ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2023-76-6
УДК 004.056:621.397.3:004.942

МАЙОР Євген
Хмельницький національний університет
https://orcid.org/0009-0004-1867-6241
e-mail: gorix2019@gmail.com
ДЖУЛІЙ Володимир
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
ЧЕШУН Віктор
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua

АЛГОРИТМИ ПРОГНОЗУВАННЯ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕМАТИЧНИХ ІНТЕРНЕТ-РЕСУРСІВ

Розглянуті особливості функціонування форумів тематичних інтернет-ресурсів дозволяють здійснювати прогнозування виникнення вразливостей та загроз безпеки конфіденційних даних. Для вирішення даної задачі передбачається проведення аналізу інтернет-повідомлень, створюваних учасниками форумів тематичних інтернет-ресурсів, відповідно до представлених алгоритмів. Алгоритм прогнозування вразливостей та загроз безпеки інформації відрізняється можливістю виявлення вразливостей та загроз на ранніх етапах їх практичної реалізації, ґрунтується на проведенні аналізу потоку повідомлень форумів тематичних інтернет-ресурсів, що дозволяє спеціалістам з інформаційної безпеки приймати адекватні та своєчасні заходи щодо захисту конфіденційних даних.

Алгоритм фільтрації потоку повідомлень та статистичного аналізу передбачає фільтрацію тематичних повідомлень, що не відносяться до заданої предметної області, яка задана відповідною онтологією. Запропоновані алгоритми дозволяють прогнозувати вразливості та загрози, вживати адекватних заходів щодо захисту інформації.

Ключові слова: інформаційна безпека, алгоритм прогнозування вразливостей, алгоритм фільтрації повідомлень , тематичні інтернет-ресурси.

MAIOR Yevhen, DZHULIY Volodymyr, CHESHUN Viktor, PETLIAK Nataliia
Khmelnytskyi National University

ALGORITHMS FOR PREDICTING INFORMATION SECURITY VULNERABILITIES AND THREATS BASED ON THEMATIC INTERNET RESOURCES

The considered features of the functioning of forums of thematic Internet resources allow to forecast the occurrence of vulnerabilities and threats to the security of confidential data. To solve this problem, the analysis of Internet messages created by participants of forums of thematic Internet resources is expected, according to the presented algorithms.

The algorithm for predicting vulnerabilities and threats to information security is distinguished by the possibility of detecting vulnerabilities and threats at the early stages of their practical implementation, is based on the analysis of the flow of messages of forums of thematic Internet resources, which allows information security specialists to take adequate and timely measures to protect confidential data. The result of the algorithm's work is reports on identified vulnerabilities and threats to the information security of confidential data. The reports may also include information reflecting the results of text message analysis, based on which a conclusion about the occurrence of vulnerabilities and threats was obtained.

The message flow filtering and statistical analysis algorithm involves filtering thematic messages that do not belong to the given subject area, which is specified by the corresponding ontology. The result of the algorithm is the determination of statistical indicators characterizing the flow of thematic messages during the period of data flow analysis. The algorithm also calculates the number of text messages that have passed the data flow filtering stage and determines the average rating of text message authors. The results of the algorithm can be used to build a system of logical fuzzy inference for forecasting the events of the subject area for which the analysis is conducted.

The proposed algorithms allow predicting vulnerabilities and threats, taking adequate measures to protect information. The obtained results testify to the effectiveness of the proposed algorithms for forecasting vulnerabilities and threats, and also confirm the correctness of the information and analytical system.

Keywords: information security, vulnerability prediction algorithm, message filtering algorithm, thematic Internet resources.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Актуальними та пріоритетними на сучасному етапі є задачі аналізу і класифікації існуючих механізмів реалізації атак та загроз інформаційної безпеки, які можуть призвести до отримання несанкціонованого доступу до конфіденційної інформації та порушення функціонування інформаційних систем. Постає задача визначення заходів протидії атакам та загрозам, усунення вразливостей, оцінки можливості задання шкоди, підготовки нормативно-правової бази, механізмів захисту та критеріїв безпеки.

