УДК 004.056.52: 159.942

ДОСЛІДЖЕННЯ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ. ЧАСТИНА 2. ВПЛИВ НА ЗДОРОВ'Я ЛЮДИНИ.

Шапеєв М.О.[1], Селіванова А.В.[2]

[1,2] Odessa National University of Technology, Odessa, Ukraine
ORCID: [2]https://orcid.org/0000-0002-3395-1422
E-mail: [2]alikasalvano@gmail.com

DOI: 10.15673/atbp.v14i3.2353

Анотація. *Представлена стаття присвячена дослідженню методів захисту персональних даних від впливу соціальних інженерів (СІн). В процесі роботи досліджено види персональних даних та способи їх потрапляння у мережу, методи захисту даних у мережі, методи соціальної інженерії (СІ) та методи захисту від СІ, проведено аналіз інформаційних ресурсів, що містять інформацію про соціальну інженерію та захист даних. Проведено збір даних методом опитування, що характеризує поведінку людей із персональними даними, зокрема при використанні мережі Інтернет. Отримані дані оброблені за допомогою засобів інтелектуального аналізу даних із використанням інструментальних засобів Google та Orange. Розроблено модель безпечної поведінки для збереження даних у мережі, використання якої значно ускладнить доступ соціальних інженерів до персональних даних 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.*

Abstract. *The presented article is devoted to the study of methods of protecting personal data from the influence of social engineers (SIN). In the course of the work, the types of personal data and ways of their entry into the network, methods of data protection in the network, methods of social engineering (SI) and methods of protection against SI were investigated, information resources containing information about social engineering and data protection were analyzed. Data collection was carried out by the survey method, which characterizes the behavior of people with personal data, in particular when using the Internet. The received data is processed with the help of intelligent data analysis tools using Google and Orange tools. A model of safe behavior has been developed for saving data on the network, the use of which will significantly complicate the access of social engineers to personal data of a person. 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.*

Ключові слова: соціальна інженерія, інтелектуальний аналіз даних, інформаційні технології, хакерська атака, метод k - середніх

Key words: social engineering, intelligent data analysis, information technology, hacker attack, k-means method

ВСТУП

Одним з найбільш проблемних правових питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглиненому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу (в тому числі незаконно) [1]. На даний час більшість людей різного віку активно використовують різноманітні електронні сервіси і розуміючи це чи ні лишають свої персональні дані у відкритому доступі. З розвитком технологій, одним з найпопулярніших методів шахрайства стала соціальна інженерія (СІ). Цим терміном називають будь-які психологічні маніпуляції над людиною, за допомогою яких можна отримати доступ до конфіденційної інформації про жертву. Здебільшого ця інформація використовується для крадіжки грошей у користувача безпосередньо або виманювання їх під різними приводами. Захист персональних даних у мережі стає найактуальнішою задачею сьогодення тому аналіз методів захисту персональних даних у мережі від впливу соціальних інженерів є актуальним напрямком дослідження.

Актуальність тематики дослідження

В Україні багато політичних та правових питань що пов'язані із активним розвитком сфери ІТ є неврегульованими. Стрімка поява та розвиток цифрових технологій призвели до того, що рівень небезпеки у мережі значно зріс,

підвищилась якість загроз та ризиків. Вони виявляються настільки всеосяжними і складними, що їм не можливо протидіяти за допомогою норм діючого права. На цій основі виник новий вид злочинності — організована кіберзлочинність. Таким чином , держава з метою запобігання загрозам, вимушена приділяти увагу в інформаційно-комунікаційній сфері наступним напрямкам: захист персональних даних людини; безпека ІК-ергосистем, державних структур; захист технологій та робочого середовища. Персоналізація багатьох видів послуг та розширення цифрових сервісів значно підвищили загрозу шахрайства з боку широкого кола провайдерів або користувачів, а ризики витоку інформації вимагають постійної уваги до підвищення рівня захисту електронних систем [2].

Відповідно до цивільного кодексу України фізична особа має право вільно зберігати, збирати, використовувати і поширювати інформацію. Збирання, використання, зберігання і поширення інформації про особисте життя фізичної особи допускаються лише за її згоди, окрім випадків, що визначені законом, і тільки в інтересах економічного добробуту, національної безпеки та прав людини. Фізична особа, що поширює інформацію, зобов'язана переконатися в її достовірності. Фізична особа, що поширює інформацію, отриману з офіційних джерел (інформація органів місцевого самоврядування, органів державної влади, стенограми, звіти тощо), не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування. Фізична особа, що поширює інформацію, отриману з офіційних джерел, зобов'язана робити посилання на таке джерело.

У Законі України «Про захист персональних даних» дано наступне визначення терміну персональні дані. Це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Суб'єктом персональних даних є фізична особа, персональні дані якої обробляються. Згодою суб'єкта персональних даних можна вважати добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних надається під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки [1].

