначення «інформаційної війни», зокрема, – це цілеспрямовані інформаційні впливи, що здійснюються суб'єктами впливу на мішені (об'єкти впливу) з використанням інформаційної зброї для досягнення запланованої мети.

Тісно пов'язаним з поняттям інформаційної війни є *«інформаційна зброя»* – засіб проведення запланованих дій з інформацією або алгоритм цілеспрямованого впливу на інформаційну систему шляхом передавання такій системі інформації (або здійснення з інформацією інших запланованих дій).

Форми інформаційної війни можуть бути наступними:

1. командно-управлінська;
2. розвідувальна;
3. психологічна;
4. хакерська;
5. економічна;
6. електронна;
7. кібервійна [3, с. 222-223].

Головною метою інформаційної війни є оволодіння свідомістю населення та особового складу збройних сил країни – об'єкта впливу, тобто підготовка підґрунтя для досягнення конкретних політичних, економічних та військових цілей.

Слід *відрізняти війну інформаційної ери від інформаційної війни*. Війна інформаційної ери використовує інформаційні технології для успішного проведення бойових операцій, в той час як інформаційна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активна протидія у інформаційному просторі [4].

Характерними рисами інформаційної війни, які відрізняють її від звичайної, наступні.

1. Відсутність видимих фізичних руйнувань, через що оборонна реакція країни може бути запізнілою.
2. Засоби ведення інформаційної війни є майже непередбачуваними та постійно змінюються в оперативному плані, тому варіанти протидії таким засобам мають спиратися на високий інтелектуальний потенціал, зокрема, аналітичні здібності всіх ланок управління країни, що є досить складним в умовах сьогодення.
3. Під час ведення інформаційної війни не обов'язково відбувається фізичне захоплення людських ресурсів, але встановлюється контроль над їх свідомістю.
4. Вибірковість за принципом досягнення найбільшого ефекту, тобто інформаційна війна буде результативною, коли досягатиме реального ефекту у впливі на суб'єктів прийняття рішень в країні, щодо якої відбувається атака.
5. Короткострокова інформаційна війна є малоефективною у випадку слабкої інформаційної інфраструктури країни впливу [5, с. 25].
6. Розуміння правди нівелюється, дискусії зводяться до абсурду, здійснюється саботаж здорового глузду.
7. Вплив на хід думок супротивника з метою прийняття останнім вигідного для атакуючого рішення.
8. Переведення переваг супротивника в його недоліки.
9. Гра на емоціях, відволікання розуму на негідний об'єкт.

Схожою за змістом до поняття «інформаційна війна» є «*інформаційний тероризм*», який відрізняється, перш за все, суб'єктом відповідних дій. Якщо у першому випадку це держава, то у другому – це, як правило, різного штибу терористичні угруповання.

Зараз можна спостерігати ефективне ведення інформаційної війни в мережі Інтернет. Її елементами можуть виступати так звані фейки – неправдиві сторінки, що містять, зокрема, інформацію з минулого, яку видають за новину дня. Фейк може бути і візуальним, для чого користуються графічними та відеоредакторами. В рамках інформаційного впливу під час доведення інформації використовується певний набір характеристик: видовищність, порушення звичної моделі миру, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг. У розрізі інформаційного протиборства застосовується спеціальна термінологія як от «хом'ячки» – довірлива та легко маніпульована частина населення, яка, на думку британських вчених, є домінуючою, при цьому кожен «хом'ячок» впевнений, що він розумніший за інших. Вони беруть участь в усіх флешмобах та піарах, підписують онлайн-петиції тощо [6, с. 2].

Інформаційне протиборство, залежно від виду операції, здійснюється на стратегічному, оперативному або тактичному рівнях за допомогою інформаційних засобів впливу, які застосовуються з метою нанесення відповідного інформаційного або психологічного впливу на середовище.