Проблеми інформаційної безпеки розвитку суспільства у більшості сфер діяльності виходять на перший план. Це пов'язано зі значним зростанням кількості реалізованих проектів інформатизації, більшість з яких спрямовано на побудову єдиного телекомунікаційного та інформаційного простору з метою оптимізації процесів обробки різноманітної інформації великих об'ємів, наприклад, для забезпечення оперативного доступу до інформації, надійного зберігання даних для користувачів інформаційного обміну

Важливість даних проблем пов'язана з наступними основними факторами [1-3]: зростанням різноманітності та кількості засобів комп'ютерної техніки та сфер людської діяльності їх застосування; високим рівнем довіри до інформаційно-пошукових систем обробки та управління даними; зростанням числа користувачів інформаційного простору взаємодії; накопиченням великих об'ємів різнотипної інформації; інтенсивним обміном потоком даних в мережі між користувачами; використання широкого спектра механізмів доступу до конфіденційних ресурсів, інформаційних процесів; промисловим шпигунством та конкурентною боротьбою у сфері інформаційних послуг суспільства; недостатньою кількістю фахівців високої кваліфікації в сфері інформаційної безпеки; ринковими відношеннями в галузі розробки програмного забезпечення, обслуговування, розповсюдження, виробництва обчислювальної комп'ютерної техніки для реалізації інформаційної безпеки; різноманіттям атак, загроз і різнотипних каналів отримання несанкціонованого доступу до конфіденційних ресурсів та диференціацією негативних наслідків.

Більшість існуючих моделей безпеки інформації, на сучасному етапі, ґрунтуються на забезпеченні конфіденційності, доступності, цілісності задіяної інформації [9]. Вразливості мережевих інформаційних систем, як правило, є наслідком внесених в систему помилок. Помилки, що є причиною формування вразливостей, в свою чергу, поділяються на помилки реалізації та помилки адміністрування [2,6].

Постановка задачі

На сьогодні не існує єдиного підходу до вирішення проблеми захищенності інформаційно-пошукових систем стосовно предметних областей [1,2]: забезпечення надійного захисту інформаційних ресурсів потребує реалізації технічних та організаційних заходів в комплексі, що супроводжуються розробкою відповідної документації, а розробниками програмно-апаратних засобів захисту інформації пропонуються відповідні компоненти на вирішення конкретних задач.

Таким чином, є необхідність вирішення наступних задач для забезпечення інформаційної безпеки [4,7,8]: формування основ для опису процесів реалізації та виникнення атак, загроз, вразливостей інформаційної безпеки системи в умовах невизначеності та непередбачуваності їх прояву; розробка відповідних засобів забезпечення захисту конфіденційної інформації на основі проведеного дослідження та класифікації вразливостей і загроз; визначення загальних підходів до створення інформаційних систем забезпечення захисту конфіденційних даних, механізмів управління захистом на різних рівнях діяльності суспільства.

Більшість сучасних програмно-апаратних систем виявлення комп'ютерних загроз та атак працюють із використанням підходів сигнатурного аналізу та фіксації інтернет-мережевих аномалій. Дані підходи мають недоліки, пов'язані із використанням потужних обчислювальних ресурсів на їх реалізацію, а також мають низьку ефективність при виявленні нових комп'ютерних загроз [8].

Основними джерелами надходження знань про вразливості та атаки інформаційної безпеки є бази даних та знань, створювані державними та комерційними структурами. Наповнення інформаційних баз даних здійснюється із залученням дослідних авторитетних центрів експертним шляхом. Разом з тим, інформація, що міститься в базах даних та знань вразливостей та загроз не є повною. Актуальною залишається задача виявлення доступних інформаційних ресурсів про комп'ютерні загрози, віруси, вразливості, а також можливість доступу до результатів досліджень компаній з виявлення загроз інформаційної безпеки. Одним із джерел надходження інформації про вразливості та загрози інформаційної безпеки є інтернет-ресурси (інформаційні соціальні ресурси, анонімні тощо, які відносяться до сфкри інформаційної безпеки), що обумовлено популярністю спеціалізованих інтернет-ресурсів у зацікавлених відповідними предметними областями. Події, що відбуваються в відповідних предметних областях, є предметом для обговорення учасників дискусійних тематичних інтернет-майданчиків. Даний фактор дозволяє прогнозувати виявлення вразливостей, атак, загроз безпеки інформації, ґрунтуючись на проведенні аналізу потоку повідомлень тематичних інтернет-ресурсів. Як один із підходів вирішення задачі розглянуто можливість використання інформаційних систем нечіткого логічного виводу, вхідними даними яких є результати проведеного аналізу інформації тематичних інтернет-ресурсів. Фахівець безпеки інформації

зможе оцінити ступінь інформаційної небезпеки ресурсів на основі отриманих результатів прогнозування виникнення вразливості, атаки, загрози, оцінити коректність моделі загроз безпеці інформації та задіяти протидію щодо нейтралізації вразливостей.