За даними Української асоціації міжбанківських платіжних систем, у 2019 році шахраям вдалося викрасти з банківських карток користувачів всередині країни понад 360 млн грн. До того ж найпопулярнішим методом крадіжки виявилася соціальна інженерія. Сьогодні більшість сервісів мають можливість провести двофакторну автентифікацію, — підтвердження будь-якої дії через мобільний телефон користувача. Саме тому доступ до чужого телефону став головною метою для шахраїв [3].

З огляду на вищесказане аналіз існуючих види персональних даних, методів їх потрапляння у мережу, способи захисту, методи соціальної інженерії та методи захисту від дій соціальних інженерів є актуальним напрямом дослідження.

Аналіз публікацій

Проблемам захисту персональних даних присвячено роботи багатьох вчених зокрема В.Г. Пилипчук, В.М. Брижко, О.В. Гронь, А.К. Погореленко, Л.О. Шапенко, Я.А. Семенюк, Ю.І. Крилової, І. Яворської, М. Микієвич та ін.

У статті Пилипчука В. Г. та Брижка В. В. [4] проаналізовані історико-правові аспекти формування національного законодавства з питань захисту персональних даних, процеси трансформації та нові правові стандарти Європейського Союзу у цій сфері, розглянуто проблеми захисту приватності, прав і безпеки людини в умовах розбудови інформаційного суспільства, а також надано пропозиції щодо розвитку системи захисту персональних даних у контексті євроінтеграції України.

У статті Гронь О. В. та Погореленко А. К. [5] проведено аналіз європейських законодавчих основ та принципів захисту персональних даних, що становлять основу сучасної практики в цій сфері. Викладено базові положення української системи правового захисту персональних даних. Визначено правові підстави для реалізації та захисту інтересів суб'єкта персональних даних. Окреслено подальші напрями вдосконалення системи захисту персональних даних.

У роботі Шапенко Л. О. та Семенюк Я. А. [6] висвітлено загрози протиправного використання персональних даних при використанні нових інформаційно-комунікаційних технологій.

У роботі [7] представлено методику протидії соціальному інжинірингу на об'єктах інформаційної діяльності.

До персональних даних відносять такі відомості, по яких може бути ідентифікована або ідентифікується фізична особа. Зокрема, ім'я, прізвище, по батькові, адреса, паспортні дані, національність, телефони, освіта, сімейний стан, світоглядні та релігійні переконання, матеріальний стан, стан здоров'я, місце і дата народження, місце перебування та проживання тощо. Також до персональних даних відносять дані про особисті немайнові та майнові відносини цієї особи з іншими особами, зокрема членами сім'ї. Крім того, до персональних даних можна віднести відомості про явища та події, що відбуваються або відбувались у побутовому, товариському, інтимному, діловому, професійному та інших сферах життя особи (за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану із здійсненням функцій держави або органу місцевого самоврядування) тощо.

В наш час мають велику популярність різні соціальних мережі і дуже частим є опублікування фото та відео що дуже часто порушують права стосовно особистих даних фізичної особи. Практично кожний має доступ до фото та

відео альбомів, розміщених у мережі Інтернет. Це дозволяє будь-кому ознайомитись з великою кількістю власних фотографій та відеофайлів, що часто може спричинити порушення особистої інформації людини, у зв'язку з неправомірним розміщенням її персональних даних. Правовідносини у галузі захисту персональних даних на законодавчому рівні регулюються Цивільним кодексом України [8] та рядом інших законів. В цілому, фізична особа може бути знята на фото виключно за її особистої згоди. Разом з тим, законом передбачений виняток: якщо фотозйомка проходить відкрито на вулиці, мітингах, зборах або на інших заходах, що носять публічний характер, така згода не є обов'язковою.

Якщо після надання згоди на фотозйомку, фізична особа відмовляється від публічного показу своїх фотографій, то подальша відмова від їх публічного показу можлива лише в тій частині, що стосується особистого життя особи.

Відповідно до положення статті 308 ЦК України фотографії та інші твори, на яких зображено фізичну особу, можуть бути розповсюджені, публічно показані або відтворені, лише за згодою цієї особи.

Відтворенням законодавець вважає навіть розміщення зображення на веб-сайті в мережі Інтернет.

Положення Закону України «Про захист персональних даних» [9] окремо не виділяють під поняттям «персональні дані» фотографії. Поняття «персональні дані», що закріплене у статті 2 вищевказаного Закону, вказує, що персональні дані - це відомості чи сукупність відомостей про фізичну особу, яка може бути ідентифікована. Таким чином, по фотографіям може бути встановлено певну особу, а отже, вони підпадають під визначення персональних даних [10].

