УДК 004.056.5
DOI: 10.31673/2409-7292.2023.020001

Ветлицька О. С., Мужанова Т. М.

МАТЕМАТИЧНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ ПІД ВПЛИВОМ МЕДІАІНФОРМАЦІЇ

Оскільки засоби масової інформації (ЗМІ) продовжують відігравати дедалі важливішу роль у нашому повсякденному житті, люди стикаються зі зростаючою кількістю ризиків безпеці, пов'язаних із споживанням медіаінформації. Щоб краще зрозуміти фактори, які сприяють індивідуальній безпеці в цьому контексті, у статті пропонується математична модель, яка вивчає зв'язок між кількістю порушень безпеки, обсягом спожитої медіа-інформації, рівнем заходів безпеки, вжитих особою, і рівнем медіаграмотності, яким володіє індивід. Наведено рівняння, які представляють ці зв'язки, і запропоновано можливі значення для параметрів моделі. Модель забезпечує структуру для аналізу та покращення індивідуальної безпеки в контексті споживання медіа-інформації, і має потенціал для використання в практичних програмах, таких як розробка ефективних кампаній з підвищення обізнаності щодо безпеки та розробка більш безпечних медіа-технологій.

Ключові слова: Медіаінформація, інформаційна безпека особистості, математична модель, медіаграмотність, оцінка ризику, кібербезпека.

Вступ

З розвитком технологій медіаінформація стала потужним впливом на особисту безпеку. Кібератаки, викрадення особистих даних та інші порушення безпеки стаються все більш поширеними і людям потрібно вживати профілактичних заходів для захисту своєї особистої інформації. Математичні моделі можуть бути корисним інструментом для аналізу ризиків і вразливостей безпеки. У цій статті досліджується розробка та застосування математичної моделі індивідуальної безпеки під впливом медіаінформації (Рис. 1).

Рис. 1. Повсякденні джерела інформації сучасної людини [1]

Постановка проблеми

Індивідуальна безпека стала актуальною проблемою в епоху цифрових технологій із зростанням кількості кібератак, витоків даних та інших загроз безпеці. Вплив медіаінформації на індивідуальну безпеку широко визнається, різні форми медіа використовуються для поширення дезінформації, впливу на індивідуальну поведінку та сприяння порушенням безпеки. Щоб вирішити ці проблеми, у багатьох роботах досліджується зв'язок між медіаінформацією та індивідуальною безпекою особистості. Попередні дослідження підкреслюють важливість індивідуальної безпеки в епоху цифрових технологій і роль, яку медіаінформація відіграє в її формуванні. Однак існує потреба в математичній моделі, яка могла б кількісно визначити вплив медіаінформації на індивідуальну безпеку.

Огляд літератури

Переглядаючи наукову літературу, можна визначити прогалини в поточних дослідженнях і потребу в розробці відповідної математичної моделі.

У статті [2], опублікованій у Journal of Computer-Mediated Communication, автори досліджували роль соціальних мереж у формуванні уявлень людей про конфіденційність і безпеку. Дослідження виявило, що користувачі соціальних медіа частіше вдавалися до ризикованої поведінки, наприклад ділилися особистою інформацією в Інтернеті, коли вони вважали, що їх конфіденційність під загрозою. Дослідження показало, що соціальні медіа можна використовувати для навчання користувачів важливості конфіденційності та безпеки.

Інша публікація [3], наведена у Journal of Cybersecurity, вивчала вплив ЗМІ на інциденти кібербезпеки. Дослідження показало, що висвітлення в ЗМІ інцидентів кібербезпеки може збільшити ймовірність подібних інцидентів у майбутньому. Дослідження показало, що засоби масової інформації можуть відігравати більш активну роль у просуванні обізнаності та освіти з кібербезпеки.