В результаті аналізу виявлено невирішенні питаня стосовно автоматизації інформаційних процесів прогнозування вразливостей та загроз безпеки інформації. Актуальною постає задача проектування та розробки методу і системи прогнозування, виявлення вразливостей, загроз безпеки інформації.

Вирішення поставлених задач спрямоване на підвищення якості прийнятих рішень у процесі виявлення та протидії шкідливій інформації; сортування інформаційна об'єктв впливу для оператора за пріоритетом; задання вхідних даних налаштування системи виявлення та протидії поширенню шкідливої інформації в мережах.

Основна частина

На теперішній час в мережі Інтернет функціонує велика кількість інтернет-майданчиків та форумів (спеціалізованих інформаційних ресурсів), які використовуються учасниками мережі для обговорення механізмів та способів несанкціонованого доступу до конфіденційних даних, а також забезпечення безпеки інформації. Частина зареєстрованих користувачів цікавляться відомостями про захист та безпеку інформації, інші – способами здійснення атак на інформаційно-комунікаційні системи і мережі. Форуми можуть розглядатися як джерела інформації про вразливості, шкідливе програмне забезпечення, комп'ютерні атаки тощо.

На інтернет-ресурсах переважна більшість тем обговорення присвячено висвітленню наступних питань: програмування з метою реалізації вразливостей та загроз безпеки інформації; програмне забезпечення, що використовується для організації та проведення комп'ютерних атак; шахрайство з використанням сучасних інформаційних технологій; поширення та створення шкідливого програмного забезпечення; забезпечення сеансу анонімності при здійсненні протиправних дій із застосуванням сучасних інформаційних технологій; переведення в готівку викрадених коштів, протиправні операції з банківськими картками; захист інформації. Перераховані теми відповідають актуальним загрозам безпеки конфіденційним даним [6,8,12], що надає можливість розглядати тематичні інтернет-ресурси як джерела повідомлень для проведення аналізу та виявлення вразливостей і загроз. Події, що відбуваються у конкретній предметній області, знаходять свій відбиток на відповідних дискусійних інтернет-майданчиках. Серед тематичних учасників інтернет-ресурсів присутні учасники, які володіють відомостями про вразливості та загрози безпеці інформації, а також потенційні зловмисники, зацікавлені в подоланні механізмів та засобів захисту конфіденційних даних.

Зазначені фактори надають можливість прогнозувати вразливості та загрози інформаційної безпеки даних, ґрунтуючись на проведеному аналізі повідомлень тематичних інтернет-ресурсів, використовуючи, при цьому, закономірності, характерні для процесу обговорення вразливостей та загроз. В загальному вигляді процес аналізу тематичних інтернет-ресурсів та їх інформаційного наповнення наведено на рис. 1.

