



УДК 004.056.52: 159.942

ДОСЛІДЖЕННЯ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ. ЧАСТИНА І. ВПЛИВ НА ЗДОРОВ'Я ЛЮДИНИ.

Селіванова А.В.¹, Левитський Ю.О.²^{1,2} Odessa National University of Technology, Odessa, UkraineORCID: ¹<https://orcid.org/0000-0002-3395-1422>, ²<https://orcid.org/0000-0002-2245-3364>E-mail: ¹alikalasvano@gmail.com, ²levitskiy199916@gmail.com

Copyright © 2021 by author and the journal "Automation of technological and business – processes".

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0>

DOI: 10.15673/atbp.v14i2.2334

Анотація. Представлена робота присвячена дослідженню впливу методів соціальної інженерії (СІ) на здоров'я людини.

В процесі роботи досліджено визначення терміну соціальна інженерія, його популярність, алгоритм дії соціальних інженерів (СІн), методи впливу СІ на людину, види агресивного психологічного впливу на особистість у кіберпросторі, засоби подолання наслідків впливу методів СІ на людину, інформаційні системи, що інформують про методи СІ та їх вплив на здоров'я людини.

Проведено збір даних методом опитування, що характеризує вплив дії СІн на здоров'я людей. Отримані дані оброблені за допомогою засобів інтелектуального аналізу даних із використанням інструментальних засобів Google та Orange. Розроблено модель впливу СІ на здоров'я людини.

Результати дослідження було впроваджено у аналітичну платформу KitStat у якості оновлення, що дозволяє надати інформаційну підтримку та забезпечити продовження збору даних для подальшого дослідження.

В процесі проведення дослідження використано такі засоби та технології як Google Forms, Google Analytics, Orange, мови HTML5, CSS3, PHP, JavaScript.

Результати дослідження можуть бути використані як фахівцями при дослідженні методів СІ так і звичайними людьми для захисту від дії соціальних інженерів.

Abstract. The presented work is devoted to the study of the impact of social engineering (SI) methods on human health.

In the course of the work, the definition of the term social engineering, its popularity, the algorithm of action of social engineers (SI), methods of influence of AI on a person, types of aggressive psychological influence on a person in cyberspace, means of overcoming the consequences of the influence of AI methods on a person, information systems that inform about AI methods and their impact on human health.

Data collection was carried out using the survey method, which characterizes the impact of SIN on people's health. The received data is processed with the help of intelligent data analysis tools using Google and Orange tools. A model of the impact of AI on human health has been developed.

The results of the study were implemented in the analytical platform KitStat as an update, which allows to provide informational support and ensure the continuation of data collection for further research.

In the process of conducting the research, such tools and technologies as Google Forms, Google Analytics, Orange, HTML5, CSS3, PHP, JavaScript languages were used.

The results of the research can be used both by specialists in the study of AI methods and by ordinary people to protect against the actions of social engineers.

Ключові слова: соціальна інженерія, Google Forms, Google Analytics, дослідження методів СІ

Key words: social engineering, Google Forms, Google Analytics, research on AI methods

Вступ

Соціальна інженерія - метод отримання необхідного доступу до інформації, що ґрунтується на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем. Хоча термін соціальної інженерії з'явився не так давно, сам метод отримання інформації у такий спосіб використовується досить довго [1]. Соціальна інженерія спрямована не на комп'ютерну техніку, а на її користувача. Інтерес представляють усі платоспроможні особи, а також користувачі, що мають цінну інформацію, співробітники підприємств і державних установ. Метод застосовується з метою виконання



фінансових операцій, злому, крадіжки відомостей (наприклад, клієнтських баз, персональних даних) і іншого несанкціонованого доступу до інформації. Соціальна інженерія допомагає конкурентам здійснювати розвідку, виявляти слабкі сторони організації, переманювати співробітників [2].