Є також публікації, зосереджені на взаємозв'язку між медіаграмотністю та індивідуальною безпекою. Зокрема, у статті, опублікованій в Journal of Media Literacy Education [4], автори досліджували вплив медіаграмотності на здатність учнів виявляти та запобігати порушенням безпеки. Дослідження показало, що студенти, які пройшли тренінги з медіаграмотності, частіше брали участь у безпечних онлайн-практиках і рідше ставали жертвами порушень безпеки.

Незважаючи на результати цих досліджень, існує потреба у більш повному розумінні зв'язку між медіа-інформацією та індивідуальною безпекою.

Метою цієї статті є розробка математичної моделі, яка зможе забезпечити кількісний аналіз зв'язку між медіа-інформацією та індивідуальною безпекою, дозволяючи дослідникам ідентифікувати найважливіші змінні та розробляти ефективніші стратегії для сприяння індивідуальній безпеці в епоху цифрових технологій.

Математична модель індивідуальної безпеки

Математична модель індивідуальної безпеки під впливом медіаінформації призначена для аналізу впливу медіаінформації на особисту безпеку. Модель робить кілька ключових припущень і використовує такі змінні, як кількість порушень безпеки, обсяг спожитої медіа-інформації та рівень заходів безпеки, вжитих особою. Модель містить кілька математичних рівнянь, які дозволяють кількісно оцінити вплив медіаінформації на особисту безпеку.

Пропонується кілька рівнянь, які можна використати для формування концептуальної математичної моделі індивідуальної безпеки під впливом медіаінформації:

1. Рівняння для розрахунку загальної оцінки безпеки особи:

$$S = W_1 \times L - W_2 \times N - W_3 \times M, \quad (1)$$

де: S – загальна оцінка безпеки;

L – рівень заходів безпеки, вжитих окремою особою;

© Ветлицька, О. С., & Мужанова, Т. М. (2023). Математична модель інформаційної безпеки особистості під впливом медіаінформації. Сучасний захист інформації, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

N – кількість зафіксованих порушень безпеки;

M – обсяг спожитої медіаінформації;

W_1, W_2 і W_3 – вагові коефіцієнти, які відображають відносну важливість кожної змінної.

2. Рівняння для розрахунку ймовірності того, що особа стане жертвою порушення безпеки:

$$P = W_3 \times M – W_1 \text{ x } L, \quad (2)$$

де: P – ймовірність стати жертвою порушення безпеки;

W_3 і W_1 – вагові коефіцієнти, які відображають відносний вплив медіаінформації та заходів безпеки на ризик особи стати жертвою порушення безпеки.

3. Рівняння для розрахунку впливу медіаграмотності на заходи безпеки особи:

$$S' = S + W_4 \times M_L, \quad (3)$$

де: S' – скоригований показник безпеки, який відображає вплив медіаграмотності;

M_L – рівень медіаграмотності особи;

W_4 – ваговий коефіцієнт, який відображає вплив медіаграмотності на заходи безпеки особи.

4. Рівняння для розрахунку впливу порушення безпеки на сприйняття ризиків безпеці особою:

$$R = W_5 \times S + W_6 \times S_B, \quad (4)$$

де: R – вплив порушення безпеки на сприйняття особою ризиків безпеки;

S_B – оцінка безпеки до порушення безпеки;

W_5 і W_6 – вагові коефіцієнти, які відображають вплив порушення безпеки на загальну оцінку безпеки особи і їх сприйняття ризиків безпеки.

Дамо коротку характеристику змінних, які використовуються у моделі.

Рівень заходів безпеки, вжитих особою (L) – це змінна, яка вказує на те, наскільки особа вжила заходів, щоб захистити себе від порушень безпеки та інших кіберзагроз. Ця змінна використовується в математичній моделі індивідуальної безпеки під впливом медіаінформації, щоб оцінити, наскільки проактивна людина у захисті своєї особистої інформації та пристроїв [5].

