УДК 004.65

ДОСЛІДЖЕННЯ АСПЕКТУ ДІДЖИТАЛІЗАЦІЇ ТА ІМПЛЕМЕНТАЦІЇ СТАНДАРТІВ PAPERLESS ПРИ ФОРМУВАННІ ТА БЕНЧМАРКІНГОВУ АНАЛІЗУ ЗВІТНИХ ПОКАЗНИКІВ З НАУКОВОЇ ДІЯЛЬНОСТІ

Борцова Ю.В., Люлька Б.В.

DOI: 10.15673/atbp.v14i4.2437

Анотація. *Ця стаття допоможе розглянути проблему використання суспільством web – ресурсів та потребу захисту від кібератак. В даному випадку – це захист даних.*

В даній статті описуються три підходи до локалізації віддаленого хоста в мережі: whois, traceroute, and distributed traceroute. whois основна база даних, яка містить інформацію про мережі, підтримується організацією InterNic. Також приведений загальний вигляд DoS–атак, та один з підходів до їх класифікації. Розробка системи захисту інформації неможлива без знань можливих наслідків від загроз. Далі йдеться про класифікацію загроз, поділених на 3 групи: інформаційна безпека, спосіб здійснення, за розташуванням джерела загрози.

Розповідається про шляхи несанкціонованого доступу до інформації та деякі класичні засоби захисту. про проведення аналізу вразливостей які можна виявити у системах, які користуються попитом у численної кількості хостинг провайдерів: cPanel на CentO. Інжекція SQL– це один з найпоширеніших типів вразливості безпеки веб-додатків.

Проблеми безпеки збору даних є дуже важливим питанням. Про Open Data Kit (ODK), дозволяє створювати цифрові форми без глибокого технічного досвіду.

Abstract. *This article will help to consider the problem of society's use of web resources and the need for protection against cyber attacks. In this case, it is data protection.*

This article describes three approaches to locating a remote host on a network: whois, traceroute, and distributed traceroute. whois, the main database that contains information about networks, is maintained by the InterNic organization. A general view of DoS attacks and one of the approaches to their classification is also given. The development of an information protection system is impossible without knowledge of the possible consequences of threats. Next, we talk about the classification of threats, divided into 3 groups: information security, the method of implementation, by the location of the source of the threat.

It tells about ways of unauthorized access to information and some classic means of protection. on conducting an analysis of vulnerabilities that can be detected in systems,

which are in demand by a large number of hosting providers: cPanel on CentO. SQL injection is one of the most common types of web application security vulnerabilities.

Data collection security issues are a very important issue. About the Open Data Kit (ODK), allows you to create digital forms without deep technical expertise.

Ключові слова: кібер атака, захист даних, інформаційна безпека, інформаційні технології
Keywords: cyber attack, cyber security, information security, information technology

Вступ

Останні кілька років стали періодом надзвичайно стрімких та масштабних змін у сфері інформаційно-комунікаційних технологій. Розвиток комп'ютерної сфери напряму впливає на цей процес. Для нашої держави цей період виявився сповненим нових викликів та загроз у кібербезпеці, які актуалізувались через низку зовнішніх і внутрішніх чинників. При цьому сформована за попередні періоди недостатність та невідповідність національної системи захисту безпеки держави у кіберпросторі призвела до того, що Україна досить повно відчула на собі наслідки реалізації загроз кібернетичній безпеці, а успішні кібератаки, вмотивовані інтересами окремих держав-суб’єктів, призвели до завдання значної шкоди численним комунікаційним системам та об’єктам критичної інфраструктури [1].

Кожна система потребує присутності технологій, які можуть оптимізувати роботу з нею. Аналіз існуючого іноземного досвіду свідчить про те, що в окремих державах здійснення перевірки готовності інфраструктурних об'єктів до кібератак і кіберінцидентів є усталеною практикою та невід'ємною складовою національної системи забезпечення кібербезпеки. При чому до вказаної діяльності поряд із державними органами активно залучаються представники приватного сектору.

Держава здійснює свої заходи для забезпечення інформаційної безпеки через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають необхідні повноваження, відповідно до законодавства [2].

Теоретичні основи:

Сучасний світ неможливо уявити без використання суспільством web – ресурсів. Проте традиційною ситуацією залишається і те, що коли щось входить до широкого вжитку суспільства – потребує захисту. В даному випадку – це захист даних [6].