Під час пандемії і карантину міняється звичне докільця, стратегії поведінки, система планування (відпустки, навчання, бюджет, способи пересування). Психіка людини приходить в стресовий стан, і запускаються адаптаційні процеси. Організм використовує резерви, які в нормі не задіяні, когнітивні функції стають обслуговуваними і реагують на емоційний стан, тому пам'ять і увага на деякий період часу погіршуються. Як наслідок, підвищена схильність впливу шахраїв. Тобто якщо в нормі людина не схильна вірити в "підозрілі транзакції", про які повідомляють з незнайомого номера, в стані стресу тривожність перемагає, і людина стає жертвою [3]. Дії соціальних інженерів у випадку якщо вони призводять до втрат можуть нанести психологічну травму людині. Таким чином, дослідження методів впливу соціальної інженерії на здоров'я людини, методів захисту від нього та подолання наслідків є актуальним напрямком дослідження.

Динаміка і ритм сучасного життя, прагнення до успіху вимагають від людини постійною зібраності, концентрації уваги, мобілізації усіх сил. Це, у свою чергу, є причиною виникнення у людини численних стресів, депресій, коливань психоемоційного стану. Стреси займають значне місце в житті людей. Вони впливають на здоров'я, поведінку людини, взаємовідносини з іншими людьми, стосунки в сім'ї, працездатність, а отже, на досягнення або недосягнення людиною успіху [4]. Пандемія і карантин, що тривають вже понад 2 роки, ще більш додали напруженості, психіка людини приходить в стресовий стан і запускаються адаптаційні процеси. Організм використовує резерви, які в нормі не задіяні, когнітивні функції стають обслуговуваними і реагують на емоційний стан, тому пам'ять і увага на якийсь період часу погіршуються. Наслідком цього може стати підвищена схильність до впливу шахраїв або соціальних інженерів. Якщо в звичайному стані людина не схильна вірити в "підозрілі транзакції", про які повідомляють з незнайомого номера, в стані стресу тривожність перемагає, і людина стає жертвою.

Під час карантину і віддаленої роботи з'явилися нові чинники, які доводиться враховувати службам безпеки банків та інших організацій: обробка клієнтських документів на домашніх комп'ютерах, використання погано захищеного домашнього інтернету і незахищених каналів зв'язку (Skype, ZOOM). За спостереженнями фахівців [3] стає очевидним, що при роботі у віддаленому режимі з конфіденційними даними у недобросовісного працівника більше можливостей для різних зловживань, ніж на робочому місці в офісі, де є і системи відеоспостереження, і колеги. Так, наприклад, деякі компанії організують віддалений доступ таким чином, що при цьому примусово підключається відеокамера домашнього комп'ютера співробітника, що фіксує усі його дії в період видаленої роботи в корпоративній мережі. Також можуть виникати ризики, пов'язані з недостатньою захищеністю каналів зв'язку з корпоративною мережею тощо. За даними аналітики INFOSECURITY зараз спостерігається збільшення фішингових атак на корпоративних клієнтів банків а також активізувалися і шахраї, націлені переважно на фізичних осіб, причому, найчастіше це теплі дзвінки. Безумовно, негативну роль в цьому ланцюжку грають численні витoki клієнтських даних з баз даних банків, служб доставки та інших ресурсів але незважаючи на різноманітність прийомів, технічно і технологічно більшість схем базуються на методах маніпулювання поведінкою людей, тобто методах соціальної інженерії (CI) [3].

На відміну від шахраїв ("хакерів"), більшість людей не готова до безпечного життя у цифровому світі. Якщо в звичайному житті дітей учать основам безпеки : не розмовляти з незнайомцями, не відкривати чужим двері, то в цифровій сфері багато дорослих не знають або не розуміють, що є загрозою і несе небезпеку. Дії соціальних інженерів в умовах карантину можуть спричинити нанесення психічної травми та значне погіршення стану здоров'я людини.

За визначеннями наведеними у [5-8], соціальна інженерія – це:

- а) будь-які дії, що спонукають людину зробити те, що може як піти їй на користь так і нанести шкоду [6];
- б) маніпулювання людиною або групою людей з метою злому систем безпеки та викрадення важливої інформації [7];
- в) метод несанкціонованого доступу до інформації шляхом психологічного впливу, маніпулювання та управління діями людини з метою змусити її скоїти бажане [8];
- г) метод управління діями людини без використання технічних засобів, заснований на використанні слабкостей людського фактору [8];
- е) «цей термін є синонімом диктатури й тоталітарної тиранії. Ідея полягає у тому, щоб поводитися з людськими істотами так само, як інженер поводить з матеріалом, з якого він буде мости, дороги і машини. Воля соціального інженера має замінити волю багатьох людей, яких він планує використати для побудови своєї утопії» [7].