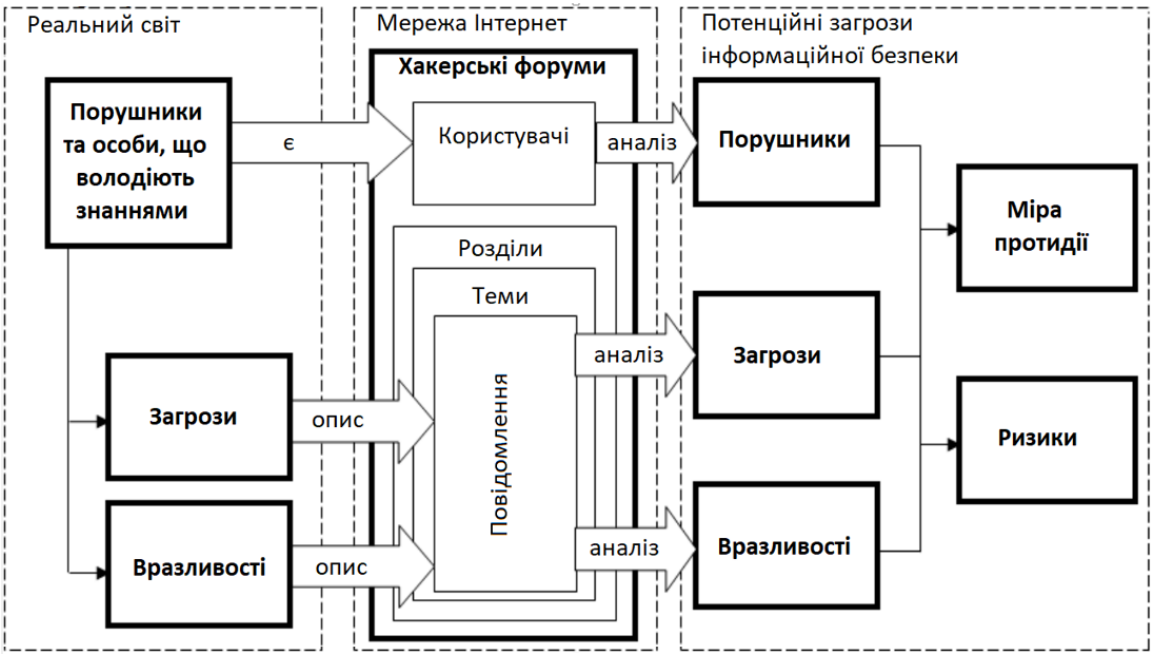

Рис.1. Інформаційне наповнення тематичних інтернет-ресурсів

Для повідомлень інтернет-форуму, доступна інформація, про автора, час його створення, приналежність до відповідного форуму та до теми форуму, кількості повідомлень по темі форуму, рейтинг автора. Наведена структура повідомлень дозволяє проводити статистичний та семантичний аналіз інформації форуму. В результаті проведення семантичного аналізу інформації форумів можливо здійснення фільтрації тих даних, які не мають відношення до заданої предметної області вразливостей та загроз безпеці інформації. На наступному кроці проведення аналізу виключаються дані, що не містять інформації про інформаційну безпеки, відповідно, досліджується інформація, що відноситься до вразливостей і загроз.

На теперішній час, для ефективного опису предметної галузі застосовується онтологія. При використанні даного підходу для опису предметної галузі застосовують її представлення у вигляді сукупності понять, враховуючи організацію та існуючі властивості, зв'язки між ними. Онтологічні механізми та методи дозволяють обчислювати відстань (близкість) повідомлень форумів до термінів предметної області, заданої онтологією. Повідомлення, що мають нульове значення коефіцієнта близькості (відстані) до термінів онтології, не мають відношення до предметної області, що аналізується [12].

Для функціонування тематичних інтернет-ресурсів характерна закономірність, яка полягає в наступному: з появою вразливості чи загрози безпеці інформації користувач форуму, якому відомо про загрозу, створює нову тему на інтернет форумі та залишає інформацію. Інші користувачі інтернет форуму залишають у новій створеній темі повідомлення, в яких спростовують чи доповнюють попередні повідомлення. Таким чином, в залежності від важливості інформації, що обговорюється на тематичному інтернет-ресурсі, проводиться оцінка внутрішнього рейтингу користувачів повідомлень. Високій значущості теми інтернет форуму відповідний високий рейтинг користувачів повідомлень, також закономірне збільшення частоти появи інформації у темі інтернет форуму, де обговорюється важливі повідомлення, особливо на початковій стадіяї проведення дискусії. Зазначені закономірності можуть бути задані та описані у вигляді відповідних правил нечітких продукцій, що застосовуються в інформаційних системах логічного нечіткого виводу.

Для прогнозування вразливостей та загроз безпеці конфіденційних даних можуть використовуватись результати проведеного аналізу повідомлень тем інтернет-ресурсів. Для вирішення даної задачі необхідно провести статистичний аналіз потоку даних інтернет-форуму та застосувати, при цьому, системи логічного нечіткого виводу. Учасники тематичних інтернет-форумів можуть створювати повідомлення, які не відносяться до предметної області, що аналізується. Для виключення їх з числа аналізованих доцільно застосовувати методи семантичного аналізу. Тобто, вхідними даними в системі нечіткого виводу можуть бути використанні статистичні параметри, що характеризують інформаційний процес обговорення вразливостей та загроз інформаційної безпеки. Нечіткі правила системи нечіткого виводу описують закономірності зміни потоку інформації інтернет-ресурсів, правила розміщенні в базі нечітких продукцій. Обґрунтованість використання нечітких моделей в системі протидії пов'язана зі значним ступенем присутньої невизначеності в інформації, що підлягає аналізу, складності предметної області та неповноти інформації інтернет-форумів [12,14].

Грунтуючись на результатах прогнозування, отриманих при виникненні раніше невідомих вразливостей та загроз інформаційної безпеки, спеціаліст, який здійснює захист інформації підприємства, може оцінити ступінь небезпеки атак та вжити необхідних заходів щодо усунення можливих загроз та вразливостей, переглянути відповідно ситуації моделі загроз інформаційної безпеки системи протидії.

