УДК:343.983
https://doi.org/10.32703/2663-6352/2024-2-16-265-275

https://orcid.org/0000-0002-0892-1694
Михайлов Володимир Олександрович
старший викладач кафедри правосуддя
юридичного факультету
Інституту управління та технологій
Державного університету інфраструктури та технологій,
м. Київ Україна

Романенко Олександр Віталійович
Студент 2 магістерського курсу
Юридичного факультету
Інституту управління та технологій
Державного університету інфраструктури та технологій,
м. Київ Україна

ТЕМНА МЕРЕЖА (DARKNET) ЯК ДИНАМІЧНЕ СЕРЕДОВИЩЕ КІБЕРПРОСТОРУ ТА ІНСТРУМЕНТ ДЛЯ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Анотація. *В статті досліджено феномен темного інтернету (Darknet) як частини кіберпростору та інструменту для вчинення кримінальних правопорушень. Визначені основні ознаки та запропонований понятійний апарат "темної мережі" як із технологічної точки зору, так і інструменту і місця для вчинення кримінальних правопорушень. Зроблено висновок про те, що Darknet являє собою багатогранну загрозу для суспільства та національної безпеки, надаючи платформу для широкого спектру незаконної діяльності. Розкрито динамічність темної мережі через створення аналогів по типу месенджера Telegram, також вказано на інтеграцію штучного інтелекту в екосистему темної мережі, що створює нову, більш складну парадигму кіберзлочинності.*

Темна мережа (darknet) є частиною інтернету, яка не індексується традиційними пошуковими системами і доступна лише через спеціальне програмне забезпечення, як-от Tor. Вона забезпечує високий рівень анонімності, що робить її привабливою для різних користувачів, включаючи тих, хто хоче уникнути цензури, а також кіберзлочинців.

Темна мережа використовується для різних цілей, від легальних до незаконних. Наприклад, вона може бути інструментом для захисту свободи слова в країнах з жорсткою. Однак, вона також відома як місце для торгівлі

наркотиками, зброєю, фальшивими документами та іншими незаконними товарами.

Боротьба з незаконною діяльністю в темній мережі (darknet) є складним завданням, яке вимагає комплексного підходу. Ось кілька основних стратегій:

1. Міжнародна співпраця: Оскільки темна мережа не має кордонів, співпраця між країнами є ключовою. Це включає обмін інформацією та координацію дій правоохоронних органів.

2. Технічні засоби: Використання передових технологій для моніторингу та аналізу активності в темній мережі. Це може включати використання штучного інтелекту для виявлення підозрілих дій.

3. Правові заходи: Розробка та впровадження законодавства, яке дозволяє ефективно переслідувати кіберзлочинців. Це також включає посилення покарань за кіберзлочини.

4. Освіта та підвищення обізнаності: Інформування громадськості про ризики, пов'язані з темною мережею, та способи захисту від кіберзлочинів.

5. Спеціалізовані підрозділи: Створення спеціалізованих підрозділів у правоохоронних органах, які займаються виключно кіберзлочинами.

Ці заходи допомагають зменшити незаконну діяльність у темній мережі та підвищити безпеку в кіберпросторі.

Ключові слова. *Darknet, темна мережа, кіберпростір, незаконна діяльність.*

Annotation*. The article examines the phenomenon of the dark Internet (Darknet) as a part of cyberspace and a tool for committing criminal offenses. The author identifies the main features and proposes the conceptual framework of the Darknet both from the technological point of view and as a tool and a place for committing criminal offenses. It is concluded that the Darknet poses a multifaceted threat to society and national security, providing a platform for a wide range of illegal activities. The author reveals the dynamism of the Darknet through the creation of analogs such as the Telegram messenger, and also points to the integration of artificial intelligence into the Darknet ecosystem, which creates a new, more complex paradigm of cybercrime.*

The darknet is a part of the internet that is not indexed by traditional search engines and is only accessible through special software such as Tor. It provides a high level of anonymity, making it attractive to a variety of users, including those seeking to evade censorship, as well as cybercriminals.