Узагальнюючи визначення можна зробити висновок, що соціальний інженер (СІ) здійснює психологічний вплив на людину з метою спонукати людину для вчинення деяких дій.

Вплив соціальної інженерії може бути не шкідливим, якщо використовуються методи СІ з дозволу самої людини чи керівника підприємства з метою виявити та усунути недоліки у політиці безпеки [6].

Але методи СІ можуть бути використані зловмисниками із метою заволодіти інформацією або іншими цінностями, що може завдати матеріальної або моральної шкоди людині.

У роботі [7] Крістофера Хеднегі дії соціальних інженерів представлені у вигляді піраміди СІ (рис. 1).



Рис. 1 – Піраміда СІ

На етапі підготовки СІ визначає чи легко потенційна жертва заводить нові знайомства, чи є вона товариською. Визначається коло інтересів людини. Наприклад, якщо жертва полюбляє відвідувати кафе, бари, паби, то СІ також може їх відвідувати і в процесі частих перетинань зав'язати дружні відносини. Іноді жертва знаходиться в тяжкому матеріальному та/або психологічному стані тоді встановити довірчі відносини стає легше. Виникнення умов для цього може бути забезпечено зловмисником). В цьому випадку СІ надає допомогу людині, і спочатку нічого не просить взамін. Жертва, через несподівану безкорисливу допомогу починає відчувати симпатію та довіру до «рятівника». Потім спілкування може перерости в дружбу, яку СІ використовує у власних інтересах у повному обсязі. Іноді СІ не обов'язково встановлювати довірчі відносини на тривалий строк та підтримувати спілкування довго. Якщо людина має алкогольну, наркотичну або іншу залежність, то СІ може вистачити й одного вечора.

У наш час, при розвитку сучасних інформаційно-комунікаційних технологій (ІКТ) значно розширились можливості агресивного психологічного впливу на особистість у віртуальному світі. Дослідження Бедфордського університету показали, що у останні роки злочинці частіше віддають перевагу кіберпереслідуванню, ніж фізичному переслідуванню [8]. Кіберпереслідуванням називають використання сучасних ІТ для цькування груп людей або окремих осіб, що передбачає систематичне, психологічне насильство, що застосовується до жертви. Це може бути приниження честі та гідності через поширення завідомо неправдивої інформації у віртуальному просторі, пліток, чуток, і компрометуючих матеріалів, які містять провокації, глузування, залякування, прямі образи, насильство та погрози з боку кіберпереслідувача. Ці дії тривають протягом тривалого часу. Метою кіберцькування та кіберпереслідування є нанесення максимальної психологічної шкоди жертві.

Аналітична складова дослідження

З метою виявлення чинників, що здійснюють вплив на здоров'я людини у наслідок дій соціальних інженерів було проведено дослідження. На базі проведеного аналізу описаного у розділі 1 було розроблено анкету для опитування.

У якості сервісу для опитування було обрано Google Forms. Це зручний сервіс для швидкого створення якісних та інформативних форм для опитування, яким можуть користуватися усі бажаючі без будь-яких проблем. Відсутність необхідності у реєстрації та її швидке завантаження дозволяє охопити велику аудиторію [7].

Orange - це інструмент для візуалізації і аналізу даних з відкритим початковим кодом. Інтелектуальний аналіз даних (Data mining) у Orange здійснюється за допомогою візуального програмування або сценаріїв Python. Сценарії Python можуть виконуватися у вікні терміналу, інтегрованих середовищах, таких як PyCharm і PythonWin, або оболонках, таких як iPython. Цей інструмент містить компоненти для машинного навчання, доповнення для біоінформатики і інтелектуального аналізу тексту, а також безліч функцій для аналізу даних. Orange складається з інтерфейсу Canvas, на який користувач поміщає віджети і створює робочий процес аналізу даних.

Віджети пропонують базові функції, такі як читання даних, відображення таблиці даних, вибір функцій, предиктори навчання, порівняння алгоритмів навчання, візуалізація елементів даних і т. д. Користувач може інтерактивно досліджувати візуалізацію або передавати вибрану підмножину в інші віджети.