Громадяни часто ігнорують проблеми, пов’язані із захистом персональних даних через низький рівень правової обізнаності. Звичайна людина, підписуючи документи різного роду стає учасником інформаційних відносин і часто вимушена поставити себе у нерівні права у порівнянні з іншою стороною, а інколи навіть може потрапити у своєрідну рабську залежність якогось банка, «товариства», супермаркетам, тощо. Продаючи за копійки конфіденційну інформацію, недосвідчена особа навіть не уявляє, ким і задля чого її персональні дані будуть використані.

У ході дослідження описаного у [11] виявлено, що найчастіше персональні дані з використанням веб-ресурсів обробляються в рамках таких процесів як:

- заповнення відвідувачами веб-ресурсів анкет;
- реєстрація та отримання логіна та пароля;
- реєстрація з використанням облікового запису соціальної мережі;
- надання електронної адреси відвідувача для зворотного зв’язку.

У того ж дослідження [11] з’ясовано, що у соціальних мережах зазвичай реєстрація проводиться із врахуванням введення даних, відповідно до яких особа може бути ідентифікована:

- ім’я та прізвище;
- географічні об’єкти, місце навчання;
- телефонні номери.

Всі ці дані про особу заповнюються суб’єктом персональних даних без попередження про їх можливе користування в процесі функціонування сторінки в соціальній мережі.

Для збору необхідних відомостей про людину та/або організацію соціальний інженер (СІн) може також скористатись відкритими джерелами.

Більшість відкритих державних баз даних та реєстрів, якими може скористатись СІн для пошуку необхідної інформації, розміщені на єдиному державному веб-порталі відкритих даних (data.gov.ua). Згідно [12] на data.gov.ua представлені 34 895 наборів даних, пошук серед яких можна здійснювати за ключовими словами, назвами, певними групами, розпорядниками (центральними, місцевими та іншими).

Наприклад, до наборів даних корисних для соціального інженера можна віднести:

- єдиний реєстр нотаріусів, що містить регіон, назву організації, контактні дані, ПІБ, номер свідоцтва нотаріуса;
- єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, що містить перелік юридичних та фізичних осіб- підприємців;
- реєстр громадських об‘єднань, що містить реєстраційний номер запису, найменування громадського об‘єднання, ЄДРПОУ, ПІБ/найменування засновників;
- реєстр громадських формувань, що містить підсистеми «Політичні партії», «Благодійні організації», «Творчі спілки», «Торгово-промислові палати», Постійно діючі третейські суди», «Статути», Асоціації місцевого самоврядування»;
- відомості про транспортні засоби та їх власників;
- єдиний реєстр боржників (хоча він також доступний і на erb.minjust.gov.ua).

Для полегшення пошуку певних відомостей існують спеціальні інтернет-сервіси такі як Namechk, Pipl, Searchface, KnowEm, Findface, що дозволяють знайти певні відомості про людину за наявності у зловмисника певної інформації, наприклад про адресу електронної пошти, номер телефону, нікнейм, за наявності фотографії (зазвичай такі сервіси видають посилання на сторінки людини у соціальних мережах, які прив’язані до цієї інформації). Існує спеціальне програмне забезпечення, що призначено для збору інформації з різних інтернет-джерел та баз даних, а також її представлення в зручному для розуміння форматі наприклад, Maltego.

Великий об'єм інформації СІн може отримати з метаданих, що є складовою частиною будь-яких електронних документів, відео, графічних та музичних файлів. Метадані автоматично додаються до файлів і можуть містити, в залежності від виду файлу, наступні відомості: дату та час його створення/відкриття/редагування, ім'я автора і користувачів, які відкривали та/або редагували файл, загальний час витрачений на його редагування, версію/модель та технічні характеристики програми/пристрою, у якій/за допомогою якого був створений документ/файл, місце розташування (у разі включеної геолокації на пристрої), теги та ключові слова, що описують зміст файлу та іншу інформацію.

Існує багато програм та інтернет-сервісів, що дозволяють зчитувати та/або редагувати метадані. Переглянути/редагувати/видалити метадані файлів, при використанні операційної системи Windows, можна також у властивостях файлу, наприклад фото.

За допомогою спеціальних інтернет-сервісів, наприклад, таких як карти Google, можна визначити місце зйомки за координатами.

В деяких випадках зловмиснику необхідно добути дуже важливу але доволі специфічну для успішної реалізації впливу на жертву інформацію, таку як: IP-адреса, User, операційну систему тощо. Отримати цю інформацію можна багатьма способами, наприклад, шляхом: звернення до провайдера жертви, особистої бесіди з нею, аналізу мережевого трафіку, створенням свого інтернет-ресурсу, використання спеціальних інтернет-сервісів.