The darknet is used for a variety of purposes, from legal to illegal. For example, it can be a tool to protect freedom of speech in countries with strict laws. However, it is also known as a place for the trafficking of drugs, weapons, fake documents, and other illegal goods.

Combating illegal activities on the darknet is a complex task that requires a comprehensive approach. Here are some key strategies:

1. International cooperation: Since the darknet has no borders, cooperation between countries is key. This includes sharing information and coordinating law enforcement efforts.

2. Technical means: Using advanced technologies to monitor and analyze dark web activity. This may include using artificial intelligence to detect suspicious activities.

3. Legal measures: Developing and implementing legislation that allows for effective prosecution of cybercriminals. This also includes increasing penalties for cybercrimes.

4. Education and awareness-raising: Informing the public about the risks associated with the dark web and ways to protect themselves from cybercrimes.

5. Specialized units: Creating specialized units within law enforcement agencies that deal exclusively with cybercrimes.

These measures help reduce illegal activities on the dark web and increase security in cyberspace.

***Keywords**. Darknet, dark web, cyberspace, illegal activity.*

Постановка проблеми. Інтернет за останні два десятиліття став невід'ємним елементом людського життя і новим (зручним і оперативним) інструментом комунікації в суспільстві. Поза всяким сумнівом, у цифрову епоху значна частина економічного, політичного і культурного життя протікає саме в інтернеті. Кіберпростір стає заміною фізичному простору.

Поряд із цілою низкою переваг, мережа Інтернет породила проблеми й виклики, яких раніше не існувало. Кіберпростір – як складник мережі Інтернет може бути використаний організованими злочинними групами, одиночними зловмисниками, військовими та спецслужбами держав для скоєння кримінальних правопорушень, проведення кібератак, дестабілізації військової та цивільної інфраструктури (включаючи критичну), збору конфіденційної інформації, а також для шпигунства в інтересах держав або великих корпорацій.

Цифровий всесвіт величезний, все набагато глибше, ніж те, що ми бачимо під час звичайного перегляду. За своєю структурою, мережа Інтернет складає певний "льодовик". Більшість користувачів Інтернету мають доступ до Інтернету через звичайні браузери, такі як Google Chrome. Інтернет, доступ до якого здійснюється за допомогою звичайного браузера, називається поверхневим Інтернетом (Clearnet), однак значна частина вмісту залишається прихованою на глибокому рівні мережі Інтернету (Deepnet). Термін "Темна мережа" (Darknet) є частиною глибокої мережі, на яку спрямована більшість злочинців, і вони координують та здійснюють злочинну діяльність саме в глибині темного Інтернету.

Саме останній "шар льодовика" і є предметом нашого дослідження, як найбільш анонімний, та небезпечний спосіб використання мережі Інтернет для вчинення кримінальних правопорушень, у тому числі кіберзлочинів. Злочинці можуть діяти з будь-якої точки світу, не зважаючи на кордони держав, і ховаючись від правоохоронних органів за допомогою технологій шифрування та анонімізації.

Аналіз досліджень і публікацій. Дослідження сучасної проблематики правового регулювання тіньового інтернету "Darknet" як простору для

незаконного використання мережі Інтернет висвітлюють такі вітчизняні вчені як Лановий О.Ф, М.В. Гуцалюк, В.О. Тімашов, Д.Ш. Діденко, О.Г. Козицька, М. Бутиріна, В.В. Степанчук, О.С. Тарасенко, а також іноземні вчені: Lacey D., Salmon P. M, Rathod Digvijaysinh, Worner and Preetz, Jason Chan, Shu He, Dandan Qiao, Andrew Whinston. Стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі, в тому числі мережі "Darknet", його динамічність та еволюція спонукає для подальших досліджень цієї сфери. Створення нових ресурсів для анонімізації, месенджерів такі як Signal, Telegram та масове поширення штучного інтелекту, розширюють темну складову мережі Інтернет.