Кількість користувачів мережі Internet стрімко зростає, що розширює можливості зловмисникам для отримання вигоди за рахунок можливості застосування зловмисного програмного забезпечення до більшої кількості комп'ютерних систем. Основним об'єктом для зловмисників є інформація, для якої необхідно забезпечити при її зберіганні цілісність, доступність і конфіденційність, що визначається стандартами безпеки [3].

Кібератака (англ. cyber-attack) — спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації і/або завдання збитків автоматизованій системі [4].

Можливість визначити джерело кібератаки дуже допомагає у припиненні таких атак. Якби ця здатність була добре розробленою, він би діяв як стримуючий фактор проти таких атак, оскільки може бути точне знання джерела таких атак використовується для юридичних, кримінальних, економічних або військових санкцій [13]. Процес відстеження атаки до її джерела також може бути розкрити корисні деталі, які допомогли б розробити ефективні заходи протидії подібним атакам у майбутньому. Це могло б навіть дозволити перервати поточну атаку [5].

Сучасне зловмисне програмне забезпечення представляє собою складні багатофункційні програмні системи та комплекси, які побудовані з використанням ефективних методів створення програмних засобів та методів поширення зловмисного коду.

Виявлення зловмисного програмного забезпечення здійснюється за допомогою різноманітних засобів. Ефективність та достовірність виявлення суттєво залежать від архітектури таких засобів, а також їх позиціонування та місця розміщення в комп'ютерних системах, зокрема, і локальних мережах. Дослідження відомих антивірусних методів та засобів вказують, що реалізація нових принципів, моделей та методів виявлення конкретних типів зловмисного програмного забезпечення шляхом створення відповідних систем потребує подальшого розвитку [3].

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт [9].

Аналіз досліджень і публікацій останніх років

Захист даних є однією з найважливіших завдань у сучасному світі. Репозиторії з відкритим доступом є таким типом джерел даних що виховує open access publishing (публікаційні) активності, а також є цінними ресурсами для аналітиків (open access analytics with open access repository).

Аналіз публікацій

В даній статті [5] описуються три підходи до локалізації віддаленого хоста в мережі: whois, traceroute, and distributed traceroute. whois основна база даних, яка містить інформацію про мережі, підтримується організацією InterNic. Послуга Whois доступна кожному користувачу Інтернету та запитам можна виконати електронною поштою. Whois має обмеження в тому, що він надає інформацію лише про домени верхнього рівня, але комп'ютери, пов'язані з доменом, можуть бути широко розповсюджені [10].

Traceroute - це програма, яка відображає маршрут, за яким слідує

IP -дейтаграма через Інтернет від вихідного хоста до хост призначення. Він використовує поле TTL (Time To Live) заголовка IP. Кожен маршрутизатор, який обробляє дейтаграму IP зменшує поле TTL. Коли поле TTL досягає нуля, маршрутизатор повинен відкинути пакет і надіслати повідомлення про помилку ініціатору дейтаграми.

Підхід до розподіленого трасування, використовуючи декілька шляхів через Інтернет, був представлений у [11]. Основна ідея полягає в тому, щоб запустити traceroute з кількох географічно розподілених комп'ютерів на той самий цільовий комп'ютер [11]. В статті також йдеться мова про Time Delay Method суть якого полягає в порівняні часових затримок між комп'ютером -жертвою та атакуючим комп'ютером.

В статті [6] приведений загальний вигляд DoS–атак, та один з підходів до їх класифікації, а саме за характером впливу, за метою впливу, за умовою початку атаки, за наявності зворотного зв'язку з об'єктом атаки, по розташуванню щодо об'єкта атаки, за рівнем моделі OSI на якому здійснюється атака. далі розповідається про два принципи виявлення DoS–атак: сигнатурний та поведінковий. Методи виявлення DoS–атак: методи контекстного пошуку (сигнатурні); методи аналізу станів (сигнатурні); методи на основі статистичних моделей (поведінкові); методи продукційних правил (комбіновані); методи імітації поведінки біологічних систем. Причини виникнення DoS–атак в комп'ютерній системі можна класифікувати наступним чином: помилка в програмному коді, що призводить до звернення до не використовуваних фрагментів адресного простору, виконанню неприпустимої інструкції або іншої необроблюваної виняткової ситуації, коли відбувається аварійне завершення серверного додатку; недостатня перевірка даних користувача, що призводить до нескінченного або тривалого циклу, вичерпання процесорних ресурсів, виділення занадто великого обсягу оперативної пам'яті; флуд – атака, пов'язана з великою кількістю зазвичай безглуздих або сформованих в неправильному форматі, запитів до комп'ютерної системи або мережевого обладнання, що призвела до відмови в роботі системи через вичерпання ресурсів системи – процесора, пам'яті або каналів зв'язку; атаки другого роду – атаки на системи безпеки, що призводять до їх помилкового спрацювання і недоступності комп'ютерної системи [12].