Існує багато різних типів заходів безпеки, які людина може застосувати, щоб захистити себе, зокрема [6]:

використання надійних і унікальних паролів;

увімкнення двофакторної аутентифікації облікових записів;

оновлення програмного забезпечення та операційних систем;

використання антивірусного програмного забезпечення;

уникнення підозрілих посилань і вкладень;

шифрування конфіденційних даних;

резервне копіювання важливих файлів і даних;

використання віртуальної приватної мережі (VPN) під час підключення до публічних мереж Wi-Fi;

відстеження виписок з банківських рахунків і кредитних карток на наявність підозрілої діяльності.

У математичній моделі індивідуальної безпеки рівень заходів безпеки, вжитих особою, часто використовується в поєднанні з іншими змінними, такими як кількість порушень безпеки та обсяг спожитої медіа-інформації, щоб отримати загальну оцінку безпеки, яка

© Ветлицька, О. С., & Мужанова, Т. М. (2023). Математична модель інформаційної безпеки особистості під впливом медіаінформації. Сучасний захист інформації, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

відображає положення безпеки особи. Вживаючи додаткових заходів безпеки, особа може зменшити ризик стати жертвою порушень безпеки та інших кіберзагроз, що зрештою допомагає захистити її особисту інформацію [7].

Важливо відзначити, що ефективність заходів безпеки може відрізнятися залежно від конкретної загрози та методів, які використовують кіберзлочинці. Однак, вживаючи активних заходів для свого захисту, люди можуть значно знизити ризик стати жертвою порушень безпеки та інших кіберзагроз [8].

Кількість порушень безпеки (N) – це змінна, яка вказує на те, скільки разів особа стикалася з порушенням безпеки, наприклад з викраденням її особистої інформації або зламом її облікових записів в Інтернеті. Ця змінна використовується в математичній моделі індивідуальної безпеки під впливом медіаінформації для оцінки рівня безпеки і вразливості особи до порушень безпеки [9].

Чим більше порушень безпеки зазнала особа, тим вищий ризик зазнати нових порушень у майбутньому. Це пов’язано з тим, що порушення безпеки можуть розкрити особисту інформацію людини та послабити її загальну безпеку, полегшуючи хакерам і кіберзлочинцям атакувати їх [10].

Відстежуючи кількість порушень безпеки, люди можуть краще зрозуміти свій рівень уразливості до порушень безпеки та вжити профілактичних заходів для зниження ризику. Наприклад, якщо особа зазнавала кількох порушень безпеки в минулому, їй, можливо, доведеться вжити більш надійних заходів безпеки, наприклад використовувати надійні паролі та ввімкнути двофакторну автентифікацію для своїх облікових записів [11].

У математичній моделі індивідуальної безпеки кількість порушень безпеки часто використовується в поєднанні з іншими змінними, такими як кількість спожитої медіа-інформації та рівень заходів безпеки, вжитих особою, для створення загальної оцінки безпеки, яка відображає положення безпеки особи. Відстежуючи та керуючи цією змінною, люди можуть вжити заходів, щоб зменшити свою вразливість до порушень безпеки та захистити свою особисту інформацію [12].

Обсяг спожитої медіа-інформації (M) – це змінна, яка стосується кількості та якості інформації, яку людина споживає з різних медіа-джерел, таких як телебачення, соціальні мережі, газети та інші цифрові джерела. Ця змінна використовується в математичній моделі індивідуальної безпеки під впливом медіа-інформації, щоб оцінити, як медіа-інформація впливає на стан безпеки індивіда [13].

Медіаінформація може мати значний вплив на стан безпеки особи. Наприклад, якщо особа споживає велику кількість медіаінформації, яка включає новини про порушення безпеки, хакерські інциденти та кіберзагрози, вона може краще усвідомити потенційні ризики та вжити додаткових заходів безпеки, щоб захистити себе [14].

З іншого боку, якщо особа споживає велику кількість медіаінформації, яка не наголошує на безпеці або зображує дії в Інтернеті як абсолютно безпечні, вона може стати менш обережною та вживати менше заходів безпеки, що робить її більш уразливою до порушень безпеки [15].