Згідно [18] за допомогою онлайн-сервісу canarytokens.org можна створити спеціальну мітку (канарітокен, токен, ханітокен, ханіпот), що дозволяє вбудувати/замаскувати її в/під такі об'єкти:

- зображення (картинку);
- документ в форматі PDF;
- документ Microsoft Word;
- посилання (URL);
- виконуваний файл (.exe);
- адресу електронної пошти (несправжню);
- QR-код;
- інше;

При спробі завантаження зображення, відкриття документів, запуску виконуваного файлу, при надходженні листа на несправжню адресу електронної пошти, при здійснені переходу за QR-кодом чи посиланням людині, що створила токен (мітку), на вказану при його створенні адресу електронної пошти, прийде повідомлення про те, що токен спрацював. Із отриманого повідомлення можна отримати наступну інформацію:

- позначення токена;
- дату та час взаємодії з об'єктом (перехід за посиланням відкриття документу, тощо);
- коментар для ідентифікації (може задаватися під час створення токену);
- тип токену: в залежності від об'єкту, наприклад ms_word;
- IP-адреса, з якої здійснювалася взаємодія з об'єктом (звісно, при використанні VPN або TOR-браузеру інформація може не відповідати дійсності);
- User Agent користувача, який здійснив взаємодію з об'єктом;
- орієнтовне розташування користувача, що здійснив взаємодію з токеном: місто, область, країна (з вказівкою орієнтовної точки на карті);
- інтернет-провайдер [18];

Інтернет-сервіс grabify.link дозволяє створити посилання на реальний інтернет-ресурс у замаскованому вигляді (це робиться для того, щоб інтернет-сервіс зміг зафіксувати факт переходу за посиланням і зберегти певну інформацію стосовно користувача, який його здійснив). Таким чином, ніби обману немає, користувач потрапляє туди, куди й хотів потрапити, але перед цим grabify.link записує інформацію у журнал стеження. Переглянути цей журнал можна на сайті grabify.link шляхом введення спеціального трекінгового коду або за прямим посиланням до журналу відстеження (формується на етапі створення спеціального посилання). Запис в журналі містить наступну інформацію про користувача, що перейшов за посиланням:

- IP-адресу;
- дату та час здійснення переходу;
- країну;
- часовий пояс;
- мало місце чи ні використання VPN або Proxy-серверу для зміни IP-адреси;
- орієнтацію екрану пристрою;
- чи здійснювався перехід за допомогою режиму інкогніто;

- розкладку клавіатури (мову);
- чи використовується блокувальник реклами;
- розширення екрану;
- браузер, що використовується;
- графічний процесор пристрою;
- User Agent;
- операційна система;
- наявність сенсорного екрану;
- інтернет-провайдер [18].

Методи захисту даних у мережі

З даними Міністерства цифрової інформації України є 5 основних порад, як убезпечити свої персональні дані у мережі [12]:

1. Не надавати свої дані нікому. Не припадати на заманливі пропозиції типу «Саме ваш номер може виграти приз». Не реагувати на смс-повідомлення з подібним змістом. Найчастіше такі пропозиції надають шахраї.
2. Перевіряти інформацію. Не поширювати новини із занадто гучними заголовками. Також не менш важливо перевіряти інформацію, якщо просять пожертвувати гроші на якусь операцію чи зробити репост посту із новиною подібного змісту.
3. Захищати паролі. Не використовувати один пароль для доступу до різних ресурсів. Міняти паролі з певною частотою, використовувати для цього спеціальні менеджери паролів (приміром, 1password, LastPass або KeePass). Зберігати паролі в надійному місці, а краще — запам‘ятовувати.
4. Використовувати двохфакторну автентифікацію. Google, Facebook, Instagram та ін. якісні сервіси надають таку можливість. Завершувати сеанс одразу після виходу із соцмережі.
5. Користуватись офіційними програмами. Перевіряти програми, що завантажуються. Завантажувати з офіційних джерел. Офіційні програми проходять перевірку на наявність фішингу — несанкціонованого збору та передачі даних. Тож, користуючись саме офіційним програмним забезпеченням, можна бути впевненим, що комп’ютер чи смартфон не буде зараженим якимось вірусом. Також необхідно використовувати лише перевірені мережі інтернет-з’єднання.

Методи соціальної інженерії

У 2019 році Zogby Analytics провело опитування для Національного альянсу з кібербезпеки США. В ході опитування було виявлено, що велика кількість компаній усвідомлюють, що вони є потенційними цілями кіберзлочинців. Зокрема, 44% (майже половина) компаній з числельністю працівників 251-500 заявили, що стикалися з випадками втрати даних протягом останніх 12 місяців. Також опитування показало, що 88% представників малого бізнесу вважають, що вони є принаймні «ймовірною» ціллю для кіберзлочинців, у тому числі 46% (майже половина), вважають, що вони є «дуже ймовірною» ціллю.

За оцінками Центру прийому скарг на шахрайство в Інтернеті при ФБР, лише в 2018 році внаслідок кібератак американські компанії втратили понад 2,7 мільярда доларів, в тому числі 1,2 мільярди доларів внаслідок атак з використанням компрометації ділової переписки компрометації електронних листів, які дозволяли несанкціоновано переказувати кошти.

Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — спам та фішинг.

