КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.7280
УДК 004.056 : 519

Дудатьєв Андрій Веніамінович
к.т.н., доцент, доцент кафедри захисту інформації
Вінницькийнаціональнийтехнічнийуніверситет, м. Вінниця, Україна
ORCID ID 0000-0002-7944-2404
dudatyev.av@gmail.com

Куперштейн Леонід Михайлович
к.т.н., доцент, доцент кафедри захисту інформації
Вінницькийнаціональнийтехнічнийуніверситет, м. Вінниця, Україна
ORCID ID 0000-0001-6737-7134
kuperstein.lm@gmail.com

Войтович Олеся Петрівна
к.т.н., доцент, доцент кафедри захисту інформації
Вінницькийнаціональнийтехнічнийуніверситет, м. Вінниця, Україна
ORCID ID 0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО: МОДЕЛІ РЕАЛІЗАЦІЇ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Анотація.Життєдіяльністьсучасних великих соціотехнічних систем, які складаються з двох складових: технічної і соціальної частин, відбувається у конкурентному інформаційному просторі. Томуінформаційна безпека таких систем загалом, зокрема держави, у великій мірі залежить від рівня захищеності соціуму. Спеціальні деструктивні інформаційно-психологічні операції, що проводяться проти соціальної складової соціотехнічної системи, переслідують головну мету інформаційного протиборства, а саме: зміну його стану, шляхом перепрограмування свідомості суспільства (соціальної частини соціотехнічних систем).Одним із шляхів реалізації спеціальної інформаційної операції є використання спеціально підготовленої умовної одиниці інформації, наприклад мема, який поширюється в інформаційному просторі завдяки використанню різноманітних каналів впливу і виконує функцію фактично "інфікування" саме соціальної частини соціотехнічних систем. Розглянуто задачі, які необхідно вирішити для досягнення мети деструктивного інформаційно-психологічного впливу. Також наведено основні етапи підготовки та здійснення інформаційно-психологічної операції. Розроблена структурна модель процесів при реалізації інформаційного протиборства. У статті запропонована модель реалізації спеціальної інформаційно-психологічної операції, яка побудована на базі формули Бернуллі і дозволяє отримати ймовірнісну оцінку ефективної реалізації інформаційно-психологічної операції. Також подальший аналіз розробленої моделі, дозволяє отримати оцінку ефективності проведення спеціальної інформаційно-психологічної операції. Ефективність проведеної спеціальної інформаційно-психологічної операції оцінюється ймовірною кількістю елементів соціальної частини, яка під дією цього впливу змінила свій початковий стан, і, як наслідок, вся соціотехнічних систем вийшла зі стану рівноваги. Запропоновані моделі пропонується використовувати при вирішенні задач прогнозування ризиків проведення спеціальних інформаційно-психологічних операцій і відповіднопобудові системи протидії деструктивним інформаційно-психологічним впливам.

Ключові слова:інформаційна безпека; інформаційне протиборство; модель інформаційного впливу; формула Бернуллі.

© А.В. Дудатьєв, Л.М. Куперштейн, О.П. Войтович 2023

ВСТУП

Постановка проблеми. Початок 21 сторіччя показує, що протиріччя, кількість яких збільшується, вирішується в більшості випадків нетрадиційними методами збройних протистоянь, а з використанням сучасних інформаційних технологій. Тобто переможець у протистоянні визначається за результатом проведення спеціальних операцій, що проводяться у інформаційному просторі, які, у свою чергу, розділяються на інформаційно-кібернетичні операції, що спрямовуються на технічну складову соціотехнічної системи (СТС) та інформаційно-психологічні операції (ІПО), що спрямовуються на соціальну складову СТС. Крім того, існує опосередкована залежність між проведеними ІПО і рівнем безпеки технічної складової СТС. Результатом проведення ефективної спеціальної інформаційної операції можуть бути «запрограмовані» дії для супротивника, що можуть призвести до нестійкого стану всієї системи. В першу чергу, це актуально для систем управління, так званих «критичних систем», зокрема енергетичних, транспортних, військових систем тощо. Спеціальні інформаційні операції є механізмом проведення інформаційного протиборства, головною метою якої є перепрограмування свідомості людини. Саме тому розробка аналітичної моделі розповсюдження інформаційних впливів у соціальній частині СТС є актуальною задачею.