Загалом виділяють два методи виявлення DoS-атак – аналіз інформаційного мережевого потоку і аналіз журналів реєстрації операційної системи або додатків. Перший підхід до виявлення атак є більш ефективним з причини реагування в реальному масштабі часу. Тому основні дослідження зараз спрямовані на розробку способів і процедур виявлення атак в мережевому трафіку. Тут основним завданням є ідентифікація шкідливого трафіку. Більшість атак в даний час важко відрізнити від звичайних дій користувачів, у той же час, зворотне твердження так само справедливо – часто діяльність користувачів викликає ефекти, ідентичні ефекту від проведення розподіленої атаки відмови в обслуговуванні [7].

В тезисі [8] розповідається про те що, в даний момент відбувається інтенсивне впровадження новітніх інформаційних технологій, проникнення їх в усі сфери життєво важливих інтересів держави та суспільства, але інформаційні технології зумовили появу низки суттєвих проблемних питань. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Проблеми інформаційної безпеки України в сучасних умовах, принципи забезпечення захисту інформації є надзвичайно актуальними і вимагають поглибленого вивчення. Сьогодні точиться дискусія навколо цього питання, зокрема навколо оцінки критеріїв інформаційної безпеки, характеристик імовірних небезпек та їх структури, а також принципів побудови надійної системи захисту національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави (суспільства), так і для конкретної людини.

Розробка системи захисту інформації неможлива без знань можливих наслідків від загроз. Далі йдеться про класифікацію загроз, автор поділив їх на 3 групи: інформаційна безпека, спосіб здійснення, за розташуванням джерела загрози. В пункті про інформаційну безпеку мається на увазі загроза конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій. В пункті про спосіб здійснення автор розповів про випадкові – вихід з ладу апаратних чи програмних засобів, помилкові дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні й т.п.; навмисні – мають на меті завдання збитків інформаційній системі або користувачам та можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо, їх наслідки призведуть до руйнування (втрати) інформації, модифікації (зміни інформації на помилкову, яка коректна за формою і змістом, але має інший сенс), ознайомлення з нею сторонніх осіб, дії природного та техногенного характеру.

Вказав на актуальні загрози безпеці, спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах для створення ефективної системи безпеки інформації, розроблення та вдосконалення існуючих методів її захисту. Також звернув увагу на систему принципів ка дозволяє ефективно організувати роботу із захисту інформації. [8]

В статті [14] розповідається про шляхи несанкціонованого доступу до інформації та деякі класичні засоби захисту. Технічні засоби — електричні, електромеханічні, електронні і ін. типу пристрою. Програмні засоби — програми, спеціально призначені для виконання функцій, пов'язаних з захистом інформації. Змішані апаратно-програмні засоби, які реалізують ті ж функції, що й апаратні та програмні засоби окремо, і мають проміжні властивості. Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін) і організаційноправових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). На даний момент дані засоби захисту не є

дієвими і сучасний стан вимагає комплексного підходу. Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби мережевих ОС. найчастіше використовують Firewalls — брандмауерів (firewall — вогняна стіна). Між локальною і глобальною мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь трафік мережевого/транспортного рівнів, що проходить через них. Весь трафік мережевого/транспортного рівнів між локальною і глобальною мережами забороняється повністю — маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери посередники.