Інформаційний вплив застосовується з метою порушення роботи та виведення з ладу різних державних систем управління і баз даних за рахунок створення електромагнітних перешкод або дезорганізації їх роботи при несанкціонованому доступі до них. Психологічний вплив застосовується на людську психологію

відповідних груп населення, військ або людини з метою здійснення відповідної зміни за визначеною, заздалегідь спланованою схемою поведінки відповідної частини суспільства за допомогою засобів масової інформації та інших джерел інформації, а також різних методів психологічного впливу. Засоби здійснення інформаційного впливу постійно змінюються та вдосконалюються відповідно до розвитку теорії ведення збройної боротьби [7, с. 53].

Інформаційна війна складається із сукупності *інформаційних атак*, об'єднаних єдиним замислом.

С. Шарма та Дж. Гупта виділяють декілька типів таких атак: соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, застосування електромагнітної зброї, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів [8, с. 416].

Як відзначає, Т. А. Пода, однією з основних ознак інформаційної атаки є різкий дисбаланс позитивних та негативних повідомлень у доборі матеріалів, відсутність коректного обговорення різних точок зору, коли в ЗМІ витісняється раціональна складова і обговорення йде на рівні емоцій та особистих звинувачень. Така ситуація сприяє формуванню в масовій свідомості міфів, похідних від інтересів впливових соціальних груп. У сучасному інформаційному просторі у значній кількості народжуються соціальні, політичні, художні, релігійні міфи, та, незважаючи на свій ілюзорний характер, здійснюють досить реальний вплив на соціальне життя. В підсумку, сучасний міф перетворився на засіб соціальної мобілізації та маніпуляції суспільною свідомістю. Істина, яку для себе визначає людина, відкривається у формі міфу, тому що в ньому концентрується певне світорозуміння, автентичне даній культурі, і при цьому не вимагає будь-яких аргументів. Міф, який виступає як колосальне джерело масової енергії, здатний мобілізувати навіть групи людей до певних дій. Інформація, яка оформлена в оболонку міфу, набуває чуттєво-виразну конкретність, легко запам'ятовується, естетизуючи життєвий світ сучасної людини, кидає її, в кращому випадку, в обійми ілюзій, а в гіршому, – робить її об'єктом різних маніпуляцій, в тому числі політичних. Масово комунікаційний міф є найвагомішим ефектом масового спілкування, який відображає його сутність, сенс, цілі й мотивацію професійних комунікантів, пов'язану з необхідністю чинити вплив на людину та маси [9, с. 69].

Емоційна складова є дуже характерною рисою інформаційно-психологічного впливу під час інформаційної війни. Як зазначає О. Г. Ющенко, коли людина лякається, в неї перестають працювати аналітичні центри. Психовіруси розраховані на те, аби викликати у людини паніку та страх за рахунок спекуляції на базових потребах. Наприклад, панічні новини про те, що все «жахливо подорожчає» вводять особу у стан паніки, і вона вже не в змозі нормально аналізувати дійсність. Коли людину «зомбують», регулярно підкидаючи їй певні ідеї, то вони приживаються як негласні аксіоми. Така людина буде вкрай важко сприймати будь-які нові ідеї, якщо вони входять у конфлікт із укоріненими старими [10, с. 22].

Інколи, вивчаючи елементи інформаційної війни, говорять про інформаційну експансію. Водночас *«інформаційна експансія»*, відзначає О. Саприкін, є технологією набагато місткішою, ніж «інформаційна війна» або «інформаційна атака». Власне, ці терміни можна вважати складовими інформаційної експансії. В свою чергу, терміном «інформаційна експансія» позначають систему, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей. Інформаційну експансію можуть створювати і поширювати як державні органи (за допомогою державних і приватних інформаційних установ і заходів), так і транснаціональні корпорації для досягнення власної вигоди: забезпечення ринку збуту, участь у великих міжнародних тендерах, доступ до дешевої сировини і робочої сили, політичні та військові цілі тощо [11, с. 40].

Нерідко інформаційна війна йде поряд зі звичайною або гібридною, що можна було спостерігати під час військових дій на Балканах у 90-ті роки, в Іраку на початку XXI ст., в Естонії у 2007 році, в Грузії у 2008 році, в Україні з початку 2014 року.

Що стало передумовою для ефективного ведення інформаційної війни проти України сьогодні?