Спам — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення, SMS та соціальні мережі. Власне, спам не є соціальною інженерією, однак в деяких кампаніях використовуються його види, такі як фішинг, цілеспрямований фішинг (spearphishing), вішинг (vishing), смішинг (smishing), а також поширення шкідливих вкладень або посилань.

Фішинг — це форма кібератаки, під час якої злочинець намагається завойовувати довіру до жертви для виманювання конфіденційної інформації. Для отримання даних зловмисники також створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути націлені на велику кількість випадкових користувачів або конкретну особу чи групу.

Цілеспрямований фішинг — це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях.

Видавання себе за іншу особу є іншим популярним методом соціальної інженерії, під час якого кіберзлочинці діють нібито від імені певної особи, вводячи в оману потенційних жертв. Типовим прикладом є зловмисник, який видає себе за генерального директора певної компанії, укладає та затверджує шахрайські угоди в той час, як справжній генеральний директор перебуває у відпустці.

Шкідливе програмне забезпечення, ціль якого викликати у жертви почуття страху чи тривоги та таким чином змусити її встановити небезпечний код на пристрій. Поширеними є випадки, коли користувачам відображалось повідомлення про нібито інфікування пристрою загрозою, для видалення якої необхідно завантажити антивірус (який, насправді, є шкідливим програмним забезпеченням).

Вішинг та смішинг — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту. Зокрема, вішинг реалізовується через шахрайські телефонні дзвінки, а для смішингу використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст.

Афери з технічною підтримкою — це, зазвичай, неправдиві телефонні дзвінки або Інтернет-реклама, в якій зловмисники пропонують жертвам послуги служби технічної підтримки. Насправді, кіберзлочинці просто намагаються заробити гроші, продаючи фейкові послуги або усуваючи насправді неіснуючі проблеми.

Кібершахрайство — це схеми зловмисників, у яких часто використовують один або навіть декілька методів соціальної інженерії, описаних вище [13].

У праці [14] Кристофер Хеднегі представляє дії соціальних інженерів у вигляді СІ-піраміди (рис. 1).

Рис. 1 – Піраміда СІ

Збір даних з відкритих джерел є найбільш важливим етапом роботи соціального інженера, фундамент його діяльності. На цей етап йде найбільше часу.

Розробка легенди базується на інформації, що зібрана раніше. На цьому етапі розробляється привід для атаки, вносяться зміни та доповнення в план атаки, готуються інструменти та реквізит.

План атаки проводиться за моделлю трьох «Я»: «Який план СІ», «Яка ціль СІ», «Яка ціль клієнта». Виявляється коли краще проводити атаку, кого необхідно залучити на допомогу.

Проведення атаки та звіт власне основні етапи на яких проводиться атака за планом та готується документація яка може бути використана як для нанесення шкоди так і для побудови стратегії захисту від дії СІ, якщо соціальний інженер був найнятий замовником для перевірки власного підприємства.

Для отримання необхідної інформації про людину соціальний інженер (Сін) може скористатись такими джерелами:

- безпосередньо сама людина (потенційна жертва);
- інші люди з оточення людини (родичі, друзі, знайомі, сусіди, колеги);
- веб-ресурс організації де працює/працювала людина;
- співробітники державних і недержавних установ, які можуть повідомити певні відомості про людину;
- державні і недержавні бази даних (БД), як відкриті так і закриті;
- документи;
- публікації статті, книги, доклади;
- сторінки в соціальних мережах;
- профілі на платформах онлайн оголошень;

- профілі на сайтах для пошуку роботи;
- новинні сайти, блоги, сайти із відгуками;
- форуми за різними тематиками;
- відходи (сміття), та ін.

Методи захисту від СІ

1. *Регулярне навчання з кібербезпеки усіх працівників*, включно з топ-менеджментом та IT-спеціалістами. Таке навчання повинно показувати та моделювати випадки з реального життя, оскільки методи соціальної інженерії розраховані на користувачів з низьким рівнем обізнаності у кібербезпеці.
2. *Сканування на наявність слабких паролів,* які потенційно можуть використати зловмисники для потрапляння до мережі організації. Створення додаткового рівня захисту за допомогою двохфакторної автентифікації.
3. *Впровадження рішень для захисту*, які попереджають про можливі випадки шахрайства, а також повідомляють про виявлення спаму та фішингу.
4. *Створення політики безпеки* з чітким планом дій, які потрібно буде виконати працівникам, якщо вони стикнуться з проявами соціальної інженерії.
5. *Використання спеціальних рішень для централізованого управління корпоративною мережею*, для забезпечення повного огляду мережі, усіх рішень з безпеки та подій для виявлення та знешкодження потенційних загроз [13].

X_4 – недовіра .