В статті [15] йдеться мова про проведення аналізу вразливостей які можна виявити у системах які користуються попитом у численної кількості хостинг провайдерів: cPanel на CentO. Інжекція SQL – це один з найпоширеніших типів вразливості безпеки веб-додатків. Неправильна конфігурація безпеки охоплює кілька типів уразливості, все зосереджено на недостатньому обслуговуванні або недостатній увазі до налаштування сервера. Завдяки програмному забезпеченню, що охоплює потенційний шкідливий код, вони часто заважатимуть роботі фактичного власника. Це так звані "помилково-позитивні" тригери, які зупинятимуть показ оновлень завдяки тому, що містять ключові слова, які потенційно можуть бути використані шкідливим чином. Безпека як складова є важливим елементом загальної якості обслуговування PQoS - це оцінка якості інформаційного обслуговування з точки зору сприйняття користувача як споживача цієї послуги. у кожному заході цифрової безпеки завжди існує людський фактор, оскільки соціальні інженери намагатимуться ввести власників хостингу чи постачальників послуг хостингу в обмін даними входу на ресурси, інакше недоступні для них. Цей спосіб злому не вимагає поглиблених технічних знань і складних сценаріїв, тому жоден брандмауер не може захистити його.

У статті [16] розповідається про те що дані мають вирішальне значення для багатьох неурядових організацій та дослідників для моніторингу та оцінки розгортання чи втручання та звітування перед донорами діяльність. Наприклад, організації можуть збирати інформацію про пацієнтів під час відвідування поліклініки оцінити поширеність шкідників на сільських угіддях, або документальна інфраструктура, що потребує ремонту. ODK дозволяє використовувати цифрові форми та буде використовуватися як платформа багатьох організацій.

Проблеми безпеки збору даних є дуже важливим питанням. Автори розповідають про Open Data Kit (ODK), який було спочатку створено дослідниками у 2008 році з метою надання загального інструменту для полегшення збору даних. ODK дозволяє створювати цифрові форми без глибокого технічного досвіду. Він підтримує традиційний текст та питання з кількома варіантами вибору і використовує датчики на пристроях для збору різноманітних типів даних, включаючи місцезнаходження GPS та фотографії. автори провели опитування та співбесіди з організаціями, які використовують ODK, щоб зрозуміти, які моделі загроз розглядаються на місцях.

Використовуючи модель загроз, опитування та результати інтерв'ю, є можливість надавати рекомендації організаціям, які прагнуть зберегти їхні дані захищені

Практичне значення отриманих результатів

Виявлені та передбачені заздалегідь кібератаки можна звести до мінімуму.

Багаторівнева система безпеки дозволяє вчасно виявляти різну підозрілу активність в інфраструктурі, забезпечує додатковий захист облікових даних користувачів від крадіжки та захищає комп'ютери працівників від запуску шкідливого програмного забезпечення. Система дозволяє мінімізувати наслідки у разі успішної атаки, ізолюючи заражений ПК від решти інфраструктури. Інструменти аналітики дозволяють визначити джерело загрози захисту від поширення вірусів. Знижує ризики зупинення бізнес-процесів та фінансових втрат у результаті спрямованої кібератаки. Знижує репутаційні ризики. Мінімізує наслідки у разі успішної атаки.

Сам собою активний захист передбачає своєчасний аналіз загроз у сукупності з плануванням та вжиттям заходів протидії конкретним сценаріям реалізації подібних загроз. Активний захист означає не відмову від традиційних функцій служби ІБ, а їхнє вдосконалення в рамках існуючої системи управління інформаційною безпекою.

Для ефективної побудови системи співробітники служби ІБ повинні переконатися, що вони мають чітке уявлення про ті активи, які є найбільш ймовірними цілями потенційної атаки.

На наступному етапі фахівці в галузі ІБ мають отримати уявлення про нормальний стан мережі. Визначення та розуміння базового стану є важливим для підвищення ефективності служби інформаційної безпеки, оскільки активний захист передбачає подальше його застосування для аналізу аномальної активності, відхилень від базового стану та пошуку/ідентифікації зловмисників. Раніше згадувалося, що дії кіберзлочинців не потрапляють у категорію загальновідомих, оскільки методи та механізми зараження постійно вдосконалюються, а під час атаки маскуються. Проте за наявності моделі нормальної поведінки в мережі існує можливість розпізнати подібну шкідливу активність.

Для команди фахівців ІБ програма активного захисту допомагає розробити чіткий набір заходів щодо покращення системи безпеки на основі отриманих даних про кіберзагрози та аналізу результатів моніторингу, а потім пов'язати їх із конкретними цілями. Так, команда фахівців розробляє заходи протидії загрозам, вишукує прихованих порушників, які отримують доступ до мережі, та точково посилює захист на підставі актуальних звітів щодо поведінки реальних зломщиків.