У Orange процес аналізу даних може бути розроблений за допомогою візуального програмування. Orange запам'ятовує вибір, пропонує часто використовувані комбінації. Orange має функції для різної візуалізації, таких як діаграми розсіяння, гістограми, дерева, дендрограми, мережі і теплові карти.

Комбінуючи віджети, можна створити структуру аналітики даних. Існує більше 100 віджетів з охопленням більшості стандартних і спеціалізованих завдань аналізу даних для біоінформатики.

Навчання базових наборів навчальних даних включає прогнози окремих моделей, щоб досягти максимальної точності. Моделі можуть бути отримані з різних вибірок навчальних даних [8].



У опитуванні взяли участь жінки та чоловіки віком від 18 до 59 років (рис. 2).



Рис. 2 – Вік (а) та стать (б) опитуваних

На питання «Що таке соціальна інженерія?» 20% опитуваних відповіли, що не знають. Обробка даних методами ІАД за допомогою Orange допомогло виявити факт, що такі є і серед жінок і серед чоловіків у всіх вікових групах.

Наступні питання були спрямовані на виявлення проценту опитуваних, що розуміють чи стикались вони із різними методами впливу СІн. Аналіз даних показав, що 36% опитуваних стикались із шантажем, причому 5% виконали умови шантажистів щоб компрометуюча інформація про них або знайомих не була розповсюджена. Це були чоловік і жінка віком від 19 до 29 років. 35% опитуваних стикались із залякуванням, ніхто з опитуваних не виконав вимоги і у 2 % людей погрози були здійснено. Майже 40% опитуваних стикались із проявами фальшивої дружби або фальшивого кохання. Майже 36 % опитуваних пережили розповсюдження про них неправдивої інформації із метою тиску. Наступний блок питань показує процент опитуваних, що стикались із нав'язливими дзвінками із вимогами, їх частоту та тривалість. Таким чином, 32% опитуваних отримували нав'язливі дзвінки. Від 12% до 15% опитуваних потерпали через них більш за пів року отримуючи 50 та більше дзвінків на день. 30% опитуваних отримували дзвінки через незнайому людину. Наступні питання характеризують вплив на здоров'я опитуваних зазначених у попередніх питаннях дій. 26% опитуваних зазначили, що було важко перенести вказаний вплив, але вважають що проблем зі здоров'ям в них не виникло. 8% опитуваних поскаржились на проблеми зі здоров'ям. 11% зазначили, що схудли, 13%, що набрали вагу. Не дивлячись на те, що більшість вважає, що не отримала проблем зі здоров'ям великий відсоток людей зазначили, що відчували почуття, що відносять до характеристик психічної травми. 40 % людей отримали короткотривалий стан безпорадності, 29 % отримали безсоння, 26% отримали відчуття жаху, 16 % отримали панічні атаки, 12% опитуваних навіть мали думки про суїцид, а 10% здійснили спробу суїциду. Наступні питання показали як опитувані справлялись із отриманими проблемами. Наступні діаграми (рис. 3-4) показують які методи подолання психічної травми використовували опитувані як опитувані справлялись із отриманими проблемами.

Якщо Ви стикались із ознаками психічної травми які методи подолання Ви використовували (можна обрати декілька варіантів)