Декілька причин цього явища було викладено С. П. Смольцем, який у 2011 році відзначив, що, соціальна апатія, песимізм переважають в українському (і не тільки в українському) суспільстві. Падіння якості та престижності освіти, небажання навчатись, розвиватись, викривлення життєво-світоглядних орієнтирів – дані обставини стали причиною різкого зростання безграмотності населення, попри збільшення кількості осіб, хто отримав диплом про вищу освіту. Зростання загальної пасивності в суспільно-політичному житті, повна деградованість політичних еліт. Відповідно ми отримуємо інертне суспільство з пасивними громадянами. Все це є наслідком тоталітарного минулого нашого суспільства та тих інформаційних впливів на його суспільну свідомість яких воно зазнавало і продовжує зазнавати. Таким чином, деструктивні установки, закладені в свідомості, спричинили до зміни в суспільному бутті, моделях поведінки [12, с. 73].

Наведені причини є далеко не вичерпаними, проте їх усунення сприятиме оздоровленню вітчизняного інформаційного простору та створить передумови для провадження ефективної національної

інформполітики всередині країни.

III Методи протидії інформаційній війні

Для ефективної протидії інформаційній віні потрібно регулярно вживати заходи протидії. Велика роль у вирішенні цього завдання відводиться засобам масової інформації. Саме факти, які висвітлюють медіа, акценти на певні явища чи аспекти протистояння, стверджує М. О. Кондратюк, формують думку аудиторії про конфлікт, стимулюючи до потрібної реакції. Засоби масової інформації надають можливості перетворити маленький конфлікт на велике протистояння або, навпаки, – швидко нівелювати серйозну проблему. Саме від ставлення медіа до події, їхньої упередженості та заангажованості значною мірою залежить перебіг самого конфлікту [13, с. 112-113].

Велику роль у протидії інформаційній війні відіграє громадськість, особи з активною життєвою позицією, які через мережу Інтернет доносять інформацію, відмінну від тієї, яка нав'язується суспільству ззовні. У даному випадку можна згадати як досвід Грузії [14, с. 365], так і сучасний досвід України щодо створення проукраїнських та викриваючих Інтернет-ресурсів (http://www.stopfake.org/) тощо.

Корисними у даному випадку також вважаємо розроблені для бізнесу рекомендації з протидії негативу в інформаційному просторі, які можуть бути адаптовані до більш широкого вжитку (див., наприклад, [15]).

Найбільш складним та часовитратним, проте достатньо ефективним методом протидії інформаційній віні, на нашу думку, є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій. У цьому сенсі можна продемонструвати декілька прикладів.

Приклад 1. В мережі Інтернет 15.02.2015 на сайті big-rostov.ru була розміщена інформаційно-аналітична стаття «Выявлена «третья сила», которая терроризирует мирное население Донбасса» (http://big-rostov.ru/?page_id=20465). Аналіз цього матеріалу шляхом підрахунку кількості слів у контексті виявлення ознак маніпулювання інформацією дозволив виявити логічну структуру подачі інформації (рис. 1). Також характерною ознакою можна вважати відсутність посилання на автора статті.

	Зміст логічної частини	Відносний об'єм, %
1.	Відносно достовірні факти (події), підтвердження яких можна знайти в декількох незалежних джерелах з обох сторін протистояння	39
2.	Суперечливе трактування широко відомих подій	27
3.	Дані про невідомі (таємні) факти із неназваних джерел, які не можливо перевірити (імовірна маніпуляція)	10
4.	Думки (не факти) декількох опозиційних зарубіжних аналітиків, які непрямо можуть розглядатися як підтвердження вище наведеної маніпулятивної інформації	24

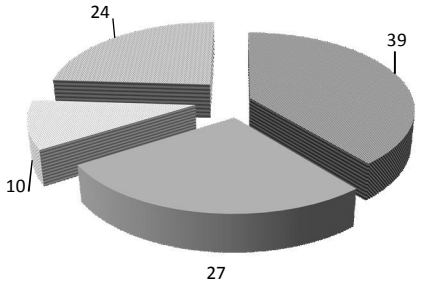

Рисунок 1 – Логічна структура подачі інформації в інформаційно-аналітичний статті «Выявлена «третья сила», которая терроризирует мирное население Донбасса» (http://big-rostov.ru/?page_id=20465)