Аналіз останніх досліджень і публікацій. Проблеми проведення інформаційних впливів присвячені дослідження багатьох закордонних і вітчизняних вчених [1-3]. У наведених роботах розглянуто достатньо широке коло проблем і задач, які пов’язані з питаннями розповсюдження інформації через різні джерела або канали впливу. Так у роботі [1] проаналізовано місце соціальних медія, як інструмента ведення інформаційної війни.У роботі [2] аналізується процес проходження інформації через так звані три шари поширення інформації: новинні статті (тобто первинна або вихідна інформація), висвітлення цих статей в різних соціальних медіа і коментарі щодо поданої інформації. Очевидно, що під цими статтями мається на увазі спеціально підготовлена інформація. Проходячи через ці три шари первинна інформація може бути змінена в силу різних причин, у тому числі може бути спеціально спотворена. У роботі [3] розроблена класифікація методів маніпулятивного впливу, а також розроблені структурні і аналітичні моделі маніпулятивного впливу, орієнтовані на ЗМІ.

У роботі [4] досліджується кіберживучість об’єктів критичної інфраструктури в умовах протиборства двох або більше сторін. Представлена методика оцінки кіберживучості об’єктів критичної інформаційної інфраструктури на прикладі об’єднаної енергосистеми України. У книзі [5] проведено загальний аналіз мема, як спеціально підготовленої інформації для реалізації ІПО, розглянуто деструктивну сторону мема і як наслідок зміну поведінки людини. Робота Джіна Шарпа [6] – представляє 198 ненасильницьких дій, метою яких є також зміна стану людини.

Разом із тим існує комплексна проблема, що полягає у відсутності системного підходу щодо побудови узагальненої аналітичної моделі інформаційного впливу, з урахуванням початкового стану об’єктів впливу, наявних джерел впливу, умов та обмежень на проведення ІПО тощо.

Мета статті.Метою роботи є розробка узагальненої моделі реалізації та оцінювання ефективності деструктивного інформаційно-психологічного впливу, як базового інструменту інформаційного протиборства.

Відповідно до мети задачами дослідження є: аналіз існуючих результатів, розробка узагальненої моделі реалізації інформаційного впливу, а також моделі для оцінювання ефективності спеціальної інформаційної операції

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Головною метою інформаційного протиборства є завоювання і утримання інформаційної переваги над протиборчою стороною.«Підкорити супротивника без бою – ось вінець мистецтва …» так писав відомий китайський філософ Сунь-Цзи у своєму трактаті «Мистецтво війни». Яким чином цю складну задачу можна вирішити? Використовуючи сучасні технології, постійно працюючи у соціальних мережах, отримуючи інформацію з тих чи інших сайтів і таким чином, опосередковано від власних думок і бажань створюється власна інформаційна модель, яка відображає уподобання, пріоритети тощо. Голова Apple Тім Кук відзначає: «Здається, що жодна інформація не є надто особистою чи надто приватною, щоб її не можна було відстежувати, монетизувати і агрегувати, щоб отримати вичерпний огляд всього вашого життя. Підсумок цього – те, що ви більше не клієнт, ви – продукт» [7].

Відповідно проведення ІПО організовуються і проводяться з метою перетворення «суб'єкта-клієнта» на «об'єкт-продукт» інформаційної взаємодії.

Відповідно, для досягнення головної мети інформаційного протиборства потрібно вирішити такі задачі.

1) Створення напруги і хаосу, шляхом маніпулювання свідомістю соціуму СТС.

2) Ініціації внутрішніх конфліктів.

3) Зниження рівня інформаційного забезпечення (своєчасності і об'єктивності подання інформації), як органів влади так і безпосередньо населення, з метою зниження керованості процесів життєдіяльності соціуму, підриву довіри до влади тощо.

4) Підрив ефективності функціонування суб'єкта інформаційної взаємодії, в тому числі на міжнародній арені.

5) Нанесення ризиків об'єктам критичної інфраструктури.

Для отримання перемоги у конкурентному інформаційному середовищі потрібно забезпечити максимально можливе охоплення соціуму, а також практично реалізувати прямі чи опосередковані контакти з окремими його елементами.