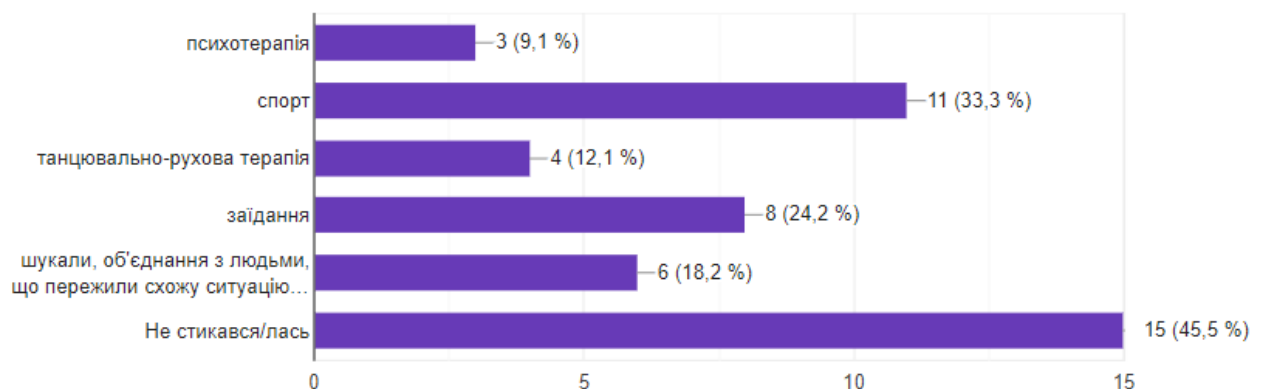


Рис. 3 – Діаграма методів подолання психічної травми

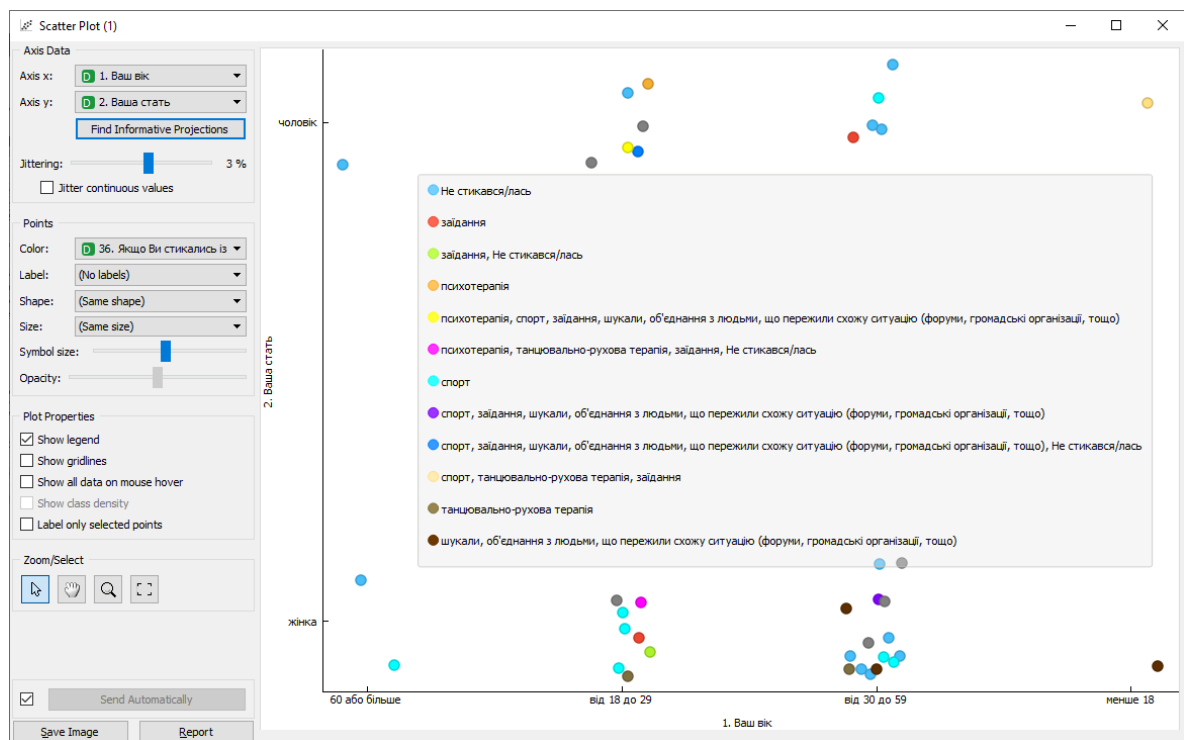


Рис. 4 – Діаграма методів подолання психічної травми за категоріями

Програмна складова дослідження

Результати дослідження було впроваджено у аналітичну платформу KitStat у якості оновлення, що являє собою розробку блоку «Аналітика СІ. Блок Впливу на здоров'я».

Інформаційна модель програмної підтримки дослідження представлена на рисунку 5.