Приклад 2. У цьому прикладі можна побачити дуже тонку спробу маніпуляції інформацією шляхом лише зміни акценту. В мережі Інтернет 14.02.2015 на сайті www.newscom.md без вказівки на авторство було розміщено інформаційно-аналітичний матеріал «Эгон фон Грейрц: ФРС – банкрот, в США разворачивается экономический коллапс, глобальная финансовая система умирает» (http://www.newscom.md/rus/egon-fon-grejrtc-frs-bankrot-v-ssha-razvorachivaetsya-ekonomicheskij-kollaps-global_naya-finansovaya-sistema-umiraet.html). Аналіз цього матеріалу дозволив встановити, що це переклад інтерв'ю Егона фон Грейрца (Egon von Greyerz) Еріку Кінгу (Eric King), розміщеному за адресою http://kingworldnews.com/man-predicted-collapse-euro-swiss-franc-time-running-global-financial-system, але зовсім з іншою назвою «Man Who Predicted Collapse Of Euro Against Swiss Franc Warns Current Global Financial System Will Cease To Exist» (Людина, яка передбачила крах євро проти швейцарського франка, попереджає, що нинішня світова фінансова система перестане існувати). Строго кажучи, нова назва перекладеної публікації не є вимислом – словосполучення взяті із підзаголовків усередині матеріалу, але, зміна назви оригіналу суттєво змінили акцент основної думки цього інтерв'ю.

Приклад 3. В мережі Інтернет 20.03.14 за адресою http://youtu.be/b6Xn0UW7tGs було розміщено відео із заголовком «США и Евросоюз уничтожат Украину! Правда о событиях на Украине. Смотреть всем!», в якому український політик критикує чинну владу, звинувачує її у цілій низці зловживань і закликає зупинити владу. Аналіз відео і пошук додаткової інформації про факти, які згадуються політиком, дозволяє

стверджувати, що відео є фрагментом, який вирізаний із загального контексту передвиборчих подій осені 2012 року, але подається у контексті політичних подій 2014 року з метою формування відповідної критичної оцінки цих подій.

Приклад 4. В мережі Інтернет 27.03.14 за адресою https://www.youtube.com/watch?v=wZoNgaFWbxM був розміщений аудіозапис із назвою «ПЕРЕХВАТ телефонного разговора бойцов СОКОЛА 27.03.2014», в якому нібито два працівники спецпідрозділу міліції України обговорюють наказ свого керівництва про злочинну ліквідацію при затриманні одного відомого громадського і політичного діяча. Аналіз мови діалогу дозволяє відзначити, що один із співрозмовників має характерний російський говір, в який він зрідка вставляє українські слова, хоча для так званого українського суржику навпаки характерна вставка російських слів в українській говір. Аналіз сигналу запису в звуковому редакторі дозволив виявити факт того, що аудіосигнал, нібито перехоплення телефонної розмови складається із двох незалежних сигналів для кожного співрозмовника. Тобто, запис учасників діалогу здійснювався із двох відокремлених незалежних мікрофонів, а потім два моносигнали були об'єднані у стереосигнал діалогу, що суперечить факту запису мовного сигналу із монофонічного телефонного каналу зв'язку. На рис. 2 показані перші 3 секунди аудіо запису, де звучить дійсна стереофонічна музикальна заставка і в кожному каналі існує корельовані сигнали, а на рис. 3 показаний наступний фрагмент некорельованих моносигналів, що об'єднані у стереосигнал нібито перехвату із монофонічного телефонного каналу зв'язку.