Важливим є те що для рішення наведених задач протиборчим сторонам потрібно мати відповідні ресурси. В першу чергу ці ресурси мають забезпечувати можливість проведення спеціальнихІПО. При цьому потрібно зауважити, що протиборчі сторони мають свої ресурси, процеси, що відбуваються в системах організації і реалізації спеціальних ІПО, внутрішні і зовнішні об'єктно-суб'єктні відносини тощо. Узагальнено можна сказати, що це стан економіки, технологічний стан протиборчої сторони, рівень інформатизації суспільства тощо.

Процес формування відгуків або ставлення до контенту інформаційних повідомлень, з яких складається ІПО відображено структурною схемою, яка наведена на рис.1.

Коментарі використовують як засіб маніпуляцій. Але для того щоб коментар був максимально ефективним потрібно виконати певний алгоритм визначених операцій.

Можна виділити такі основні етапи підготовки та здійснення інформаційно-психологічної операції :

- планування;
- формулювання робочих цілей;
- аналіз об'єкта впливу;
- аналіз конкретних видів, форм, методів інформаційно-психологічного впливу;
- планування контенту інформаційно-психологічного впливу;
- вибір відповідних джерел впливу;
- визначення обмежень та умов здійснення інформаційно-психологічного впливу;

- проведення підготовленої інформаційно-психологічної операції;
- аналіз відгуків об’єкта впливу;
- оцінювання ефективності проведення ІПО;
- коригування (за потреби) умов та обмежень здійснення ІПО;
- завершення ІПО.
-

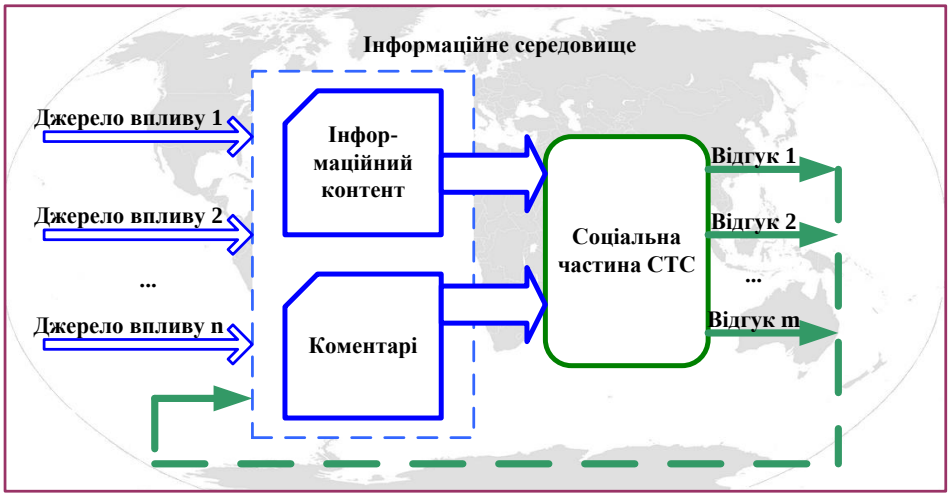

Рис.1 Процес формування ставлення до інформаційних повідомлень

Очевидно, що наведена алгоритмізація процесу проведення ІПО вимагає побудови організованої системи проведення інформаційного протиборства.

З огляду на основні етапи підготовки та здійснення інформаційно-психологічної операції пропонується структурна модель процесів інформаційного протиборства, яка наведена на рис.2.

Рис.2 Структурна модель процесів інформаційного протиборства

Елементи системи інформаційного протиборства виконують такі операціїз наведеного вище алгоритму проведення ІПО.

Підготовка ІПО:планування операції, формулювання цілей операції, аналіз об’єкта впливу.

Вибір джерела впливу: вибір та підготовка відповідних інформаційних каналів для реалізації ІПО, визначення обмежень та умов здійснення впливу.

Формування контенту та коментарів: формування контенту інформаційно-психологічного впливу та його інформаційного супроводу у вигляді коментарів.

Вибір об'єкта впливу: сегментація і вибір частини соціуму на який відбувається інформаційний вплив.

Аналіз реакції об'єкта впливу: аналіз відгуків об'єкта впливу.

Оцінювання ефективності впливу: оцінювання ефективності реалізованого впливу.

Корегування ІПО: на основі результатів аналізу відгуків об'єкта впливу, а також оцінки ефективності, відбувається корегування умов і обмежень, а також контенту спеціальної інформаційної операції.