Розглянуті особливості функціонування форумів тематичних інтернет-ресурсів дозволяють системі протидії здійснювати прогнозування виникнення вразливостей та загроз безпеки конфіденційних даних. Для вирішення цього завдання необхідне проведення аналізу інтернет повідомлень, створюваних учасниками форумів тематичних інтернет-ресурсів, що може бути здійснено відповідно до алгоритму прогнозування (рис. 2). Вхідними параметрами запропонованого алгоритму є список форумів тематичних інтернет-ресурсів, онтологія вразливостей та загроз безпеки інформації, система логічного нечіткого виводу.

Алгоритм передбачає виконання наступних кроків:

1. Пошук нових форумів тематичних інтернет-ресурсів та додавання виявлених до наявного списку форумів.

2. Пошук нових термінів предметної області у наявних тематичних інтернет-ресурсів вразливостей та загроз безпеки конфіденційних даних, додавання нововиявлених термінів в онтологію.

3. Збір потоку повідомлень тематичних інтернет-ресурсів.

4. Проведення семантичної фільтрації потоку повідомлень тематичних інтернет-ресурсів із використанням онтологічних методів.

5. Додавання інформації, що пройшла етап семантичної фільтрації інтернет-ресурсів, до бази даних прецедентів.

6. Статистичний аналіз потоку повідомлень, що зберігаються в базі даних прецендентів.

7. Логічний нечіткий вивід про виникнення вразливостей та загроз безпеки конфіденційних даних.

8. Підготовка відповідного звіту про виявлену вразливість чи загрозу безпеки інформації.