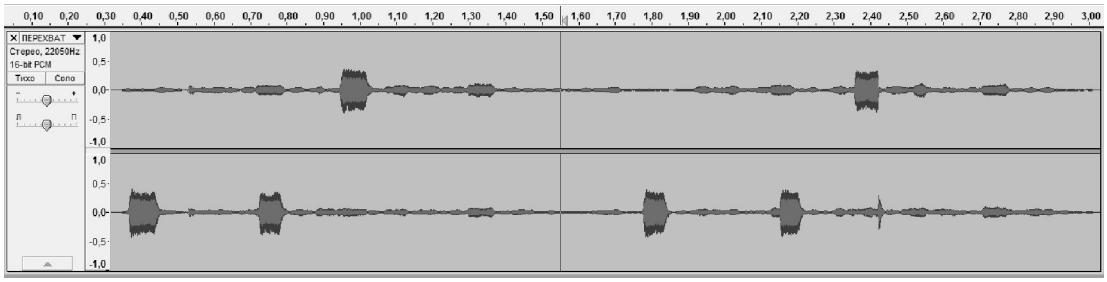

Рисунок 2 – Перші 3 секунди аудіо запису, де звучить дійсна стереофонічна музикальна заставка і в кожному каналі існують корельовані сигнали

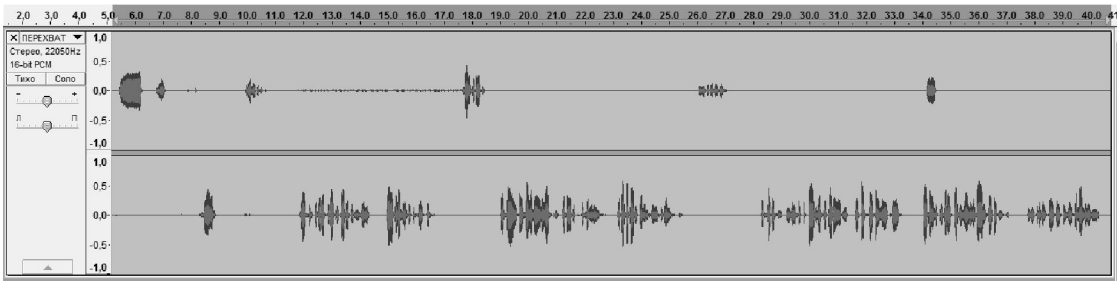

Рисунок 3 – Фрагмент аудіо запису некорельованих моносигналів, що об'єднанні у стереосигнал нібито перехвату із монофонічного телефонного каналу зв'язку

Наведені приклади є лише точкою у вирі інформаційного хаосу, за допомогою якого щоденно намагаються впливати на свідомість як окремих громадян, так і великих груп населення. Все це дає підстави говорити про необхідність активізації в нашій країні зусиль з розбудови ефективної структури інформаційного протиборства.

І. М. Рязанцева та В. В. Тулупов у цьому сенсі пропонують для протидії інформаційній війні впровадити підсистему активних операцій з інформаційного впливу. Його здійснення, на їх думку, слід організовувати у рамках політики інформаційного протиборства з використанням можливостей Служби безпеки України [16, с. 142].

На нашу думку, відповідний центр дійсно має бути створений, проте його функціонування доцільно організувати на громадських засадах за рахунок донорських вливань. Це дозволить побудувати більш гнучку та мобільну сучасну структуру інформаційної протидії. Центр має функціонувати паралельно з державними органами та тісно з ними взаємодіяти.

З урахуванням проведених досліджень основні функції згаданого центру бачаться такими.

1. Координація діяльності волонтерів з моніторингу медіа-ресурсів на предмет наявності матеріалів, які містять згубний інформаційний вплив, а також здійснення такої діяльності працівниками центру. Це може

бути, наприклад, відслідковування матеріалів, в яких містяться заклики до порушення територіальної цілісності, насильницького повалення конституційного ладу тощо. За результатами моніторингу відповідна інформація має доводитись до правоохоронних органів за належністю.

2. Заохочення громадськості до створення ресурсів з викриття неправдивих інформаційних повідомлень, а також доведення результатів у доступній формі до населення.

3. Формування пропозицій до чинного законодавства органам законодавчої та виконавчої влади щодо удосконалення системи інформаційної безпеки країни.

4. Доведення до мешканців країни, яка чинить деструктивний інформаційний вплив, правдивої інформації та створення умов для критичного аналізу громадянами цієї країни відомостей з відповідних медіа.

5. Адаптація сучасних методик інформаційного протиборства до вітчизняних реалій та надання рекомендацій щодо їх застосування відповідним державним органам.

IV Висновки

Виходячи з наведеного, можна зробити висновок, що протидія інформаційній війні та інформаційному тероризму є одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки держави. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер.

