using machine learning [Text] // IEEE Access, 2020, Vol. 8. P. 155859-155872.
[12] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization [Text] // Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018, Vol. 1. P. 108-116.

A MODIFIED METHOD FOR DETECTING APPLIED-LEVEL DDOS ATTACKS ON WEB SERVER RESOURCES

The number of devices connected to the Internet is increasing every year, while DDoS attacks are becoming more frequent, causing downtime of the attacked system. The main challenge is to detect an attack in real time and identify its source. Application layer attacks are similar to client traffic in that they have a low request rate and use software vulnerabilities to drain computing resources. Moreover, HTTP is the most common protocol among application layer attacks, and existing methods are not characterized by both high accuracy and speed. An improved method for analyzing Internet traffic data to identify application-level DDoS attacks at the HTTP protocol level is proposed, which will have a shorter response time to intrusions than existing methods and an identical level of accuracy in detecting malicious traffic. The modified method is based on the calculation of information entropy with new attributes that characterize the application layer. We have found the parameters of HTTP requests, the analysis of which indicates low-rate DDoS attacks, and derived formulas for calculating their entropy. The proposed method makes it possible to increase the speed of identifying the sources of DDoS attacks on web servers, including those that use the HTTPS protocol, by the development of middleware for web frameworks. The structural and logical organization of the attack detection system is described. The proposed method based on the microservice architecture can improve the protection of web servers from DDoS attacks, since the identification time has decreased, and the accuracy has increased.

Keywords: DDoS attacks, HTTP, HTTPS, LR-DDoS, middleware, web-framework, microservices, information entropy.

Кравчук Аркадій Андрійович, магістрант, студент кафедри програмного забезпечення комп'ютерних систем факультету прикладної математики КПІ ім. Ігоря Сікорського.
Arkadii Kravchuk, master student, student of the department of computer system software, faculty of applied mathematics, Igor Sikorsky Kyiv Polytechnic Institute.
E-mail: arkakrava@gmail.com.
Orcid ID: 0000-0002-6128-206X.

Погорелов Володимир Володимирович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Pogorelov, PhD in engineering, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: volodymyr.pogorelov@gmail.com.
Orcid ID: 0000-0002-6100-1504.

DOI: 10.18372/2410-7840.24.17379
УДК 004.056

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ЗДІЙСНЕННЯ КІБЕРВПЛИВУ

Олексій Самчишин, Ганна Носова

У сучасному інформаційному суспільстві широке поширення одержав такий тип віртуальних спільнот як соціальні мережі. Завдання таких соціальних інтернет-сервісів полягає у тому, щоб забезпечити користувачів всіма можливими шляхами взаємодії одне з одним. Соціальні мережі, окрім виконання функцій підтримки спілкування, обміну думками вирішення своїх професійних потреб, політичних амбіцій, задоволення своїх інтересів у мистецтві, дозвіллі й одержання інформації членами віртуальних спільнот, все частіше стають об'єктами й засобами інформаційного та кібервпливу. Основними етапами проведення кібероперацій у соціальних інтернет-сервісах, що використовуються найчастіше, вважається: моніторинг відкритих джерел, акаунтів, груп, застосування методів соціальної інженерії і безпосередньо реалізація кібервпливів. В

умовах широкомасштабної війни рф проти України зі значною гібридної складовою, цифрові засоби масової комунікації та соціальні інтернет-сервіси широко використовуються противником для здійснення деструктивного інформаційно-психологічного та кібервпливів на військово-політичне керівництво, особовий склад та населення країни в цілому. Отже, аналіз вразливостей окремого користувача залежно від розміщеної ним інформації у соціальних мережах є актуальним, а розробка методів захисту від деструктивних кібервпливів дасть змогу в подальшому створити ефективну систему виявлення та протидії їм.