Формулювання завдання дослідження. Мета дослідження полягає у комплексному вивченні феномену темного інтернету (Darknet) як динамічного середовища для вчинення кримінальних правопорушень. Дослідження спрямоване на вивчення сучасного стану кіберпростору, виявлення видів злочинів, що вчиняються за допомогою Darknet, включаючи роль штучного інтелекту та месенджера Telegram у цьому процесі.

Виклад основного матеріалу. Винахід телеграфу, телефону, радіо та комп'ютера підготував ґрунт для нинішньої безпрецедентної інтеграції. Інтернет одночасно є засобом світового мовлення, механізмом поширення інформації, а також середовищем для співпраці та спілкування людей, яке охоплює всю планету.

У сучасному суспільстві мережа Інтернет зайняла особливе місце, і її вже не можна розглядати лише як технологічну інфраструктуру, що задовольняє комунікаційні потреби громадян. Навколо мережі об'єдналося співтовариство її користувачів, яке утворило особливе соціальне середовище - мережевий інформаційний простір («кіберпростір»), у якому люди спілкуються, працюють, отримують освіту, здійснюють покупки, отримують різноманітні послуги, проводять дозвілля.

Кіберпростір — це абстрактний простір, не пов'язаний з фізичним місцезнаходженням, де взаємодіють різні цифрові пристрої, програмне забезпечення та мережі. Воно охоплює інтернет, вебсайти, платформи соціальних мереж та іншу цифрову інфраструктуру. Ці взаємопов'язані системи дозволяють обмінюватися інформацією, здійснювати комунікацію та співпрацювати у глобальному масштабі. [1]

Будучи надзвичайно рухомим і гнучким, середовище кіберпростору не тільки створює нескінченну кількість нових можливостей, але й породжує нові ризики, з якими людство ніколи раніше не стикалося. Кіберпростір поруч із реальним світом стає місцем здійснення кримінальних правопорушень.

Згідно з одним із джерел, станом на 15 вересня 2024 року кількість вебсторінок поверхневої мережі, проіндексованих Google, становить близько 40 мільярдів. [2]

"Глибинна мережа" (Deepnet) як друга сходинка "піраміди Всесвітньої мережі" включає веб-ресурси, які не є доступними для всіх. Це частина інтернету, до якої не можна отримати доступ через пошукові системи, такі як

Google, Yahoo та Bing. Глибока мережа складає від 90% до 95% всього інтернету. [3] Прикладами глибокого інтернету є особиста емейл-пошта в Gmail та Google Drive, оскільки вони не існують як загальнодоступні домени. Інші приклади включають, наприклад сторінку банківського рахунку в Приват24.

Окремою частиною глибинної мережі є темна мережа (Darknet), де користувачі діють анонімно та в зашифрованому вигляді. Темна мережа (Darknet) — це зароджувана «terra incognita», термін, який вперше з'явився в географії Птолемея близько 150 року н. е. для позначення регіонів, що не були нанесені на карту або задокументовані.

Термін «Даркнет» стосується підмножини інтернет-сайтів і сторінок, які не індексуються пошуковими системами. Даркнет часто асоціюється з доменом верхнього рівня ".onion", сайти якого називаються «Onion-сайтами» (від англ. onion – цибуля) і доступні через спеціальний браузер, наприклад Tor. [4]

Для доступу в темну мережу, особі, по суті, потрібно лише отримати доступ до правильних .onion-посилань або знати відповідні облікові дані. Однак додатково для доступу до даркнету потрібно встановити спеціальний клієнт, такий як Tor Browser, який приховує доступ і анонімізує користувача.

У випадку з Tor, доступ до "цибулевих сервісів" повністю зашифрований. Це означає, що особистість користувача краще захищена під час перегляду цибулевих сервісів у порівнянні зі звичайними вебсайтами, де останній запит з мережі Tor відправляється у незашифрованому вигляді.