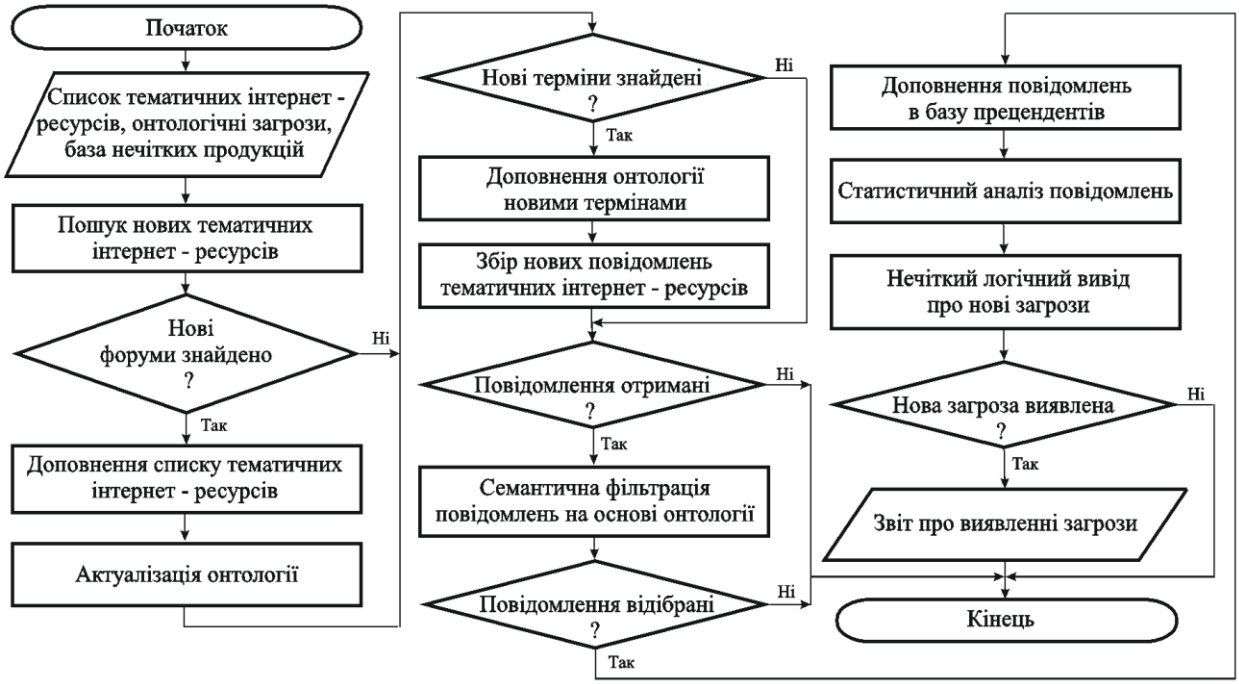

Рис.2. Алгоритм прогнозування вразливостей та загроз інформаційної безпеки

Результатом роботи алгоритму прогнозування вразливостей та загроз інформаційної безпеки є звіти про виявлених вразливостей, загроз інформаційної безпеки конфіденційних даних. До звітів можуть також включатися відомості, що відображають отриманні результати аналізу текстових повідомлень, на підставі яких здійснено висновок про виникнення вразливостей та загроз. Такими відомостями в період проведення аналізу можуть бути: частота створення участниками на форумах тематичних інтернет-ресурсів повідомлень, що відносяться до предметної області вразливостей та загроз інформаційної безпеки даних; частотна характеристика термінів вразливостей та загроз інформаційної безпеки даних, присутніх у повідомленнях інтернет-ресурсів; середній рейтинг користувачів повідомлень, що відносяться до предметної галузі вразливостей та загроз інформаційної безпеки даних; список присутніх у повідомленнях користувачів термінів онтології вразливостей та загроз інформаційної безпеки даних, що дозволяє класифікувати прогнозовані вразливості та загрози; добірка текстів тематичних інтернет-ресурсів, що містять терміни вразливостей та загроз інформаційної безпеки даних, створені на форумах.

Алгоритм прогнозування вразливостей та загроз безпеки інформації відрізняється можливістю виявлення вразливостей та загроз на ранніх етапах, їх практичної реалізації, ґрунтується на проведення аналізу потоку повідомлень форумів тематичних інтернет-ресурсів, що в даній ситуації дозволяє спеціалістам з інформаційної безпеки приймати адекватні та своєчасні заходи щодо захисту конфіденційних даних організації.

На підставі описаних вище особливостей функціонування тематичних інтернет-ресурсів та методів семантичної фільтрації текстових повідомлень послідовність проведення аналізу створюваних учасниками форуму повідомлень в період проведення аналізу може бути представлена алгоритмом фільтрації потоку тематичних повідомлень та статистичного аналізу інформаційної безпеки (рис. 3).

Запропонований алгоритм фільтрації потоку повідомлень та статистичного аналізу передбачає фільтрацію тематичних повідомлень, що не відносяться до заданої предметної області, яка задана відповідною онтологією, а також підрахунок кількості текстових повідомлень, що пройшли етап фільтрації потоку даних, та визначення середнього рейтингу авторів текстових повідомлень.

Вхідними параметрами алгоритму фільтрації потоку повідомлень та статистичного аналізу інформаційної безпеки є: D_τ – множина текстових повідомлень тематичних інтернет-ресурсів, створених в період проведення аналізу потоку даних; O – онтологія предметної області вразливостей та загроз інформаційної безпеки конфіденційних даних.

Основні кроки алгоритму проведення аналізу потоку текстових повідомлень наступні:

1. Обнулення значень K_τ – кількості тематичних повідомлень про вразливості та загрози інформаційної безпеки конфіденційних даних та A_τ – середнього рейтингу авторів тематичних повідомлень створених у період часу проведення аналізу τ.

2. Обчислення для кожного текстового повідомлення коефіцієнта k_{Ont} – близькості до термінів предметної області O заданої онтології.

3. Додавання тематичних повідомлень множини D_τ, для яких виконується нерівність $k_{Ont}>0$, до бази даних прецедентів для їх подальшого використання для формування відповідних звітів про прогнозування вразливостей та загроз інформаційної безпеки конфіденційних даних.

4. Обчислення K_τ – кількості повідомлень множини D_τ, для яких виконується нерівність $k_{Ont}>0$.

5. Обчислення A_τ – середнього рейтингу авторів тематичних повідомлень множини D_τ , для яких $k_{Ont}>0$.