Ключові слова: *соціальна мережа, соціальний інтернет-сервіс, віртуальна спільнота, кібервплив, соціальна інженерія, вразливості користувача соціальної мережі.*

ВСТУП

Стрімкий розвиток високотехнологічного суспільства не в останню чергу обумовлений повсюдним проникненням в усі сфери його життєдіяльності новітніх досягнень у галузі інформаційних технологій. Важливу роль у такому суспільстві відіграють новітні цифрові засоби масової комунікації. При цьому основна функція яких зводиться до надання послуг соціального інтернет-сервісу (СІС), що забезпечує оперативний обмін інформаційними потоками між його суб'єктами та, як правило, спонукає до хаотичної керованої вихідної дії [1].

У сучасному інформаційному суспільстві поширення одержав такий тип віртуальних спільнот (ВС) в СІС, як соціальні мережі (СМ). СМ, окрім виконання функцій підтримки спілкування, обміну думками вирішення своїх професійних потреб, політичних амбіцій, задоволення своїх інтересів у мистецтві, дозвіллі й одержання інформації членами ВС – акторами, все частіше стають об'єктами й засобами інформаційного та кібервпливу. За допомогою СМ люди можуть здійснювати зв'язок між собою та об'єднуватися за специфічними інтересами. Завдання такого сервісу полягає у тому, щоб забезпечити користувачів всіма можливими шляхами взаємодії одне з одним [2].

Таким чином ВС у кіберпросторі є принципово новою стійкою формою існування соціальних відносин, які перевершують традиційні соціальні групи суспільства за ступенем організованості та впливу. Дослідження проведення кібервпливів у ВС переконливо свідчить про необхідність посиленої уваги з боку держави до діяльності та розвитку СМ. Водночас така увага має бути у межах зафіксованих у законодавстві прав людини [3, 9]. При цьому з'являється вразливість особистих даних громадян країни – зареєстрованих користувачів соціальних мереж через доступність для перегляду, моніторингу та незаконного використання інформації, яку користувач розміщує сам чи одержує від інших суб'єктів цієї мережі. Виявлені протиріччя надають можливості для порушників здійснювати кібервпливи більш точно з використанням даних розміщених користувачем у СМ.

В умовах широкомасштабної війни рф проти України зі значною гібридної складовою, цифрові засоби масової комунікації та СІС широко використовуються противником для здійснення деструктивного кібервпливу на військово-політичне керівництво, особовий склад та населення країни. Отже, аналіз вразливостей окремого користувача залежно від розміщеної ним інформації у СІС та розробка ефективної системи захисту від деструктивного кібервпливу з використанням СМ є актуальним і перспективним напрямом наукових досліджень та практичним розв'язанням питань посилення інформаційної безпеки держави.

ОСНОВНА ЧАСТИНА

Основними етапами проведення кібероперацій у СІС, що використовуються найчастіше, вважається: моніторинг відкритих джерел, акаунтів, груп у СІС (OSINT), застосування методів соціальної інженерії (СІ) і безпосередньо реалізація кібервпливів.

Методи СІ вважають одним із найбільш перспективних способів кібервпливу у СІС [4-8]. СІ може застосовуватись як самостійно, без використання технічних засобів, так і бути інструментом під час планування та проведення інших видів кібератак на об'єкт впливу із застосуванням закладених пристроїв та/або програмних закладок. У загальному тлумаченні СІ полягає в одержанні неавторизованим користувачем (порушником) несанкціонованого доступу до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншої конфіденційної інформації про об'єкт

впливу – актора (або групу людей), використовуючи його (їх) слабкість або некомпетентність, непрофесіоналізм або недбалість та керуючи його (їх) діями [10].

Технології СІ найчастіше використовують нині для таких цілей:

-збору довідкової інформації про об'єкт впливу, а саме з'ясування інтересів та особливостей поведінки потенційної жертви, чатів і форумів, якими вона користується, а також імен, під якими вона з'являється у мережі Internet шляхом ведення діалогу з нею або з її оточенням у ВС;

-одержання закритої (конфіденційної) інформації про об'єкт впливу або інформації, що становить для порушника певний інтерес, наприклад, номери телефонів потенційної жертви, адресу її прописки/проживання, реальне ім'я, прізвище та іншої подібної інформації шляхом встановлення контакту з нею та/або введення її в оману;

-одержання інформації про об'єкт впливу, що необхідна для забезпечення несанкціонованого доступу до системи, а саме пароля, яким користується потенційна жертва, серії й номеру її паспорта та інших відомостей про неї шляхом входження до жертви у довіру;

-примушення об'єкта впливу до дій, необхідних порушнику шляхом нав'язування такому об'єкту нової моделі поведінки.