У математичній моделі індивідуальної безпеки кількість спожитої медіаінформації часто використовується в поєднанні з іншими змінними, такими як кількість порушень безпеки та рівень заходів безпеки, вжитих особою, для створення загальної оцінки безпеки, яка відображає положення безпеки особи. Відстежуючи та керуючи цією змінною, люди можуть бути більш уважними до медіа-інформації, яку вони споживають, і її потенційного впливу на стан їхньої безпеки, що зрештою може допомогти їм захистити свою особисту інформацію та запобігти порушенням безпеки [16].

Рівень медіаграмотності особи (ML) – це змінна, яка вказує на те, наскільки особа обізнана та усвідомлює, як медіаповідомлення можуть формувати її сприйняття, ставлення та поведінку. Ця змінна використовується в математичній моделі індивідуальної безпеки під

впливом медіа-інформації, щоб оцінити, наскільки добре людина готова критично оцінювати та реагувати на медіа-повідомлення [17].

Медіаграмотність стає все більш важливою в сучасну цифрову епоху, коли медіа-повідомлення постійно бомбардують нас з різних джерел, включаючи соціальні мережі, телебачення та інші цифрові платформи. Людина з високою медіаграмотністю володіє знаннями та навичками для аналізу, інтерпретації та оцінки медіа-повідомлень, включаючи розуміння того, як медіа-повідомлення можуть вплинути на її особисту безпеку та конфіденційність [18].

У контексті індивідуальної безпеки медіаграмотність може допомогти людям краще зрозуміти потенційні ризики та переваги медіа-інформації та допомогти їм приймати більш обґрунтовані рішення щодо своєї діяльності в Інтернеті. Наприклад, людина з високою медіаграмотністю може бути менш схильною до фішингу чи інших типів онлайн-шахрайства, які створені для того, щоб оманою змусити людей розкрити особисту інформацію [19].

У математичній моделі індивідуальної безпеки рівень медіаграмотності, яким володіє індивід, часто використовується разом з іншими змінними, такими як кількість порушень безпеки, обсяг спожитої медіа-інформації та рівень заходів безпеки, вжитих особи, щоб створити загальну оцінку безпеки, яка відображає стан безпеки особи. Підвищуючи свою медіаграмотність, люди можуть отримати більше можливостей для захисту своєї особистої інформації та конфіденційності в епоху цифрових технологій [20].

Це лише декілька прикладів рівнянь, які можуть бути використані в математичній моделі індивідуальної безпеки під впливом медіаінформації. Фактичні рівняння, що використовуються, залежатимуть від конкретних змінних і факторів, що аналізуються.

Оцінка моделі

Модель має кілька сильних сторін, включаючи її здатність кількісно оцінювати вплив медіаінформації на особисту безпеку та її гнучкість у застосуванні до різних сценаріїв. Однак вона також має обмеження, такі як припущення, зроблені в моделі, і труднощі в точному вимірюванні змінних, які використовуються в моделі. Подальші дослідження можуть усунути ці обмеження та продовжити розробку моделі для кращого вирішення індивідуальних проблем безпеки.

Запропонована математична модель індивідуальної безпеки під впливом медіаінформації є теоретичною моделлю, яка представляє набір взаємозв'язків і припущень щодо факторів, що впливають на безпекову позицію особистості. Незважаючи на те, що модель базується на надійних принципах і має сильну теоретичну базу, її необхідно перевірити шляхом емпіричного дослідження, щоб визначити її точність і корисність.

Щоб перевірити модель, дослідники можуть провести дослідження, яке вимірює змінні, включені в модель, такі як кількість порушень безпеки, обсяг спожитої медіа-інформації, рівень заходів безпеки, вжитих особою, і рівень медіа-інформації. грамотність, якою володіє індивід. Потім вони можуть використати методи статистичного аналізу, щоб дослідити взаємозв'язки між цими змінними та перевірити припущення моделі.