МОДЕЛЬ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ОПЕРАЦІЇ

Якщо розглядати позитивний результат (відбулася зміна стану відповідної соціальної частини СТС) проведення ІПО, як випадкову подію, то для оцінювання ймовірності результату проведення деструктивного інформаційного впливу використаємо теорему Бернуллі.

Теорема Бернуллі в теорії ймовірностей стверджує, що при багаторазовому повторенні випадкового експерименту, в даному випадку проведенні ІПО, з двома можливими результатами (ефективна атака або неефективна атака) відносна частота успіхів наближається до ймовірності успіху за умови проведення одного випробування [8]. Важливою умовою практичного використання формули Бернуллі є стійкість умов щодо проведення експерименту. Тобто нас завжди цікавить одна подія А – проведення ІПО, ефективність проведення якої становить p.

Ймовірність ефективних впливів за допомогою формули Бернуллі, можемо подати:

$$P_n(k) = C_n^k \cdot p^k \cdot q^{n-k}, \quad (1)$$

де C_n^k – кількість сполучень, q=1-p.

Спочатку інформація, що надсилається, певним чином систематизується, а по мірі її повторення, ймовірність її впливу, тобто ефективність проведення спеціальної інформаційної операції збільшується.

За умови домінування у інформаційному просторі мета проведення ІПО з великою ймовірністю буде достатньо швидко реалізована.

ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

Приклад 1.Проведемо чисельне моделювання ситуації, яка відображає наявність у інформаційному просторі декількох різних незалежних інформаційних джерел, перед якими сформульована одна мета.

Розглянемо ситуацію, коли для реалізації ІПО використовують 10 незалежних інформаційних джерел. Приймемо умови проведення експерименту, такі що не змінюються: ймовірність того, що інформаційна операція проведена ефективно p=0,6. Відповідно q=1-0,6=0,4. Необхідно визначити ймовірність ефективної спеціальної інформаційної операції за умови використання 3-х і 4-х незалежних джерел впливу.

За допомогою виразу (1) отримано ймовірністьреалізації атак для 3-х і 4-х джерел:

$P_{10}(3)=C_{10}^3p^2q^7=(10!|3!7!)p^3q^7=(10!|3!7!)*0,6^{3*}0,4^7=0,004.$

$P_{10}(4)=C_{10}^4p^4q^6=(10!|4!6!)p^4q^6=0,108.$

ISSN 2663 - 4023

Як видно із проведеного чисельного експерименту ймовірність ефективної атаки із залученням 4-х джерел більше ніж для 3-х джерел, при цьому різниця суттєва.

Продовженням практичного застосування розглянутого підходу може бути використання отриманих співвідношень для рішення задачі оцінювання ефективності інформаційного впливу, з урахуванням кількості осіб, що змінили свій початковий стан. В роботі [9] запропонована модель для оцінювання ефективності інформаційного впливу, однак при цьому розглядався процес атаки за умови одного каналу впливу.

З урахуванням вищенаведеної інформації можемо представити модель для оцінювання оцінки ефективності ІПО, за ймовірною кількістю осіб, які складають певну соціальну групу і потравляють під відповідний інформаційний вплив.

$$N(t) = \sum_{i=1}^{m} \left(N_{0i} \cdot s_i\right) \cdot C_n^k \cdot p^k \cdot q^{n-k}, \quad (2)$$

де m – кількість груп, на які спрямований вплив; t – час впливу; s_i – коефіцієнт емоційної складової мема. Мем в цьому випадку розглядається як умовна одиниця інформації – носій спеціально підготовленої інформації для реалізації впливу [10].

Як приклад дослідимо задачу, яка розглянута у роботі [9]. Відмінністю використання запропонованої моделі у роботі є те, що ймовірність потрапляння певного сегмента соціуму під одне джерело впливу – $p = e^{-\tau/t}$. Ймовірність ефективного потрапляння цього ж сегмента соціальної частини СТС під дію декількох джерел впливу, зокрема 3-х і 4-х джерел впливу можемо оцінити використовуючи вираз (2). В цьому випадку: t – час впливу, τ_i – час до перших змін стану елементів соціальної частини СТС.

Приклад 2. На соціальну складову СТС, яка складається з $N_0 = 2700$ осіб спрямована спеціальна інформаційна операція. Потрібно визначити точку неповернення в стійкий стан соціальної складової СТС, за умови, що її стійкий стан зберігається не менше $\tau = 24$ години. Стан системи досліджується протягом $t = 100$ годин. Коефіцієнти емоційної складової мема, який може бути представлений, наприклад, відповідними коментарями (маніпулятивна складова) – $k = 0{,}6$.