У свою чергу обрана модель залежить від наступних чинників (2.2-2.5):

$$X_1 = F(x_1, x_2, x_3, x_4) \quad (2.2)$$

де X_1 – обережне поводження;
x_1 – користуватись офіційними програмами;
x_2 – не підключати до системи невідомі носії інформації (наприклад знайдені);
x_3 – не запускати невідомі файли
x_4 – не викидати чеки після оплати карткою не знищивши дані, що там містяться.

$$X_2 = F(x_5, x_6, x_7, x_8, x_9) \quad (2.3)$$

де X_2 – захист;
x_5 – відключати геолокацію;
x_6 – використовувати двофакторну автентифікацію;
x_7 – не використовувати у паролях особисту інформацію
x_8 – не використовувати один пароль для різних ресурсів
x_9 – змінювати паролі.

$$X_3 = F(x_{10}, x_{11}, x_{12}, x_{13}) \quad (2.4)$$

де X_3 – конфіденційність;
x_{10} – не повідомляти інформацію про себе або рідних незнайомцям;
x_{11} – не зазначати інформацію про себе у СМ на ресурсах підприємств або обмежити до неї доступ;
x_{12} – не викладати свіжі фото у СМ або обмежити доступ до них
x_{13} – не використовувати фото у якості аватара.

$$X_4 = F(x_{14}, x_{15}, x_{16}) \quad (2.5)$$

де X_4 – недовіра;
x_{14} – не переходити за невідомими посиланнями;
x_{15} – не довіряти повідомленням про виграш або необхідність допомоги та ін.;
x_{16} – перевіряти інформацію перед підписом, не використовувати електронний підпис на невідомих ресурсах.

Використання зазначеної моделі не убезпечить вас від дій соціальних інженерів повністю, але зробить процес доступу до вашої інформації значно складнішим та затратним, що допоможе зробити Вас менш цікавими для СІн.

Структура програмної підтримки

Результати дослідження було впроваджено у аналітичну платформу KitStat у якості оновлення, що являє собою розробку блоку «Аналітика СІ. Блок захисту персональних даних» .

Інформаційна модель програмної підтримки дослідження представлена на рисунку 2.

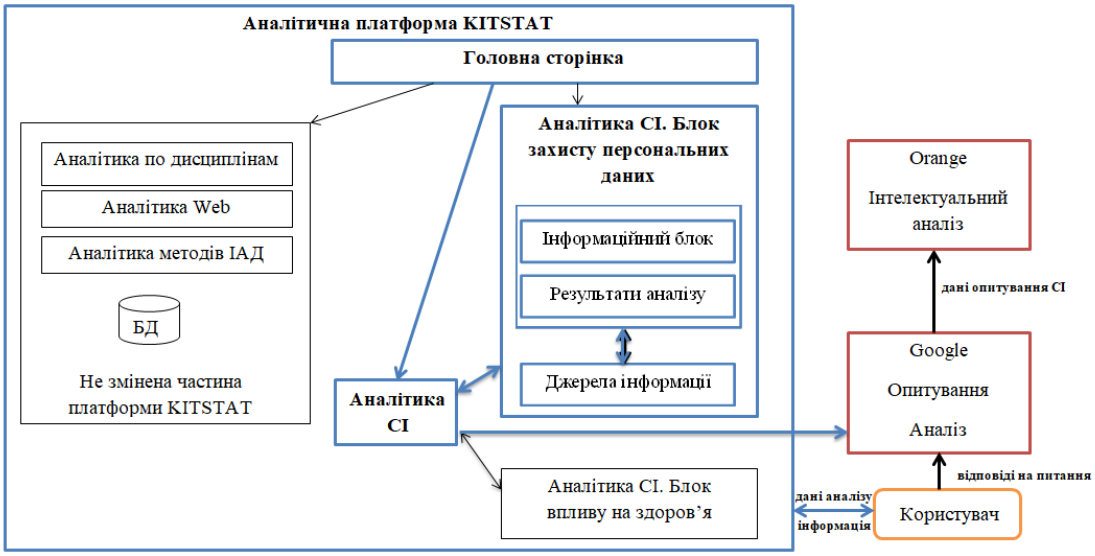

Рис. 2 – Інформаційна модель програмної підтримки дослідження

Практичне значення отриманих результатів

Практичне значення одержаних результатів полягає у тому, що розроблена модель та програмна підтримка дозволить підвищити рівень інформованості людей про методи захисту персональних даних у мережі тим самим підвищивши рівень безпеки у мережі.

Список використаних джерел

[1]. Захист персональних даних: використання, захист та відповідальність [Електронний ресурс] // Координаційний центр з надання правової допомоги: [Веб-сайт]. – 2021. – Режим доступу до ресурсу: https://www.legalaid.gov.ua/publikatsiyi/zahyst-personalnyh-danyh-vykorystannya-zahyst-ta-vidpovidalnist/.

[2]. Цифровізація як нова реальність України [Електронний ресурс] // LexInform: [Веб-сайт]. – 2020. – Режим доступу до ресурсу: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/.