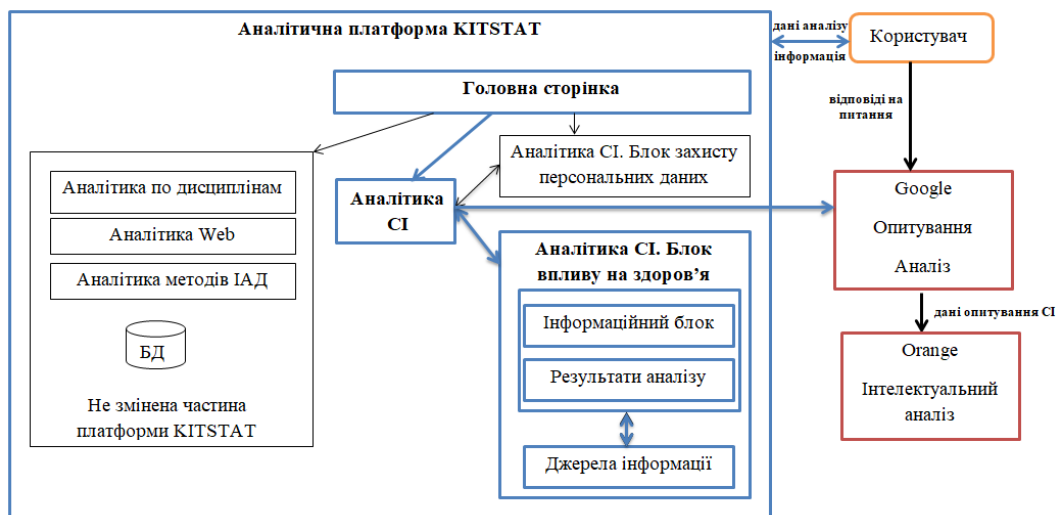


Рис. 5 – Структура оновленої системи KitStat

Система KitStat розроблена із використанням таких технологій як мова розмітки HTML5, таблиця стилів CSS3, мова програмування JavaScript, мови PHP. Вона розміщена на хостингу та є діючою. Це обумовило обрання саме цих інструментів при здійсненні програмної підтримки даного дослідження.

Система KitStat розроблена із використанням таких технологій як мова розмітки HTML5, таблиця стилів CSS3, мова програмування JavaScript, мова PHP. Вона розміщена на хостингу та є діючою. Це обумовило обрання саме цих інструментів при здійсненні програмної підтримки даного дослідження.

Результати роботи було впроваджено у якості оновлення у аналітичну платформу KitStat, що дозволяє надати інформацію про наступне.

1. Методи соціальної інженерії (рис. 6) .



ВПЛИВ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ЗДОРОВ'Я ЛЮДИНИ

Узагальнюючи визначення можна зробити висновок, що соціальний інженер (СІ) здійснює психологічний вплив на людину з метою спонукати людину для вчинення деяких дій.

Методи соціальної інженерії

Шантаж - це метод впливу, в процесі якого людину ставлять перед вибором: або вона виконує усі вимоги шантажиста, або інформація, що може її зганьбити та/або підірвати до неї довіру, буде повідомлена певним особам. Компрометуюча інформація стосовно потенційної жертви може бути виявлена або підготовлена (сфабрикована) у процесі збору інформації про неї. Можливі випадки, коли СІ режисує подію у якій потенційна жертва має взяти участь, та ставши учасником якої, остання своїми діями зробить на себе компромет або ж соціальний інженер може інсценувати якісь події, участь у яких потенційна жертва не приймала, але це участь дуже правдоподібно приписується їй. В останні роки відомі часті случаи, коли СІ фабрикують неправдиву компрометуючу інформацію про людину використовуючи дійсні фото та відомості про людину в обробці технічними засобами.

Підкуп - це взаємовигідний обмін, коли за реальне сприяння або згоду співпрацювати об'єкт отримує певну винагороду [13]. У якості винагороди при підкупі зазвичай виступають матеріальні цінності: гроші, коштовності, нерухомість, предмети антикваріату (картини, книги, прикраси, тощо), колекційні предмети, транспортні засоби, радіоелектронна апаратура, засоби зв'язку і т. д., сприяння об'єкту та/або його родичам та близьким: просування по службі, отримання керівних посад, допомога у вирішенні юридичних питань, доступ до вищих навчальних закладів, отримання документів (паспортів, закордонних паспортів, віз, різноманітних довідок та дозволів) і т. д.; можливі потреби об'єкта (алкоголь, наркотичні засоби). СІ може штучно створити певні умови, за яких у людини з'явиться або збільшиться потреба в тому, що згодом він їй може запропонувати.