Що потрібно здійснити терміново? По-перше, слід нарешті не декларувати, а почати створювати систему кібербезпеки, а також забезпечити функціонування центру реагування та проведення спеціальних операцій з метою нейтралізації інформаційних загроз. По друге, доцільно впровадити в освітній процес, починаючи зі старших класів школи, хоча б факультативні заняття з «Основ інформаційної безпеки». Це дозволить підійти до вирішення досліджуваного в даній роботі питання стратегічно. Третім кроком має бути підтримка держави в ініціюванні та проведенні наукових пошуків проблем інформаційного протиборства та вироблення захисних механізмів. З цією метою мають бути залучені спеціалісти у багатьох сферах знань: медичних, технічних, психологічних, юридичних тощо. На міжнародному рівні варто активізувати дискусію щодо врегулювання в рамках ООН та інших міжнародних організацій з безпеки визначення понять та заборони інформаційної агресії й інформаційної зброї. Вказані заходи є далеко невичерпаними, але мають бути вжиті одночасно у якомога коротший термін.

Список використаної літератури: ***1.*** *Конституція України від 28.06.1996 // Відомості Верховної Ради України. – 1996. – № 30 (23.07.1996).* ***2.*** *Турчинов: Приоритетным направлением информбезопасности является обеспечение наступательности [Електронний ресурс]. – Режим доступу: http://112.ua/obshchestvo/turchinov-prioritetnym-napravleniem-informbezopasnosti-yavlyaetsya-obespechenie-nastupatelnosti-218242.html.* ***3.*** *Панарин И. Н. Информационная война и геополитика / И. Н. Панарин. – М. : Издательство «Поколение», 2006. – 560 с.* ***4.*** *Леонтєва Л. Інформаційна війна в епоху глобалізації [Електронний ресурс] / Л. Леонтьєва. – Режим доступу: http://www.ji-magazine.lviv.ua/seminary/2000/sem13-04.htm.* ***5.*** *Манжай О. В. Правові засади захисту інформації: навчальний-посібник / О. В. Манжай. – Харків : Ніка Нова, 2014. – 104 с. – з іл.* ***6.*** *Зеленина Е. В Королевстве кривых зеркал… / Е. Зеленина // Время. – Вторник. – Декабрь 17. 2013. – № 181 (17337). – С. 1-2.* ***7.*** *Медведєв В. К. Сучасна інформаційна війна та її обрис / В. К. Медведєв, Ю. Ф. Кучеренко, Р. М. Гузько // Системи озброєння і військова техніка. – 2008. – № 1. – С. 52-54.* ***8.*** *Sharma S. Securing Information Infrastructure from Information Warfare / Sushil K. Sharma, Jatinder N.D. Gupta // Logistics Information Management. – 2002. – № 15(5/6). – P. 414-422.* ***9.*** *Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості(соціально-філософський аналіз) / Т. А. Пода // Вісник Національного авіаційного університету. Сер. : Філософія. Культурологія. – 2014. – № 1. – С. 67-70.* ***10.*** *Ющенко А. Г. Украина обязана выиграть информационную войну / А. Г. Ющенко // Україна третє тисячоліття. – 2014. – № 3. – С. 21-23.* ***11.*** *Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012 / О. Саприкін // Вісник Книжкової палати. – 2013. – № 1. – С. 40-43.* ***12.*** *Смольц С. П. Інформаційна війна як чинник формування суспільного буття / С. П. Смольц // Вісник Національного технічного університету України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка. – 2011. – № 3. – С. 70-74.* ***13.*** *Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах / М. О. Кондратюк // Вісник Харківської державної академії культури. – 2013. – Вип. 41. – С. 108-113.* ***14.*** *Osepashvili D. New Media and Russian-Georgian August 2008 War / Dali Osepashvili // Journalism and Mass Communication. – 2014. – Vol. 4, No. 6. – P. 360-366.* ***15.*** *Противодействие негативу в информационном пространстве: методические рекомендации / З. Чистяков, М. Шпаченко. – Агентство конфликтного PR – /PR і Z/, 2012. – 32 с.* ***16.*** *Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 140-144.*