Порушники, розробивши сценарій кібератаки, надсилають повідомлення об'єкту впливу, яке в свою чергу складається з інформаційного наповнення, відомостей про відправника й довідкового посилання на злоякісне програмне забезпечення та засіб доставки через СІС.

Застосування інформаційного наповнення повідомлення в атаках методом СІ вважається, порівняно з іншими складовими такого повідомлення, найбільш ефективним. Його перевага полягає в тому, що атака завжди буде вдалою, якщо порушник після завчано проведеної OSINT здатний сформулювати текст повідомлення таким чином, щоб зацікавити об'єкт впливу й примусити його відкрити.

Ще одним варіантом атак методом СІ, використовуваних порушниками для одержання спеціальної інформації, вважається створення підставних профілів у СМ і додавання у "друзі" до об'єкта впливу.

Все це дає підстави стверджувати, що повністю позбутися атак методом СІ нині неможливо.

Можна виділити такі напрямки щодо протидії кібервпливу у ВС: силові методи – закриття серверів; юридично-правові методи – притягнення до кримінальної відповідальності учасників ВС, інтернет-цензура; моніторинг ВС та протидія методами кібервпливу.

Перші два методи є більш ефективними в короткостроковій перспективі. Їх недоліками щодо недопущення правопорушень у кіберпросторі зумовленими багатьма об'єктивними причинами, які витікають з характерних властивостей ВС, серед яких насамперед доцільно виділити:

1) відсутність географічних кордонів та обмежень для миттєвого поширення, збирання, обробки та використання інформації, внаслідок чого Інтернет з його глобальними комунікаціями залишається поза сферою правового регулювання законів будь-якої держави, яка завжди має певну обмежену територію, де поширюється її суверенітет;

2) анонімність, яка підриває традиційне застосування юридичної відповідальності за скоєне правопорушення або злочин в інформаційній сфері, що забезпечує високий рівень латентності та низький рівень розкриття правопорушень;

3) легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної документально оформленої інформації електронна інформація не має форми, сталої у часі та просторі.

Основна особливість та головна небезпека деструктивних кібервпливів у ВС пов'язана з тим, що визнати за законом таку діяльність як деструктивну в умовах дії норм свободи слова, друку, віросповідання можливо тільки після реалізації в реальному світі їх учасниками якихось заходів. Тільки тоді факти події можуть бути співвіднесені з нормами чинного законодавства та кваліфіковані відповідним чином [11].

За таких умов метод моніторингу ВС, до яких в першу чергу належать СМ, є більш ефективним в довгостроковій перспективі щодо інформаційної та кіберпротидії деструктивним кібервпливам.

Тому визначення рівня вразливості окремого користувача за критерієм вільного доступу до інформації, реакції на вплив інформації на суб'єкт, доступності суб'єкта для кібервпливів є актуальним питанням.

Для проведення аналізу вразливості актора як об'єкта кібервпливу було обрано три СМ, які за статистикою (кількість користувачів, частота відвідування тощо) є найбільш популярними, а саме "Фейсбук", "ВКонтакте", "Однокласники".

"Фейсбук". Сторінка окремого актора СМ "Фейсбук" може містити великий обсяг інформації про його власника, однак розробники потурбувалися, аби доступ до цієї інформації був доволі закритим за бажанням користувача: незареєстрований у даній СМ суб'єкт не має доступу до особистих даних актора.

Виходячи з цього проведення кіберрозвідки або моніторингу об'єкта впливу з метою організації подальшого деструктивного кібервпливу на них передбачає наявність у суб'єкта протиправної діяльності (порушника) зареєстрованого акаунту.

