Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: **“РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ”**

Виконала: студентка групи KN1-M22
спеціальності 122 Комп’ютерні науки
Войцехівська Олександра Віталіївна

Керівник: **Моцик Р.В.,**
доцент кафедри комп’терних наук,
кандидат педагогічних наук, доцент

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

В сучасному світі інформаційних технологій соціотехнічні системи стали необхідною складовою нашого повсякденного життя. Вони об'єднують технології та суспільство, створюючи екосистеми, в яких інформація та взаємодія відіграють ключову роль. Однак разом із неймовірними можливостями, які надають соціотехнічні системи, приходить і загроза деструктивного інформаційно-психологічного впливу.

Деструктивний вплив може приймати різні форми, включаючи дезінформацію, фішинг, кібератаки, маніпуляцію громадською думкою та багато інших. Він може завдавати шкоду як окремим користувачам, так і суспільству в цілому, порушуючи приватність, розкриваючи конфіденційну інформацію та психологічно впливаючи на нашу поведінку та переконання.

Саме тому розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах стає актуальною і важливою проблемою. Ця тема об'єднує інформаційні технології, психологію та кібербезпеку в спробі розробити ефективні методи виявлення та захисту від деструктивного впливу.

У нашому дослідженні ми ставимо за мету розкрити сутність деструктивного впливу в соціотехнічних системах, вивчити психологічні аспекти цього явища та розробити методологію та інструменти для виявлення і запобігання його наслідкам. Наша робота спрямована на створення безпечних та стійких соціотехнічних систем, де користувачі можуть вільно спілкуватися та обмінюватися інформацією без страху перед деструктивними загрозами.

Подальше дослідження цієї теми має потенціал впливати на розвиток кібербезпеки, психологічної науки та суспільства в цілому, роблячи інформаційні технології безпечнішими та надійнішими для всіх користувачів.

Тема нашого дослідження: "Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах" є досить

актуальною і важливою в сучасному світі, особливо з відкриттям нових можливостей для впливу на суспільство за допомогою інформаційних технологій.

Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є актуальною темою сьогодення, оскільки вона стосується різних сфер життя і може мати велике значення для захисту інформаційної безпеки, захисту від маніпуляцій та покращення психологічного здоров'я користувачів.

Метою дослідження є розробка ефективного методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах з метою захисту користувачів та суспільства від негативних наслідків цього впливу.

Завдання дослідження:

1. Аналіз основних видів деструктивного інформаційно-психологічного впливу.
2. Дослідження методології виявлення видів деструктивного інформаційно-психологічного впливу в соціотехнічних системах.
3. Аналіз алгоритмів та програмних засобів для виявлення деструктивного впливу на основі дослідженої методології.
4. Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах.

Ці завдання спрямовані на досягнення загальної мети - створення ефективного методу виявлення деструктивного впливу в соціотехнічних системах і забезпечення захисту суспільства від цього впливу.

Об'єкт дослідження. Соціотехнічні системи. Соціотехнічні системи включають в себе комплекс взаємодій між технічними елементами (наприклад, інформаційні технології, платформи, соціальні мережі) і людьми, що використовують ці технології.

Предмет дослідження. Дослідження методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах.

Апробація результатів дослідження. Результати дослідження були оприлюднені на звітній науковій конференції студентів та магістрів за підсумками науково дослідної роботи у 2022-2023 навчальному році та публікаціях: .

Структура роботи. Магістерська робота складається із вступу, трьох розділів, висновків, списку використаних джерел.

ВИСНОВКИ

Метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є актуальним та важливим в сучасному світі, особливо з відкриттям нових можливостей для впливу на суспільство за допомогою інформаційних технологій.

Розроблений метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є важливою складовою інформаційної безпеки сьогодення, оскільки він стосується різних сфер життя і може мати велике значення для сучасного соціуму, захисту від маніпуляцій та покращення психологічного здоров'я користувачів.

У нашому дослідженні нами було виконано усі визначені завдання, а саме:

1. Проаналізовано сучасні алгоритми виявлення деструктивного впливу в соціотехнічних системах, розкрито психологічні аспекти деструктивного впливу, зокрема впливу на психіку та поведінку користувачів, що можуть допомогти краще розуміти механізми атак та розвивати ефективні методи захисту. Зроблено висновок, щодо важливості розвивати механізми взаємодії з користувачами та співпрацю з ними для виявлення та реагування на деструктивний вплив.