Для керівництва перевага активного захисту полягає у можливості розподіляти ресурси з використанням більш практичних індикаторів ефективності кібербезпеки. Замість таких показників, як кількість застосованих патчів або

закритих заявок, про ефективність діяльності можна судити, наприклад, збільшення кількості виявлених і зупинених цільових атак на організацію або скорочення часу, необхідного для виявлення та усунення наслідків проникнень.

Перелік використаних джерел

[1]. http://academy.ssu.gov.ua/ua/page/page_1581426264.htm // Національна академія Служби безпеки України: [Веб-сайт]. URL: http://academy.ssu.gov.ua (дата звернення: 12.03.2021).
[2]. МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА // МІЖНАРОДНА ІНФОРМАЦІЯ ТА СУСПІЛЬНІ КОМУНІКАЦІЇ. Луцьк. С. 326.
[3]. Савенко О. С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах. : дис. на здобуття наук. ступеня доктор технічних наук : 05.13.05 : захищена 25.10.2019 : затв. naN.NaN.NaN / Савенко Олег Станіславович. - Львів. - 27 с.
[4]. Вікіпедія // Вікіпедія. - URL: https://uk.wikipedia.org/wiki/Перелік_кібератак (дата звернення: 07.09.2021
[5]. DETECTING A CYBER-ATTACK SOURCE IN REAL TIME R. Romanyak1 , A. Sachenko1 , S. Voznyak1 , G. Connolly2 , G. Markowsky2
[6]. ПРОГНОЗУВАННЯ ТА АНАЛІЗ DDOS - АТАК НА ІНФОРМАЦІЙНІ WEB – РЕСУРСИ / Вінницький національний технічний університет. - Вінниця. - 1 с.
[7]. Н.Р., Кондратенко. Виявлення аномалії на основі стохастичної нейротехнології / Кондратенко. Н.Р., Никитюк. О.М.. // Вінницький національний технічний університет. – 2015. – 15. – С. 23-27.
[8]. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ / Національна академія Служби безпеки України. - М. Київ. - 28.31 с.
[9]. Попер ЗМІСТ Наст > Методи забезпечення інформаційної безпеки // Pidru4niki [Веб-сайт]. - URL: https://pidru4niki.com/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki (дата звернення: 08.09.2021).
[10]. Savage, S., Wetherall, D., Karlin, A. and Anderson, T. "Practical Network Support for IP Traceback," 295– 306. Proceedings of ACM SIGCOMM 2000. Stockholm, Sweden, Aug. 28–Sept. 1, 2000. New York: Association for Computing Machinery, 2000. https://doi.org/10.1145/347057.347560
[11]. Connolly, G., Markowsky, G., and Sachenko, A. "Distributed Traceroute Approach to Geographically Locating IP Devices". Proceedings of 2003 Spring IEEE Conference on Technologies for Homeland Security, Boston, USA, May 7-8, 2003.
[12]. А.П., Кортко. Види ddos - атак та алгоритм виявлення ddos – атак типу flood – attack / Кортко. А.П.. // науковий журнал «Комп'ютерно – інтегровані технології: освіта, наука, виробництво». – 2015. – 18. – С. 18-25
[13]. Lee H., and Park, K. "On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack". Proceedings of IEEE INFOCOM 2001. Anchorage, Alaska, April 22–26, 2001. New York: IEEE Computer Society Press, 338–347, 2001.
[14]. Димкар В. М. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ / В. М. Димкар, І. В. Фірман; Львівський національний університет імені Івана Франка Департамент політики Міністра МВС України. - Львів. - 45.49 с.
[15]. Лагун А. АНАЛІЗ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ СУЧАСНОГО ХОСТИНГУ ПРИ ТЕСТУВАННІ НА ПРОНИКНЕННЯ / А. Лагун, А. Рудик, Ю. Рудик; Львівський державний університет безпеки життєдіяльності. - Львів. - 53.55 с.
[16]. Computer security for data collection technologies // Development Engineering. - . - № 3. - С. 1-11. https://doi.org/10.1016/j.deveng.2017.12.002