"ВКонтакте" – мережа заснована у рф. Незареєстрованим у ній суб'єктам доступна для перегляду така інформація:

1) особисті дані: дата/місце народження, місце навчання, номер мобільного телефону, наявність родичів, місце проживання (тобто особиста інформація, розміщена самим актором). Достовірність цієї інформації непідтверджена нічим, хоча угода про розміщення (офіційний документ самого сайту) передбачає відповідальність користувача за надання хибної інформації;

2) перелік груп та ВС, до яких належить користувач;

3) фото та відео матеріали, розміщені актором як на його персональній сторінці, так і в альбомах, створених ним, з інформацією про час (дату) додавання матеріалів у мережу;

4) інформація, розміщена у стрічці персональної сторінки актора.

Крім того на сторінці актора є дані про його перебування у мережі на даний момент.

СМ "Однокласники" – одна з найбільш розповсюджених на теренах колишнього СНГ. Створена та підтримується у рф.

Для незареєстрованого інтернет-користувача доступна така інформація: ім'я користувача, вік, місце проживання, місце навчання (рік закінчення), список "друзів" користувача, особисті фото, замітки у статусі.

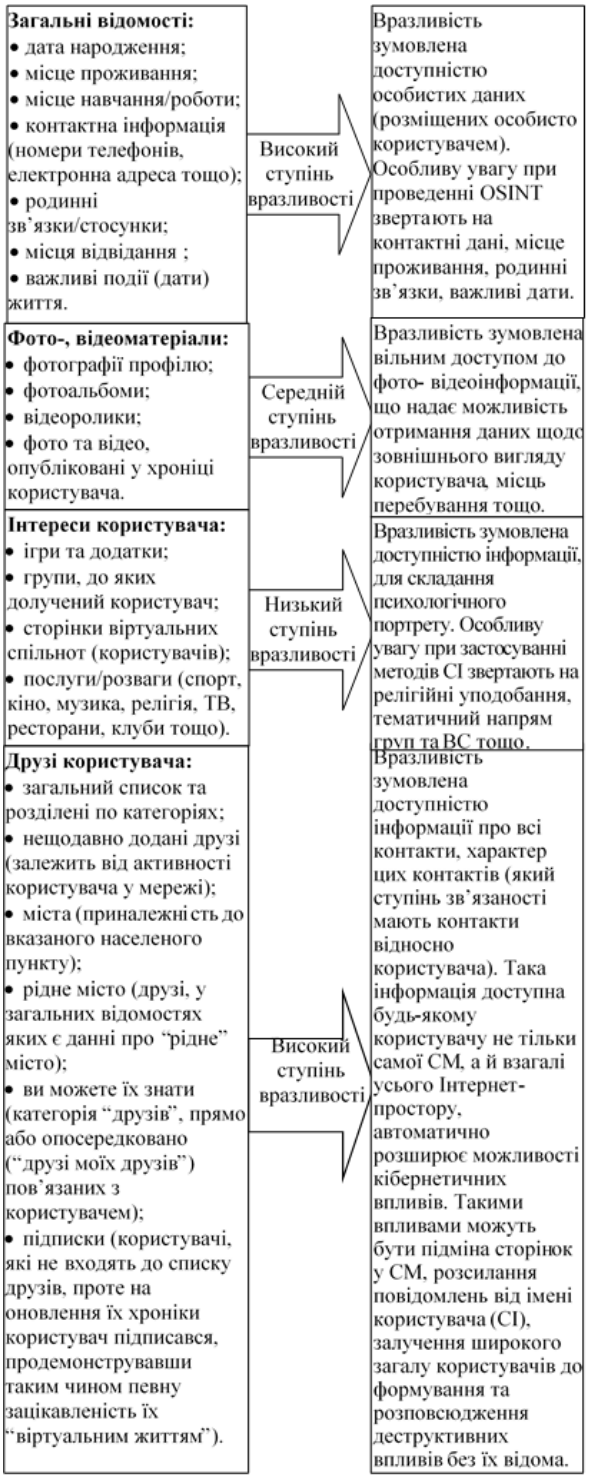

Рис 1. Схема вразливості актора СМ за аналізом його персональної сторінки

Загальними висновками з проведеного аналізу доступності персональних даних користувачів обраних СМ з позиції незареєстрованого у цих мережах інтернет-користувача є такі: достовірність розміщених даних завжди сумнівна, перевірити їх