Використовуючи запропоновану модель (2), отримаємо вираз для розрахунку кількості ймовірних змін у соціальній складовій СТС.

Для 3-х джерел впливу:

$N(t) = P_{10}^3 \cdot N_0 \cdot k = 0{,}004 * 2700 \cdot 0{,}6 \approx 7$ (осіб).

Для 4-х джерел впливу:

$N(t) = P_{10}^4 \cdot N_0 \cdot k = 0{,}108 * 2700 \cdot 0{,}6 \approx 175$ (осіб).

Наведений приклад демонструє суттєве зростання ймовірних змін у соціальній групі при використанні 4-х джерел впливу за визначених умов і обмежень.

При практичному використанні запропонованих моделей потрібно враховувати об’єктивні процеси і явища, які супроводжують життєдіяльність соціотехнічної системи. Можуть бути такі обставини.

1. Неможливість своєчасного отримання інформації, що може бути обумовлено різними форс - мажорними подіями.

2. Випадковими змінами у інформаційному середовищі, зокрема виникненням альтернативних інформаційних джерел впливу тощо.

3. Нестачею або обмеження на певні ресурси, зокрема кошти, ресурси щодо забезпечення життєдіяльності СТС, інформаційно-телекомунікаційні системи які задіяні у процесі обробки інформації тощо.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Світовий досвід показує, що проведення спеціальних інформаційних операцій є ефективною технологією проведення інформаційного протиборства. Вплив деструктивних інформаційних впливів на соціальну частину СТС може вивести її із стану інформаційної стійкості, змінити систему управління всією системою і сформувати потрібну модель поведінки для опонента.Запропоновані моделі інформаційного впливу базуються на результатах аналізу мети його реалізації, можливих джерел розповсюдження спеціально підготовленого контенту, базових ознаках об'єктів інформаційного впливу, аналізу обмежень та можливостей розповсюдження інформації тощо.

Подальші дослідження запропонованих моделейдоцільно продовжувати у практичній площині, зокрема при реалізації захисту, наприклад, персоналу будь якого підприємства, від деструктивних інформаційних впливів, під час проведення інформаційного протиборства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Voitovych, O., Kupershtein, L., Holovenko, V. (2022). Виявлення фейкових облікових записів в соціальних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 86-98. https://doi.org/10.28925/2663-4023.2022.18.8698

2 ChenhaoTan.(ICWSM 2016).Unfolding News Cycles from the Source.Proceedings of the Tenth International Conference on Web and Social Media C.378-387. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13011

3 Gnatyuk, S., Zhmurko, T. (2016). Information-Psychological Security of Society in the Context of Information Warfare. In J. Rysiński (Ed.), Inżynier XXI wiekuprojectujemyprzyszlosc (pp. 321-341). Bielsko-Biała: Wydawnictwo Naukowe AkademiiTechniczno-Humanistycznej w Bielsku-Białej.

4 Komarov, M., Honchar, S., Dimitriieva, D. (2021). Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 59-66. https://doi.org/10.32918/nrs.2021.1(89).07https://nuclear-journal.com/index.php/journal/article/view/771

5 Richard Brodie. (2011)Virus of the Mind: The New Science of the Meme Paperback. 256 p. Hay House Inc.; Reissueedition.

6 GeneSharp198 METHODS OF NONVIOLENT ACTION. https://www.aeinstein.org/nonviolentaction/198-methods-of-nonviolent-action/

7 Cook, T. (2019). Technology does not need vasttroves of personal data. Advertising existed and thrived for decades with outit. https://www.marketingweek.com/apple-data-privacy

8 Васильків І. М. (2020). Основи теорії ймовірностей і математичної статистики. https://new.mmf.lnu.edu.ua/wp-content/uploads/2020/04/Vasyl-kiv-I.M.-TIMS_CHASTYNA_1.pdf

9 Дудатьєв, А. В., Войтович, О. П. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. Інформаційні технології та комп'ютерна інженерія, 38(1), 16–21. https://itce.vntu.edu.ua/index.php/itce/article/view/657

10 Лужецький В. А., Дудатьєв А.В. (2017). Концептуальна модель системи інформаційного впливу. Безпека інформації, 23 (1), 45–49.https://doi.org/10.18372/2225-5036.23.11550