2. Досліджено методології виявлення видів деструктивного інформаційно-психологічного впливу в соціотехнічних системах. А саме:

Існуючі інформаційні технології та методи в залежності від глибини аналізу текстової інформації розглянуто за трьома класами. До першого класу відносяться технології та методи, які забезпечують аналіз IP за ключовими словами. Відповідно такі методи дозволяють з одного боку створювати, а з іншого боку виявляти інформаційні атаки першого покоління. До другого – інформаційні технології та методи, які додатково дозволяють аналізувати семантичний контент електронних TIP. Третій клас інформаційних технологій та методів формують такі технологічні рішення,

які додатково дозволяють збільшити глибину аналізу текстової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної складової особистості.

3. Проаналізовано сучасні алгоритми та програмні засоби для виявлення деструктивного впливу на основі відкритих методологій.

4. Розроблено метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах. Який включає головну особливість - це ідентифікація інформаційно-психологічного впливу структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала

Наше дослідження спрямоване на досягнення загальної мети - створення ефективного методу виявлення деструктивного впливу в соціотехнічних системах і забезпечення захисту суспільства від цього впливу.

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

11. С. В. Волобуев, *Безопасность социотехнических систем*. Обнинск, Россия: Викинг, 2012.

12. Г. А. Остапенко, и Е. А. Мешкова, *Информационные операции и атаки в социотехнических системах*. Москва, Россия: Горячая линия-Телеком, 2016.

13. А. В. Дудатьев, В. А. Лужецкий, и Д. А. Коротаев, "Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны", *Восточно-Европейский журнал передовых технологий*, т. 2, № 2 (80), с. 4-11, 2016. doi: 10.15587/1729-4061.2016.65691

14. С. И. Кравченко, "Безопасность социотехнических систем", *НБИ технологии*, т. 12, № 2, с. 20-24, 2018. doi: 10.15688/NBIT.jvolsu.2018.2.3.

15. Д. А. Горницкая, А. Г. Корченко, та В. П. Харченко, "Система социотехнических атак в информационной среде", на *Второй международной научно-практической конференции Проблемы экономики и управления на железнодорожном транспорте*, Киев, 2007, с. 137-138.

16. ДП "УкрНДНЦ". (2016, Груд. 27). *ДСТУ ISO/IEC 27032. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)*. Київ, 2018, 50 с.

17. V. V. Mokhor, O. V. Tsurkan, R. P. Herasymov, and V. V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering

Approach", *Selected Papers of the XVII International Scientific and Practical Conference Information Technologies and Security*, Kyiv, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.

18. О. Цуркан, Р. Герасимов, та О. Крук, "Методи протидії використанню соціальної інженерії", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 161-170, July-December 2019. doi:

10.20535/2411-1031.2019.7.2.190563.

19. В. В. Мохор, О. В. Цуркан, та Р. П. Герасимов, "Маніпулятивна форма соціоінженерного впливу на особистість в кіберпросторі", на *Науково-практичній конференції Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2015, с. 303-304.

20. А. Л. Тулупьев, А. Е. Пащенко, и А. А. Азаров, "Информационная модель пользователя, находящегося под угрозой социоинженерной атаки", Тр. СПИИ-РАН, вып. 13, с. 143-155, 2010.

21. В. Л. Бурячок, О. Г. Корченко, та Л. В. Бурячок, "Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем", *Захист інформації*, т. 14, № 4 (57), с. 5-12, 2012. doi: 10.18372/2410-7840.14.3471.

22. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, "Розширена класифікація методів соціального інжинірингу", *Безпека інформації*, т. 20, № 2, с. 197-205, 2014. doi: 10.18372/22255036.20.7308.

23. F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 1-54, June 2016. doi: 10.1016/j.cose. 2016.03.004.

24. F.-F. M. Amir, H.-K. Mostafa, and T.-M. Reza, "The Social Engineering Optimizer (SEO)", *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 267-293, 2018, doi: 10.1016/j.engappai.2018.04.009.

25. S. Wasserman, and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press, 2012. doi: 10.1017/CBO9780511815478.

26. O. V. Tsurkan, R. P. Herasymov, and O. M. Kruk, “Presentation the interaction of the subject and the object of socio-engineering influence with a social graph”, in *Proc. Fourth International Scientific and Technical Conference Computer and Informational Systems and Technologies*, Kharkiv, 2020, pp. 46. doi: 10.30837/IVcsitic2020201371.

27. О. В. Цуркан, та Т. М. Клименко, “Аналіз вразливостей соціотехнічних систем на основі нечітких соціальних графів”, на *Науково-практичній конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України Безпека енергетики в епоху цифрової трансформації*, Київ, 2019, с. 28.