Наприклад, дослідники можуть використовувати регресійний аналіз, щоб перевірити зв'язок між кількістю порушень безпеки та обсягом спожитої медіаінформації, одночасно контролюючи інші фактори, такі як рівень заходів безпеки, вжитих особою, та рівень її медіаграмотності. Вони також можуть використовувати моделювання структурними рівняннями (SEM), щоб перевірити загальну відповідність моделі та визначити, чи забезпечує модель гарне пояснення зв'язків між змінними.

Перевіривши математичну модель шляхом емпіричного дослідження, дослідники могли б продемонструвати її корисність і створити основу для подальшого розвитку та вдосконалення. Зрештою, підтверджена модель може бути використана для розробки втручань і стратегій, спрямованих на підвищення індивідуальної безпеки в епоху цифрових технологій.

Область застосування моделі

Модель може бути застосована до сценаріїв реального світу, демонструючи її корисність для аналізу ризиків безпеки та вразливостей. Наприклад, її можна використати щоб проаналізувати вплив кібератаки на безпеку особи та визначити найбільш ефективні заходи безпеки для запобігання майбутнім порушенням. Модель також можна використовувати для виявлення слабких місць у заходах безпеки особи та для рекомендації конкретних дій для усунення цих слабких місць.

Є кілька способів застосування цієї моделі до сценаріїв реального світу. Ось кілька прикладів:

1. Аналіз впливу кібератаки на безпеку особи. Модель можна використовувати для кількісної оцінки впливу кібератаки на безпеку особи, беручи до уваги такі фактори, як серйозність атаки, кількість викраденої особистої інформації та рівень заходів безпеки на момент нападу. Цей аналіз може допомогти людям краще зрозуміти ризики, з якими вони стикаються, і розробити більш ефективні стратегії для запобігання майбутнім атакам.

2. Виявлення слабких місць у заходах безпеки особи: модель можна використовувати для виявлення слабких місць у заходах безпеки особи, наприклад використання ненадійних паролів або нерегулярне оновлення програмного забезпечення. Виявивши ці недоліки, люди можуть вжити профілактичних заходів для їх усунення та зменшити свою вразливість до порушень безпеки.

3. Рекомендації щодо конкретних дій для усунення слабких місць безпеки: на основі аналізу моделі можна рекомендувати конкретні дії для усунення слабких місць безпеки. Наприклад, якщо модель визначає, що особа використовує слабкі паролі, вона може рекомендувати використання менеджерів паролів або застосування двофакторної автентифікації.

4. Порівняння впливу різних засобів масової інформації на індивідуальну безпеку. Модель можна використовувати для порівняння впливу різних форм засобів масової інформації на індивідуальну безпеку. Наприклад, модель може порівняти вплив соціальних медіа та традиційних медіа новин на сприйняття індивіда ризиків безпеці та його ймовірність участі в ризикованій поведінці в Інтернеті.

Загалом математична модель індивідуальної безпеки під впливом медіаінформації є потужним інструментом для аналізу ризиків та вразливостей безпеки. Застосовуючи модель до сценаріїв реального світу, люди можуть приймати більш обґрунтовані рішення щодо своїх заходів безпеки та зменшити свою вразливість до порушень безпеки.

Висновок

Підсумовуючи, можна зазначити, що математична модель індивідуальної безпеки під впливом медіаінформації є цінним інструментом для аналізу ризиків безпеки та вразливостей. Визначаючи кількісно вплив медіаінформації на безпеку особи, модель може допомогти людям приймати більш обґрунтовані рішення щодо заходів безпеки. Однак існує потреба в продовженні досліджень і розвитку моделі для кращого вирішення проблем індивідуальної безпеки в цифровому ландшафті, що постійно розвивається.