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

Andrii V. Dudatyev
Ph.D., Associate Professor, Associate Professor of Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID-0002-7944-2404
dudatyev.av@gmail.com

Leonid M. Kupershtein
Ph.D., Associate Professor, Associate Professor of Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID 0000-0001-6737-7134
kuperstein.lm@gmail.com

Olesia P. Voitovych
Ph.D., Associate Professor, Associate Professor of Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID 0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua

INFORMATION COUNTERFEATURE: MODELS OF IMPLEMENTATION AND EVALUATION OF INFORMATION OPERATIONS

Abstract. Life activity of modern large socio-technical systems, which consist of two components: technical and social parts, takes place in a competitive information space. Therefore, the information security of such systems in general, in particular of the state, largely depends on the level of societysecurity. Special destructive informational and psychological operations conducted against the social component of the sociotechnical system pursue the main goal of informational struggle, namely: changing its state by reprogramming the society consciousness (the social part of sociotechnical systems). One of the ways to implement a special information operation is the use of a specially prepared conditional unit of information, such as a meme, which spreads in the information space by the using of influence various channels and performs the function of actually "infecting" the social part of socio-technical systems. The problems that must be solved in order to achieve the goal of destructive informational and psychological influence are considered. The main stages of preparation and implementation of an informational and psychological operation are also given. A structural model of the processes involved in the implementation of information warfare is developed. The article proposes a model for the implementation of a special informational and psychological operation, which is built,based on the Bernoulli formula and allows obtaining a probabilistic assessment of the effective implementation of an informational and psychological operation. In addition, further analysis of the developed model allows getting an assessment of the effectiveness of conducting a special informational and psychological operation. The effectiveness of the conducted special informational and psychological operation is evaluated byusing the probable number of social partelements, which, under the influence changed its initial state, and, as a result, the entire socio-technical system came out of equilibrium. The proposed models are can be used in solving the forecasting the risks problems of conducting special informational and psychological operations and, accordingly, building a system for counteracting destructive informational and psychological influences.

Keywords:information security; model of information influence; Bernoulli's formula.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Voitovych, O., Kupershtein, L., Holovenko , V. (2022). DETECTION OF FAKE ACCOUNTS IN SOCIAL MEDIA. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 2(18), 86-98. https://doi.org/10.28925/2663-4023.2022.18.8698

2 Chenhao Tan.(ICWSM 2016). Unfolding News Cycles from the Source.Proceedingsof the Tenth International Conference on Web and Social Media C.378-387. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13011

3 Gnatyuk, S., Zhmurko, T. (2016). Information-Psychological Security of Society in the Context of Information Warfare. In J. Rysiński (Ed.), Inżynier XXI wiekuprojectujemyprzyszlosc (pp. 321-341). Bielsko-Biała: WydawnictwoNaukoweAkademiiTechniczno-Humanistycznej w Bielsku-Białej.

4 Komarov, M., Honchar, S., Dimitriieva, D. (2021). Study of the Cyber Survivability of Critical Information Infrastructure Objects. Nuclear and Radiation Safety, 1(89), 59-66. https://doi.org/10.32918/nrs.2021.1(89).07

5 Brodie, R. (2011). Virus of the mind: The new science of the meme (Reissue ed.). Hay House.

6 Gene Sharp 198 METHODS OF NONVIOLENT ACTION. https://www.aeinstein.org/nonviolentaction/198-methods-of-nonviolent-action/

7 Cook, T. (2019). Technology does not need vast troves of personal data. Advertising existed and thrived for decades without it. https://www.marketingweek.com/apple-data-privacy

8 Vasylkiv, I. (2020). Basics of probability theory and mathematical statistics. https://new.mmf.lnu.edu.ua/wp-content/uploads/2020/04/Vasyl-kiv-I.M.-TIMS_CHASTYNA_1.pdf

9 Dudatyev, A. V., Voitovych, O. P. (2017). Information security of the socio-technical system: The model of the information impact. Information Technology and Computer Engineering, 38(1), 16–21. Retrieved from https://itce.vntu.edu.ua/index.php/itce/article/view/657

10 Luzhetskyi V., Dudatyev A. (2017) Conceptual model of information impact system. Ukrainian Scientific Journal of Information Security, 23(1), 45-49.https://doi.org/10.18372/2225-5036.23.11550

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.