Залюквання (погроза) – це метод впливу, в процесі якого до людини та/або до її близьких застосовують фізичне або психологічне насилля з метою злому її волі і подальшого підпорядкування іншій особі. На відміну від шантажу, при залюкванні, компрометуюча інформація не використовується. При залюкванні соціальний інженер в якості мішені впливу використовує почуття страху людини за себе, здоров'я та життя своїх близьких, за збереження свого майна, за свою

Рис. 6 – Сторінка оновленої системи KitStat присвячена впливу на здоров'я людини

2. Результати дослідження станом на листопад 2021 (рис. 7). При натисканні на посилання можна перейти на сторінку використаних при дослідженні джерел.

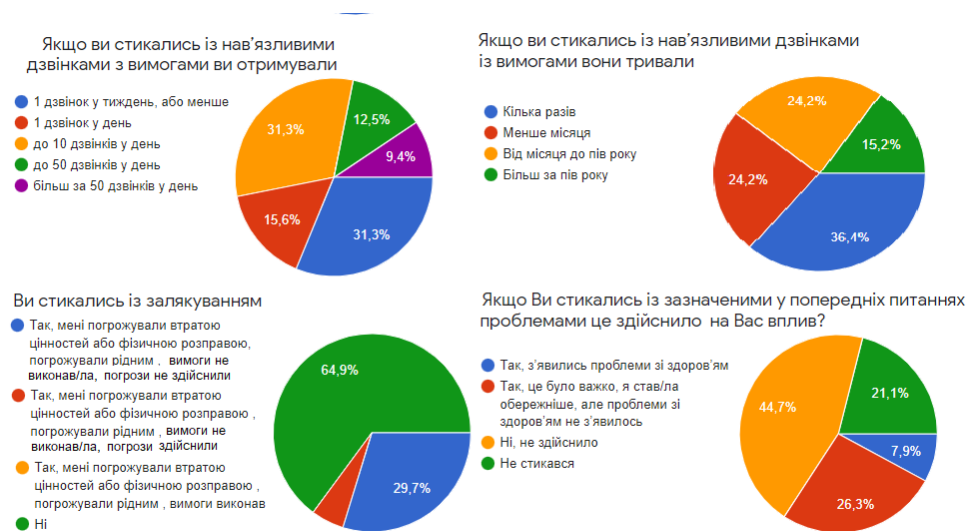


Рисунок 7 – Сторінка оновленої системи KitStat присвячена впливу на здоров'я людини. Результати дослідження

На цю сторінку також можна потрапити з головної сторінки платформи KitStat натиснувши на пункт меню CI (рис. 8).

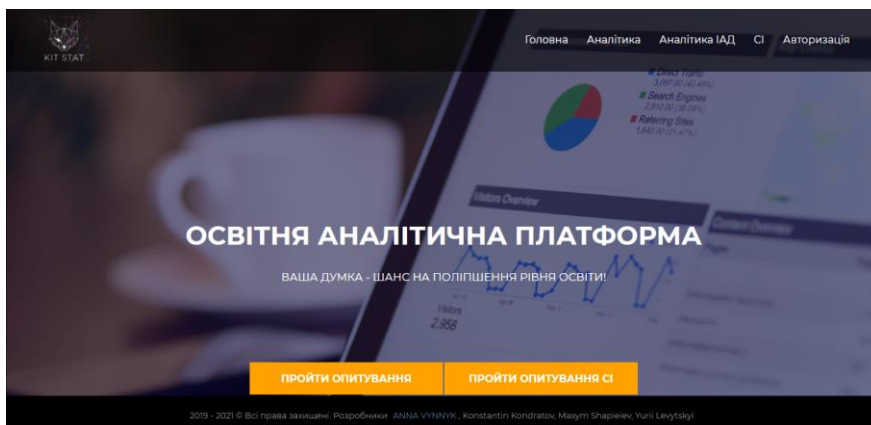


Рис. 8 – Головна сторінка оновленої системи KitStat



Доступ до оновленої аналітичної платформи KitStat можна отримати за посиланням: <https://stat.kitkb.co.ua/>.