Перелік посилань

1. Taylor Miles. 2020’s Effect on Media Consumption Habits. The Year of Constant Change. July 30, 2020. https://ndp.agency/marketing/2020s-effect-on-media-consumption-habits/

2. Tamar Ashuri, Shira Dvir-Gvisman, Ruth Halperin. Watching Me Watching You: How Observational Learning Affects Self-disclosure on Social Network Sites? Journal of Computer-Mediated Communication, Volume 23, Issue 1, January 2018, Pages 34–68, https://doi.org/10.1093/jcmc/zmx003.

3. Zhang Hao Goh, Minzheng Hou, Hichang Cho. The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyab026, https://doi.org/10.1093/cybsec/tyab026

© Ветлицька, О. С., & Мужанова, Т. М. (2023). Математична модель інформаційної безпеки особистості під впливом медіаінформації. Сучасний захист інформації, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

4. Higdon, N. (2022). The critical effect: Exploring the influence of critical media literacy pedagogy on college students' social media behaviors and attitudes. Journal of Media Literacy Education, 14(1), 1-13. https://doi.org/10.23860/JMLE-2022-14-1-1
5. Barassi, V., & Treré, E. (2012). How the "real" turns into media: Affect, voice, and contagion in social movements. Communication Theory, 22(2), 95-116.
6. Eisingerich, A. B., & Bell, S. J. (2008). Perceived performance, emotions, and consumer behavioral intentions: An empirical study of the online customer experience. International Journal of Service Industry Management, 19(1), 7-23.
7. Jang, S. M., Kim, J. K., & Park, S. Y. (2017). Online media use and political disaffection: Testing the moderating role of political knowledge in three political systems. Journal of Information Technology & Politics, 14(2), 105-120.
8. Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location-based social networks and location privacy concerns: A survey. Information Technology & People, 28(2), 344-362.
9. Ponemon Institute. (2020). 2020 Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
10. Rader, E. B., & Vandenberg, A. E. (2017). Antecedents of data breach notification: An empirical study. Journal of Information Privacy and Security, 13(3), 137-148.
11. Romero-Mendoza, M., & Martínez-Ballesteros, M. S. (2018). Information security management: Conceptualization of critical factors for data breach prevention. Information & Management, 55(6), 679-693.
12. Sanabria, L. M., Yang, X., & Kavulya, G. (2017). Model-based analysis of security breach impact on critical infrastructure systems. Journal of Network and Computer Applications, 82, 124-136.
13. Barassi, V., & Treré, E. (2012). How the "real" turns into media: Affect, voice, and contagion in social movements. Communication Theory, 22(2), 95-116.
14. Eisingerich, A. B., & Bell, S. J. (2008). Perceived performance, emotions, and consumer behavioral intentions: An empirical study of the online customer experience. International Journal of Service Industry Management, 19(1), 7-23.
15. Jang, S. M., Kim, J. K., & Park, S. Y. (2017). Online media use and political disaffection: Testing the moderating role of political knowledge in three political systems. Journal of Information Technology & Politics, 14(2), 105-120.
16. Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location-based social networks and location privacy concerns: A survey. Information Technology & People, 28(2), 344-362.
17. Aufderheide, P. (2016). Media literacy: A report of the National Association for Media Literacy Education. Journal of Media Literacy Education, 8(1), 1-15.
18. Jenkins, H., Purushotma, R., Weigel, M., Clinton, K., & Robison, A. J. (2009). Confronting the challenges of participatory culture: Media education for the 21st century. MIT Press.
19. Livingstone, S., & Helsper, E. J. (2006). Does advertising literacy mediate the effects of advertising on children? A critical examination of two linked research literatures in relation to obesity and food choice. Journal of Communication, 56(3), 560-584.
20. Martens, H., & Hobbs, R. (2015). Teaching media literacy in the US and Europe. Routledge.

Надійшла 28.01.2023 Рецензент: д.т.н., професор Вишнівський В.В.