неможливо, інформація доступна лише настільки, наскільки користувач не приховує її вбудованими у самій мережі налаштуваннями безпеки, не має доступу до повного переліку всіх можливих персональних даних.

Такі характерні риси "закриття" особистих даних мережі з одного боку слугують для забезпечення безпеки актора, а з іншого – не дозволяють проводити якісно моніторинг віртуальної поведінки та реакцій на зовнішні впливи вибраних користувачів [12].

Проаналізуємо вразливість актора СМ з позиції доступної для перегляду та моніторингу інформації, яку він розміщує сам чи одержує від інших суб'єктів цієї мережі. Для визначення ступенів вразливості можна розподілити всю інформацію за такими категоріями (рис 1).

Рівень деструктивного кібервпливу з використанням даних про актора у СМ визначається за сукупністю усіх груп показників з урахуванням ступеню важливості кожної групи (рішення обирається експертним методом).

ВИСНОВКИ

Кібервпливи у СМ методами СІ у сучасному цифровому суспільстві є одним із найпопулярніших напрямів кібератак, зважаючи на простоту реалізації, незначні фінансові вкладення та мінімальний ризик виявлення та протидії.

Це дає можливість порушникам отримати практично стовідсотковий ефект реалізації доступу до найзахищеніших інформаційних ресурсів об'єкта кібервпливу.

Важливим аспектом для забезпечення максимального захисту організацій, установ, підрозділів та органів управління від внутрішнього і зовнішнього, випадкового і навмисного деструктивного кібервпливу є привертання уваги особового складу до питань додержання кібергігієни у СІС, виконання персоналом вимог впровадженої політики безпеки, наказів, інструкцій та рекомендацій про порядок користування особистими засобами стільникового зв'язку, іншими електронними засобами для обміну інформацією, в тому числі службового характеру.

ЛІТЕРАТУРА

[1] Кремлева С.О. Сетевые сообщества. URL: http://www.follow.ru/ print. php? Id = 116&page=1 (дата звернення: 27.01. 2023).

[2] Дзюндзюк В.Б. Віртуальні співтовариства: потенційна загроза для національної безпеки // Державне будівництво [Електронне видання], 2011, №1. URL: http:// www. kbuapa. kharkov. ua. (дата звернення: 10.02. 2023).

[3] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны, монография. М.: Горячая линия-Телеком, 2003. 541 с.

[4] М. Кузнецов, И. Симдянов. Социальная инженерия и социальные хакеры. Петербург: БХВ-Петербург, 2007. 368 с.

[5] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки оперативного центру реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України. URL: http://surl. li/ewsrl (дата звернення: 12.02.2023).

[6] Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология. / под ред. В.Л. Иноземцева, 1999. С. 494-505.

[7] Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання, монографія. К.: Інтертехнологія, 2009. 163 с.

[8] Подцероб А. Б. Арабская смута: роль пропаганды и современных информационных технологий // Институт ближнего востока [Електронне видання], 2012. URL: http://www. iimes.ru/?p= 15619 (дата звернення: 12.01.2023).

[9] Доктрина інформаційної безпеки України: затверджена Указом Президента України № 514/2009 від 8 липня 2009 року [Електронний ресурс]. URL: http://www. president. gov. ua/ documents / 9570. html (дата звернення: 07.02. 2023).

[10] Сазонов В.М. Социальные сети – публичная сфера, монография. М.: Изд. Лаборатория СВМ, 2011. 223 с.