Висновки

В результаті роботи виконано досліджено основні проблеми що виникають із здоров'ям людей у наслідок впливу СІ; визначення терміну соціальна інженерія, його популярність, алгоритм дії соціальних інженерів (СІн), джерела інформації про людину якими може скористатись СІн, метод впливу СІ на людину, види агресивного психологічного впливу на особистість у кіберпросторі, засоби подолання наслідків впливу методів СІ на людину, інформаційні системи, що інформують про методи СІ та їх вплив на здоров'я людини. Виявлено чинники, що впливають на здоров'я людини від дій СІн. Розроблено модель впливу СІ на здоров'я людини та вдосконалено систему KitStat, що може бути використана для отримання інформації за тематикою та допомагає накопичувати дані для подальшого дослідження.

Перелік використаних джерел

- [1]. Социальная инженерия – как не стать жертвой [Електронний ресурс] // EFSOL. – 2021.
- [2]. Психологічна травма і шляхи її подолання [Електронний ресурс] // Марківська районна рада. – 2021. – Режим доступу до ресурсу: <http://markivska.rayrada.org.ua/stattya-na-temu-psihologichna-travma-i-shlyahi-ii-podolannya-10-35-44-09-11-2016/>.
- [3]. Хэднеги К. Искусство обмана. Социальная инженерия в мошеннических схемах / Кристофер Хэднеги; пер. с англ. – Київ: Альпина Паблішер, 2020. – 430 с.
- [4]. Чалдіні Р. Б. Психологія впливу / Роберт Б. Чалдіні. – Харків: Книжковий Клуб "Клуб Сімейного Дозвілля", 2017. – 352 с.
- [5]. Людвиг фон Мизес. Человеческая деятельность: трактат по экономической теории / Людвиг фон Мизес., 2012. – 878 с.
- [6]. Семернін Д. О. Протидія методам та засобам соціальної інженерії : 125 «Кібербезпека» / Семернін Д. О. – Харків, 2020. – 78 с.
- [7]. Google Analytics [Електронний ресурс] // Calltouch. – 2020. – Режим доступу до ресурсу: <https://www.calltouch.ru/glossary/google-analytics/>.
- [8]. Varenia V. Интеллектуальный анализ данных — используем Orange [Електронний ресурс] / Viacheslav Varenia // pro100blogger. – 2019. – Режим доступу до ресурсу: <https://pro100blogger.com/2019/06/yntellektualnyj-analiz-dannyh-yspolzuem-orange.html>.

References

- [1]. Sotsyalnaia ynzheneriia – kak ne stat zhertvoi [Elektronnyi resurs] // EFSOL. – 2021.
- [2]. Psykholohichna travma i shliakhy yii podolannia [Elektronnyi resurs] // Markivska raionna rada. – 2021. – Rezhym dostupu do resursu: <http://markivska.rayrada.org.ua/stattya-na-temu-psihologichna-travma-i-shlyahi-ii-podolannya-10-35-44-09-11-2016/>.
- [3]. Khədnehy K. Yskusstvo obmana. Sotsyalnaia ynzheneriia v moshennycheskykh skhemakh / Krystofer Khədnehy; per. s anhl. – Kyiv: Alpyna Pablysher, 2020. – 430 s.
- [4]. Chaldini R. B. Psykholohiia vplyvu / Robert B. Chaldini. – Kharkiv: Knyzhkovyi Klub "Klub Simeinoho Dozwillia", 2017. – 352 s.
- [5]. Liudvyh fon Myzes. Chelovecheskaia deiatelnost: traktat po ekonomycheskoi teoryi / Liudvyh fon Myzes., 2012. – 878 s.
- [6]. Semernin D. O. Protydiia metodam ta zasobam sotsialnoi inzhenerii : 125 «Kiberbezpeka» / Semernin D. O. – Kharkiv, 2020. – 78 s.
- [7]. Google Analytics [Elektronnyi resurs] // Calltouch. – 2020. – Rezhym dostupu do resursu: <https://www.calltouch.ru/glossary/google-analytics/>.
- [8]. Varenia V. Yntellektualnyy analiz dannykh — yspolzuem Orange [Elektronnyi resurs] / Viacheslav Varenia // pro100blogger. – 2019. – Rezhym dostupu do resursu: <https://pro100blogger.com/2019/06/yntellektualnyj-analiz-dannyh-yspolzuem-orange.html>.

Отримана в редакції 15.04.2022. Прийнята до друку 29.05.2022. Received 15 April 2022. Approved 29 May 2022. Available in Internet 15 June 2022.