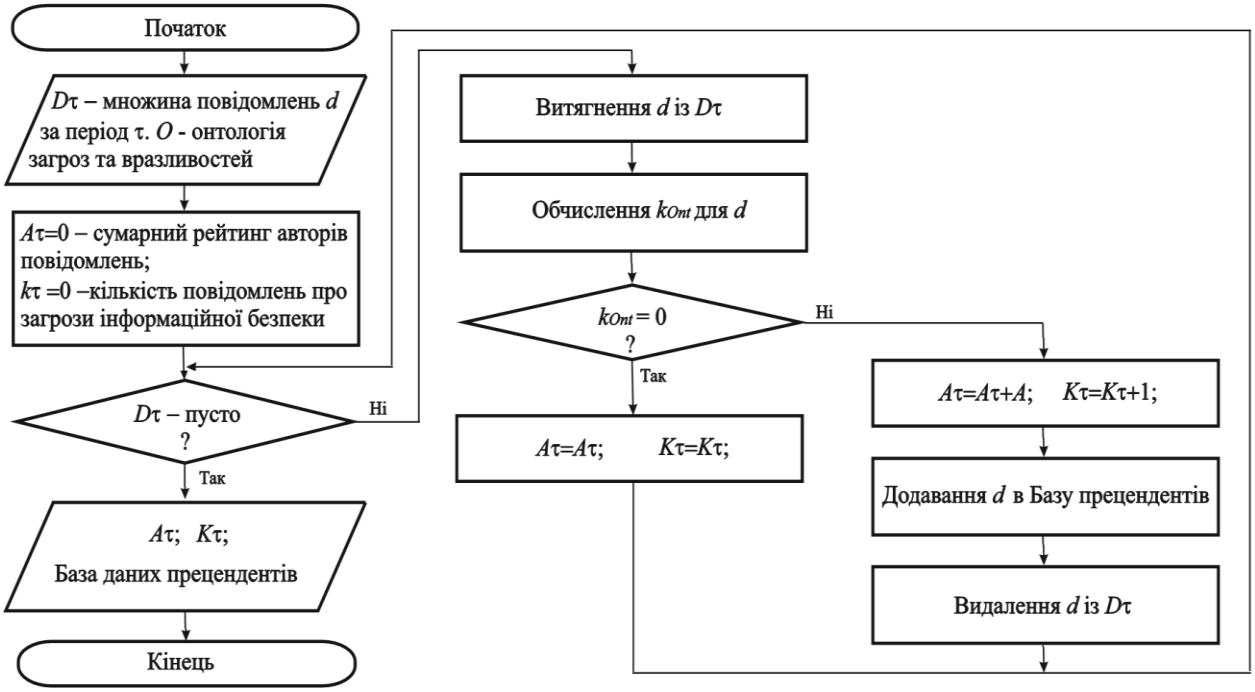

Рис.3. Алгоритм фільтрації та статистичного аналізу потоку тематичних повідомлень

Результатом роботи алгоритму є визначення статистичних показників, що характеризують потік тематичних повідомлень в період проведення аналізу потоку даних: K_τ – кількість текстових повідомлень, що містять терміни вразливостей та загроз інформаційної безпеки з онтології конфіденційним даним; A_τ – середній рейтинг авторів тематичних повідомлень, що містять терміни вразливостей та загроз інформаційної безпеки з онтології конфіденційним даним; поповнення бази даних прецедентів текстовими повідомленнями, що містять терміни вразливостей та загроз інформаційної безпеки з онтології конфіденційним даним. Алгоритм дозволяє обчислювати статистичні параметри, здійснювати семантичну фільтрацію текстових повідомлень. Результати роботи алгоритму можуть бути використанні для побудови системи логічного нечіткого виводу для прогнозування подій предметної області, для якої проводиться аналіз. Отриманні результати застосування алгоритму аналізу потоку текстових повідомлень можуть бути використані як значення вхідних параметрів у системі логічного нечіткого виводу та при формуванні звітів прогнозування вразливостей та загроз інформаційній безпеці організації.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Алгоритм прогнозування вразливостей та загроз безпеки інформації, заснований на логічному нечіткому виводі, семантичному та статистичному аналізі, відрізняється від аналогів можливістю виявлення вразливостей та загроз до їх безпосередньої реалізації. Він дозволяє гнучко описувати закономірності процесу наповнення тематичних форумів інтернет-ресурсів новими текстовими повідомленнями, що в результаті сприяє покращенню якості прогнозування загроз. Для вирішення задачі прогнозування вразливостей та загроз безпеки інформації запропоновано алгоритм фільтрації потоку тематичних повідомлень та статистичного аналізу інформаційної безпеки, заснований на семантичному та статистичному аналізі і відрізняється від аналогів можливістю обчислювати статистичні параметри, здійснювати семантичну фільтрацію текстових повідомлень, для прогнозування подій системи нечіткого логічного виводу.

Запропоновані алгоритми дозволяють прогнозувати вразливості та загрози, вживати адекватних заходів щодо захисту інформації. Отримані результати свідчать про ефективність запропонованих алгоритмів прогнозування вразливостей та загроз, а також підтверджують коректність роботи інформаційно-аналітичної системи та можливості застосування на практиці.

Література

1. Ленков С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк. // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Ленков С.В. Інформаційно-аналітична системи прогнозування вразливостей та загроз інформаційної безпеки / С.В. Ленков, В.М. Джулій, О.В. Мірошніченко, В.О. Браун, С.І. Прохорський. // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка.– К.: ВІКНУ, 2023. – Вип. №79. – С. 114-127.

3. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки / В. Джулій, Н. Петляк, Ю. Хмельницький, О. Пахар. // Вісник Хмельницького національного університету. Технічні науки. – 2022. – № 5. – С. 294-300.

4. Lienkov S., Podlipaiev V., Tolok I., Lisitsky I., .Lytvynenko N., Kuznichenko S. The Information and Analytical Using of Non-Structured Information Resources CEUR Workshop Proceedingsthis link is disabled, 2021, 3126, pp. 81–87.

5. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

6. Ленков С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К: Арий, 2008. – 464с

7. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Харків : Вид-во ХНЕУ, 2016. – 476 с.

8. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук. // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – К.: ВІКНУ. – 2017. – Вип. № 56. – С.124-132

9. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах / І.В. Муляр, В.М. Джулій, В.М. Пічура, О.О Зацепіна. // Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022). – С.73–78.

10. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки / В.М. Джулій, Ю.В. Хмельницький, Н.С. Петляк, О.В. Пахар. // Вісник Хмельницького національного університету. Технічні науки. 2022. № 5. С. 294-300с.

11. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. / Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. // Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

12. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

13. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми: Сумський державний університет, 2017. – 212 с.

14. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.

15. Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. / L.Yemchuk, O. Zhylinska; A. Chornyi; V. Dzhuliy // – Institute of Electrical and Electronics Engineers (30 September 2020); INSPEC Accession Number: 20008165; DOI: 10.1109/ACIT49673.2020.

References

1. Lenkov S.V. Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. Orlenko, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu KNU im/ Tarasa Shevchenka. – K.: VIKNU, 2020. – №68. – pp. 53-64.

2. Lenkov S.V. Informatsiino-analitychna systemy prohnozuvannia vrazlyvostei ta zahroz informatsiinoi bezpeky / S.V. Lenkov, V.M. Dzhulii, O.V. Miroshnichenko, V.O. Braun, S.I. Prokhorskyi // Zbirnyk naukovykh prats Viiskovoho instytutu KNU im/ Tarasa Shevchenka. – K.: VIKNU, 2023. – №79. – pp. 114-127.

3. Model potoku tekstovykh povidomlen tematychnykh internet-resursiv systemy prohnozuvannia informatsiinoi bezpeky / V. Dzhulii, N. Petliak, Yu. Khmelnytskyi, O. Pakhar // Herald of Khmelnytskyi National University. Technical sciences. – 2022. – № 5. – pp. 294-300.

4. Lienkov, S., Podlipaiev, V., Tolok, I., Lisitsky I., .Lytvynenko, N., Kuznichenko, S. The Information and Analytical Using of Non-Structured Information Resources CEUR Workshop Proceedingsthis link is disabled, 2021, 3126, стр. 81–87.

5. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011– 02–23/26490.htm

6. Metodyy sredstva zashchytы ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko – K: Aryi, 2008. –464s.

7. Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU, 2016. – 476 s.

8. AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnyk naukovykh prats Viiskovoho instytutu KNU im/ Tarasa Shevchenka. – K.: VIKNU. 2017. – Vip. № 56. – p.124-132

9. Informatsiino-oznakova model shkidlyvoi informatsii v sotsialnykh merezhakh/ I.V. Muliar, V.M. Dzhulii, V. M. Pichura, O.O Zatsepina – Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – № 3 (2022) –S. 73–78.

10. Model potoku tekstovykh povidomlen tematychnykh internet-resursiv systemy prohnozuvannia informatsiinoi bezpeky / V.M. Dzhulii, Yu.V. Khmelnytskyi, N.S. Petliak, O.V. Pakhar // Herald of Khmelnytskyi National University. Technical sciences. 2022. № 5. S. 294-300s.

11. Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. / V.M. Dzhulii, Yu.P. Klots, I.V. Muliar, M.L. Zhylevych, A.V. Dzhulii // Herald of Khmelnytskyi National University. Technical sciences.– Khmelnytskyi. – 2021, – №5. – pp. 22–26.

12. Dzhulii, V.M. (), Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu KNU im/ Tarasa Shevchenka. – K.: VIKNU. – 2022. – Vyp. №74. – pp. 73-82.

13. Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet? 2017. – 212 p

14. Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury : monohrafiia. / S. F. Honchar. – Kyiv, 2019. – 175 s.

15. Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. / L.Yemchuk, O. Zhylinska; A. Chornyi; V. Dzhuliy // Institute of Electrical and Electronics Engineers (30 September 2020); INSPEC Accession №: 20008165; DOI: 10.1109/ACIT49673.2020.