References

[1]. http://academy.ssu.gov.ua/ua/page/page_1581426264.htm // Natsionalna akademiia Sluzhby bezpeky Ukrainy: [Veb-sait]. URL: http://academy.ssu.gov.ua (data zvernennia: 12.03.2021).
[2]. MIZhNARODNA INFORMATsIINA BEZPEKA // MIZhNARODNA INFORMATsIIa TA SUSPILNI KOMUNIKATsII. Lutsk. S. 326.
[3]. Savenko O. S. Teoriia ta praktyka stvorennia rozpodilenykh system vyiavlennia zlovmysnoho prohramnoho zabezpechennia v lokalnykh komp'yuternykh merezhakh. : dys. na zdobuttia nauk. stupenia doktor tekhnichnykh nauk : 05.13.05 : zakhyshchena 25.10.2019 : zatv. naN.NaN.NaN / Savenko Oleh Stanislavovych. - Lviv. - 27 s.
[4]. Vikipediia // Vikipediia. - URL: https://uk.wikipedia.org/wiki/Perelik_kiberatak (data zvernennia: 07.09.2021
[5]. DETECTING A CYBER-ATTACK SOURCE IN REAL TIME R. Romanyak1 , A. Sachenko1 , S. Voznyak1 , G. Connolly2 , G. Markowsky2
[6]. PROHNOZUVANNIa TA ANALIZ DDOS - ATAK NA INFORMATsIINI WEB – RESURSY / Vinnytskyi natsionalnyi tekhnichnyi universytet. - Vinnytsia. - 1 s.
[7]. N.R., Kondratenko. Vyiavlennia anomalii na osnovi stokhastychnoi neirotekhnolohii / Kondratenko. N.R., Nykytiuk. O.M.. // Vinnytskyi natsionalnyi tekhnichnyi universytet. – 2015. – 15. – S. 23-27.

[8]. ZAKhYST INFORMATsII V INFORMATsIINO-KOMUNIKATsIINYKh SYSTEMAKh / Natsionalna akademiia Sluzhby bezpeky Ukrainy. - M. Kyiv. - 28.31 s.
[9]. Poper ZMIST Nast > Metody zabezpechennia informatsiinoi bezpeky // Pidru4niki [Veb-sait]. - URL: https://pidru4niki.com/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki (data zvernennia: 08.09.2021).
[10]. Savage, S., Wetherall, D., Karlin, A. and Anderson, T. "Practical Network Support for IP Traceback," 295– 306. Proceedings of ACM SIGCOMM 2000. Stockholm, Sweden, Aug. 28–Sept. 1, 2000. New York: Association for Computing Machinery, 2000. https://doi.org/10.1145/347057.347560
[11]. Connolly, G., Markowsky, G., and Sachenko, A. "Distributed Traceroute Approach to Geographically Locating IP Devices". Proceedings of 2003 Spring IEEE Conference on Technologies for Homeland Security, Boston, USA, May 7-8, 2003.
[12]. A.P., Kortko. Vydy ddos - atak ta alhorytm vyiavlennia ddos – atak typu flood – attack / Kortko. A.P.. // naukovyi zhurnal «Komp'yuterno – intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo». – 2015. – 18. – S. 18-25
[13]. Lee H., and Park, K. "On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack". Proceedings of IEEE INFOCOM 2001. Anchorage, Alaska, April 22–26, 2001. New York: IEEE Computer Society Press, 338–347, 2001.
[14]. Dymkar V. M. ZAKhYST INFORMATsII V KOMPIuTERNYKh MEREZhAKh / V. M. Dymkar, I. V. Firman; Lvivskyi natsionalnyi universytet imeni Ivana Franka Departament polityky Ministra MVS Ukrainy. - Lviv. - 45.49 s.
[15]. Lahun A. ANALIZ VYIaVLENNIa VRAZLYVOSTEI SUChASNOHO KhOSTYNHU PRY TESTUVANNI NA PRONYKNENNIa / A. Lahun, A. Rudyk, Yu. Rudyk; Lvivskyi derzhavnyi universytet bezpeky zhyttiediialnosti. - Lviv. - 53.55 s.\
[16]. Computer security for data collection technologies // Development Engineering. - . - № 3. - S. 1-11. https://doi.org/10.1016/j.deveng.2017.12.002

Отримана в редакції 07.11.2022. Прийнята до друку 14.11.2022. Received 07 November 2022. Approved 14 November 2022. Available in Internet 30 December 2022.