Концепція даркнету є як революційною, так і одночасно простою. Його можна уявити як низку недоступних для пошукових систем мереж, що варіюються від простого копіювання жорстких дисків між друзями до складної екосистеми багатошарових анонімних мереж.

Хоча Darknet не гарантує абсолютної анонімності, він робить аналіз трафіку практично нездійсненним. У поєднанні з періодичним видаленням жорсткого диска майже неможливо визначити особу та місцезнаходження кінцевого користувача. Це означає, що запропоновані політики збереження даних стають безглуздими та невідслідковуваними.

Ознаками темної мережі як технології анонімності в мережі Інтернет є: шифрування трафіку, що забезпечує анонімність користувачів, децентралізованість системи без єдиного центру контролю, використання криптовалют для анонімних платежів, прихованість сервісів, доступ до яких можливий лише через спеціальне програмне забезпечення, а також шифрування даних користувачів (використання P2P архітектури).

Відтак, із технологічного боку темна мережа (Darknet) є накладеною (поверховою) мережею в мережі Інтернет, що використовує спеціалізовані протоколи, програмне забезпечення та інфраструктуру для забезпечення анонімності та приховування активності її користувачів.

Як інструмент для вчинення кримінальних правопорушень, темна мережа (Darknet) характеризується наступними ознаками: анонімність транзакцій (використання криптовалют для приховування фінансових слідів), зашифровані комунікації (екстремальні заходи для приховування змісту повідомлень),

приховані сервіси (веб-сайти з доменами .onion, недоступні через звичайні браузери), специфічна термінологія (використання жаргону та кодових слів), тимчасові ринки (платформи, що часто змінюють адреси) , системи репутації (механізми оцінки "надійності" учасників), складні схеми доставки (методи приховування фізичних поставок), посередницькі сервіси (використання "гарантів" для угод), захист від відстеження (методи маскування IP-адрес та інших ідентифікаторів), обмежений доступ (закриті форуми з суворими правилами вступу).

Виходячи із вищезазначеного, темна мережа (Darknet) із криміногенного боку є спеціалізованою мережевою інфраструктурою в мережі Інтернет, що використовується як інструмент для здійснення протиправної діяльності шляхом забезпечення високого рівня анонімності користувачів, шифрування комунікацій та транзакцій, та надання доступу до прихованих онлайн-ринків нелегальних товарів і послуг, ускладнюючи виявлення та переслідування злочинців правоохоронними органами.

Еволюція суспільних стосунків стає детермінантом росту рівня злочинності. Згідно із офіційною статистикою Офісу Генерального прокурора України, за останні 8 років кількість кіберзлочинів зросла майже в 7,5 разів, не враховуючи класичні правопорушення, пов’язані із використанням комп’ютерної техніки, а також показник латентності такого виду злочинності. [5]

Сьогодні активно формується ринок хакерських послуг, завдяки якому відбувається поєднання традиційної злочинності, включаючи організовані її форми, з кіберзлочинністю – адже немає потреби бути фахівцем в сфері інформаційних технологій – достатньо замовити відповідні послуги через Інтернет та розрахуватися за послуги криптовалютою. Даний кіберринок постійно зростає завдяки анонімності на основі спеціальних протоколів зв’язку, реалізованих в цьому інтерфейсі. [7]

Не дивно, що злочинці та інші зловмисники звернулися до темної мережі через обіцянку анонімної та безпечної платформи для «спілкування, координації та дій». Наразі однією з найбільш серйозних проблем у мережі Інтернет є поширення забороненого контенту.

Торгові майданчики мережі DarkNet ведуть свою діяльність з моменту запуску «Silk Road» (анонімна торгова інтернет-платформа, яка знаходилась у зоні .onion анонімної мережі Tor) у лютому 2011 року. Торгівля наркотичними засобами та психотропними речовинами вийшла на новий рівень у всьому світі. Поділ зон впливу, кримінал та конфлікти угруповань втратили сенс з появою інтернет-ринку, і сьогодні «вуличну» торгівлю наркотичними засобами можна вважати безповоротно минулою.