[3]. Не вір нікому. Що таке соціальна інженерія та як не стати її жертвою [Електронний ресурс] // КібербезпекаОнлайн:[Веб-сайт]. – 2021. – Режим доступу до ресурсу: https://kyivstar.ua/uk/cybersecurity/ne-vir-nikomu-shcho-take-socialna-inzheneriya-ta-yak-ne-staty-yiyi-zhertvoyu.

[4]. Пилипчук В. Г. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України / В. Г. Пилипчук, В. В. Брижко. // Вісник Національної академії правових наук України. – 2017. – №3. – С. 36–50.

[5]. Гронь О. В. Проблеми захисту персональних даних у контексті сучасної комунікації / О. В. Гронь, А. К. Погореленко. // Науковий вісник Ужгородського національного університету. – 2018. – №19. – С. 102–108.

[6]. Шапенко Л.О. Захист персональних даних: теоретико-правовий аспект / Л.О. Шапенко, Я.А. Семенюк // Юриспруденція в сучасному інформаційному просторі: матеріали IX Міжнар. наук.-практ. конф., (Київ, 1 березня 2019 р.). – Тернопіль: Вектор, 2019. – С. 124-126.

[7]. Соколов В. Ю. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності / В. Ю. Соколов, Д. М. Курбанмурадов. // Кібербезпека: освіта, наука, техніка. – 2018. – №1. – С. 6–16.

[8]. Цивільний кодекс України [Електронний ресурс] // Liga 360. – 2003. – Режим доступу до ресурсу: https://ips.ligazakon.net/document/T030435?an=843030.

[9]. Закону України «Про захист персональних даних» [Електронний ресурс] // Верховна Рада України. Законодавство України. – 2010. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[10]. Захист персональних даних в інтернеті. Що робити людині, якщо фотографії з її зображенням потрапили в «мережу»? [Електронний ресурс] // Правова допомога: [Веб сайт]. – 2021. – Режим доступу до ресурсу: https://pravdop.com/ua/publications/kommentarii-zakonodatelstva/zashita-personalnih-dannih-v-internete-chto-delat-cheloveku-esli-fotografii-s-ego-izobrazheniem-popali-v-set-a-on-zhelaet-chtobi-ih-tam-ne-bilo/.

[11]. Мельник К. С. Обробка та захист персональних даних в соціальних мережах / К. С. Мельник. // Інформація і право. – 2014. – №3. – С. 64–69.

[12]. Як захистити свої дані в інтернеті [Електронний ресурс] // Міністерство та Комітет цифрової трансформації України. Офіційний веб-сайт. – 2020. – Режим доступу до ресурсу: https://thedigital.gov.ua/news/yak-zakhistiti-svoi-dani-v-interneti.

[13]. Соціальна інженерія Низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. [Електронний ресурс] // ESET, spol. s r.o.. – 2021. – Режим доступу до ресурсу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/.

[14]. Хэднеги К. Искусство обмана. Социальная инженерия в мошеннических схемах / Кристофер Хэднеги; пер. с англ. – Київ: Альпина Паблишер, 2020. – 430 с.
[15]. Защита вашего сайта с беспрецедентными метриками и отчетами [Електронний ресурс] // 2WAF ISS. – 2021. – Режим доступу до ресурсу: https://2waf.com/.
[16]. Сєдова І. Хакінг мізків, або Як урятуватися від віртуальних шахраїв [Електронний ресурс] / Ірина Сєдова // ZMINA. – 2020. – Режим доступу до ресурсу: https://zmina.info/articles/haking-mizkiv-abo-yak-vryatuvatysya-vid-virtualnyh-shahrayiv/.
[17]. Начало работы с Google Аналитикой [Електронний ресурс] // Google LLC. – 2020. – Режим доступу до ресурсу: https://support.google.com/analytics/answer/1008015?hl=ru.
[18]. Семернін Д. О. Протидія методам та засобам соціальної інженерії : 125 «Кібербезпека» / Семернін Д. О. – Харків, 2020. – 78 с.