[11] Матвиенко Ю.А. Деструктивные сетевые социальные структуры как средство информационной войны и угроза безопасности России // Информационно-аналитический портал Геополитика [Електронне видання]. 2011. URL: http:/ /old. geopolitica. ru/ Articles / 1218/ (дата звернення: 10.02.2023).

[12] Гібридна війна: сутність, виклики та загрози: зб. матер. Круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. Київ: НА СБУ, 2021. 189 с URL: https://academy.ssu.gov.ua /uploads/ p_57_ 28744724.pdf (дата звернення: 14.02.2023).

FEATURES OF USING SOCIAL NETWORKS TO ACHIEVE CYBERINFLUENCE

In the modern information society, such a type of virtual communities as social networks has become widespread. The task of such social Internet services is to provide users with all possible ways of interacting with each other. Social networks, in addition to fulfilling the functions of supporting communication, exchange of opinions, meet their professional needs, political ambitions, satisfaction of their interests in art, permission and preservation of information by members of the virtual community, increasingly become objects and use of informational and cybernetic influence. Monitoring of open sources, accounts, groups, application of social engineering methods and realization of cybernetic influences are considered the main stages of conducting cybernetic operations in social Internet services that use them. In the conditions of the Russian Federation's large-scale war against Ukraine, which has a largely hybrid component, digital means of mass communication and social Internet services are widely used by the enemy to exert destructive informational, psychological and cybernetic influence on the military-political leadership, personnel and population of the country as a whole. Therefore, it is relevant to analyze the vulnerabilities of an individual user, depending on the information posted by him in social networks, and to develop methods of protection against destructive cybernetic influences, so that it is possible to create an effective system for detecting and countering them in the future.

Keywords: social network, social Internet service, virtual community, cyber influence, social engineering, vulnerabilities of social network users.

Самчишин Олексій Володимирович, кандидат технічних наук, старший дослідник, начальник кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П Корольова.

Oleksii Samchyhsyn, Candidate of Technical Sciences (PhD), Senior Researcher, Head at the Chair of Information Protection and Cybersecurity of Korolov Zhytomyr Military Institute.
E-mail: samyj123@ukr.net.
Orcid ID: 0000-0002-1542-1065.

Носова Ганна Дмитрівна, начальник науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.

Hanna Nosova, Head of Research and Organizational Department of Korolov Zhytomyr Military Institute.
E-mail: hannanos@ukr.net.
Orcid ID: 0000-0003-3573-9828.

DOI: 10.18372/2410-7840.24.17380
УДК 004.49

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ЧАТБОТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ ДЛЯ ДОСЛІДЖЕННЯ ЖУРНАЛІВ ПОДІЙ

Іван Опірський, Віталій Сусукайло, Святослав Василишин

Дана стаття аналізує можливість використання чат ботів зі штучним інтелектом для аналізу інцидентів інформаційної безпеки. Вона визначає, як чатботи можуть допомогти організаціям покращити швидкість та точність реагування на інциденти, зменшити навантаження в групах безпеки та мінімізувати вплив інцидентів. У статті розглядаються виклики, що стоять перед організаціями в реагуванні на інциденти, включаючи все більший обсяг та складність загроз та дефіцит кваліфікованих спеціалістів безпеки. Також розглядається, як штучний інтелект може допомогти організаціям вирішити ці проблеми, автоматизуючи звичайні завдання, такі як аналіз журналів подій та визначення індикаторів компрометації систем. Пропонуються способи майбутнього реагування на інциденти та ролі автоматизації в розслідуванні кібербезпеки. Також, проведено аналіз важливості збалансування автоматизації з людським досвідом та судженням, а також необхідністю постійних інвестицій у технології та персоналу, щоб випереджати нові загрози. В цілому стаття надає інформацію про переваги використання штучного інтелекту для реагування на інциденти інформаційної безпеки та підкреслює необхідність організацій сприймати чат ботів з штучним інтелектом як ключовий компонент їх стратегії кібербезпеки.

Ключові слова: *чатбот, Штучний Інтелект, кіберзлочини, кіберзагрози, кібербезпека, SIEM, інциденти, IDR, ChatGPT.*