References

[1]. Zakhist personalnikh danikh: vikoristannya, zakhist ta vidpovidalnist [Yelektronniy resurs] // Koordinatsiyniy tsentr z nadannya pravovoyi dopomogi: [Veb-sayt]. – 2021. – Rezhim dostupu do resursu: https://www.legalaid.gov.ua/publikatsiyi/zahyst-personalnyh-danyh-vykorystannya-zahyst-ta-vidpovidalnist/.
[2]. Tsifrovizatsiya yak nova realnist Ukrayini [Yelektronniy resurs] // LexInform: [Veb-sayt]. – 2020. – Rezhim dostupu do resursu: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/.
[3]. Ne vir nikomu. Shcho take sotsialna inzheneriya ta yak ne stati yii zhertvoyu [Yelektronniy resurs] // KiberbezpekaOnlayn:[Veb-sayt]. – 2021. – Rezhim dostupu do resursu: https://kyivstar.ua/uk/cybersecurity/ne-vir-nikomu-shcho-take-socialna-inzheneriya-ta-yak-ne-staty-yiyi-zhertvoyu.
[4]. Pilipchuk V. G. Transformatsiya sistemi zakhistu personalnikh danikh ta privatnosti v konteksti yevrointegratsii Ukrayini / V. G. Pilipchuk, V. V. Brizhko. // Visnik Natsionalnoyi akademii pravovikh nauk Ukrayini. – 2017. – №3. – S. 36–50.
[5]. Gron O. V. Problemi zakhistu personalnikh danikh u konteksti suchasnoyi komunikatsii / O. V. Gron, A. K. Pogorelenko. // Naukoviy visnik Uzhgorodskogo natsionalnogo universitetu. – 2018. – №19. – S. 102–108.
[6]. Shapenko L.O. Zakhist personalnikh danikh: teoretiko-pravoviy aspekt / L.O. Shapenko, Ya.A. Semenyuk // Yurisprudentsiya v suchasnomu informatsiynomu prostori: materiali IKh Mizhnar. nauk.-prakt. konf., (Kiyiv, 1 bereznya 2019 r.). – Ternopil: Vektor, 2019. – S. 124-126.
[7]. Sokolov V. Yu. Metodika protidii sotsialnomu inzhiniringu na ob'yektakh informatsiynoyi diyalnosti / V. Yu. Sokolov, D. M. Kurbanmuradov. // Kiberbezpeka: osvita, nauka, tekhnika. – 2018. – №1. – S. 6–16.
[8]. Tsivilniy kodeks Ukrayini [Yelektronniy resurs] // Liga 360. – 2003. – Rezhim dostupu do resursu: https://ips.ligazakon.net/document/T030435?an=843030.
[9]. Zakonu Ukrayini «Pro zakhist personalnikh danikh» [Yelektronniy resurs] // Verkhovna Rada Ukrayini. Zakonodavstvo Ukrayini. – 2010. – Rezhim dostupu do resursu: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[10]. Zakhist personalnikh danikh v interneti. Shcho robiti lyudini, yakshcho fotografii z yii zobrazhennyam potrapili v «merezhu»? [Yelektronniy resurs] // Pravova dopomoga: [Veb sayt]. – 2021. – Rezhim dostupu do resursu: https://pravdop.com/ua/publications/kommentarii-zakonodatelstva/zashita-personalnih-dannih-v-internete-chto-delat-cheloveku-esli-fotografii-s-ego-izobrazheniem-popali-v-set-a-on-zhelaet-chtobi-ih-tam-ne-bilo/.
[11]. Melnik K. S. Obrobka ta zakhist personalnikh danikh v sotsialnikh merezhakh / K. S. Melnik. // Informatsiya i pravo. – 2014. – №3. – S. 64–69.
[12]. Yak zakhistiti svoyi dani v interneti [Yelektronniy resurs] // Ministerstvo ta Komitet tsifrovoyi transformatsii Ukrayini. Ofitsiyniy veb-sayt. – 2020. – Rezhim dostupu do resursu: https://thedigital.gov.ua/news/yak-zakhistiti-svoi-dani-v-interneti.
[13]. Sotsialna inzheneriya Nizka ne tekhnichnikh priyomiv manipulyuvannya koristuvachami, yaki vikoristovuyutsya kiberzlochintsyami pid chas atak. [Yelektronniy resurs] // ESET, spol. s r.o.. – 2021. – Rezhim dostupu do resursu: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/.
[14]. Khednegi K. Iskusstvo obmana. Sotsialnaya inzheneriya v moshennicheskikh skhemakh / Kristofer Khednegi; per. s angl. – Kiyiv: Alpina Pablisher, 2020. – 430 s.
[15]. Zashchita vashego sayta s bespretsedentnymi metrikami i otchetami [Yelektronniy resurs] // 2WAF ISS. – 2021. – Rezhim dostupu do resursu: https://2waf.com/.
[16]. Syedova I. Khaking mizkiv, abo Yak uryatuvatisya vid virtualnikh shakhrayiv [Yelektronniy resurs] / Irina Syedova // ZMINA. – 2020. – Rezhim dostupu do resursu: https://zmina.info/articles/haking-mizkiv-abo-yak-vryatuvatysya-vid-virtualnyh-shahrayiv/.
[17]. Nachalo raboty s Google Analitikoy [Yelektronniy resurs] // Google LLC. – 2020. – Rezhim dostupu do resursu: https://support.google.com/analytics/answer/1008015?hl=ru.
[18]. Semernin D. O. Protidiya metodam ta zasobam sotsialnoyi inzhenerii : 125 «Kiberbezpeka» / Semernin D. O. – Kharkiv, 2020. – 78 s.

Отримана в редакції 02.09.2022. Прийнята до друку 14.09.2022. Received 02 September 2022. Approved 14 September 2022. Available in Internet 30 September 2022.