Що стосується збуту і придбання зброї, то на відміну від західного сегменту Darknet, де їй присвячені великі розділи на найбільших торгових майданчиках, в Україні продаж зброї через Інтернет менш активний, хоча війна в Україні породила велику кількість незаконної зброї.

Darknet також привабливий для здійснення терористичної та екстремістської діяльності.

По-перше, у Darknet терористичні групи можуть знайти практично будь-які необхідні рекомендації та покращені схеми для підвищення ефективності своєї діяльності, серед яких: легалізація незаконно зароблених доходів, шифровані канали зв'язку, найм виконавців, включаючи потенційних смертників для терористичних атак у реальному світі та кібератак.

По-друге, Darknet містить докладну інформацію про виготовлення вибухових речовин і зброї масового ураження, керівництва з вербування, тренування, психологічної обробки та формування мотивації у терористів.

По-третє, у Darknet спеціально створюються офіційні сайти для терористичних груп, які, не боячись переслідування, контактують і взаємодіють. Так, наприклад, діяла відома терористична організація Аль-Каїда. Невивчені кордони Даркнету дозволили "Аль-Каїді" адаптуватися до обмежень, накладених міжнародною системою, і діяти як віртуальна терористична мережа. [8]

Примітно, що спочатку концепція Darknet передбачала приватний месенджер, без ризику бути виявленими. На жаль, через деякий час він перетворився на ефективний засіб для скоєння кримінальних правопорушень.

Приватний месенджер Telegram має потенціал стати сучасною версією темної мережі.

Telegram — це найпопулярніший додаток для обміну миттєвими повідомленнями в деяких країнах Європи, Азії та Африки. За словами Павла Дурова, на початок 2023 року Telegram став другим після WhatsApp месенджером у світі за популярністю. [9] Станом на липень 2024 року Telegram налічує понад 950 мільйонів активних користувачів щомісяця, а найбільша кількість користувачів знаходиться в Індії. Сервери Telegram розміщені в кількох дата-центрах по всьому світу, а штаб-квартира знаходиться в Дубаї, Об'єднані Арабські Емірати.

Особливістю Telegram є наявність можливості створення “анонімних ботів” – спеціальних сторінок, які за своєю суттю є автоматизованим чорним ринком. Потенційному злочинцю навіть не потрібно контактувати та вести діалог онлайн із покупцем забороненого контенту, зброї чи наркотичних речовин. Починаючи від вибору товару із доступного каталогу, оплати товару та отримання товару зараз відбувається через анонімних ботів Telegram.

За словами Представника Головного управління розвідки Міноборони України Андрія Юсова: "Окрема історія – це анонімні Telegram-канали. Сьогодні дуже часто Telegram використовується, як певною мірою легалізований Darknet, в якому можна знайти все: від продажу наркотиків до груп ухилянтів, або якихось інших людей, які займаються чим-завгодно – аж до дитячої порнографії". [10]

У порівнянні із традиційною темною мережею, канали в Telegram зазвичай спеціалізуються на певному типі злочинної діяльності. Маркетплейс у темній мережі може запропонувати злочинцю можливість купити наркотики, зброю, номери кредитних карток, списки акаунтів (combolists) та десятки інших незаконних товарів. Канали в Telegram та анонімні боти, на відміну від цього,

функціонують як магазини, що спеціалізуються на одному виді товарів, і можуть бути класифіковані за тим, що вони пропонують.

Даркнет є одним з найбільш динамічних та мінливих середовищ в цифровому просторі. Ця прихована частина інтернету постійно еволюціонує, адаптуючись до нових технологій та викликів. В останні роки штучний інтелект (далі – ШІ) став ключовим фактором, що впливає на розвиток та функціонування темної мережі. «Темна мережа» - останнім часом переживає наплив зростаючої кількості чат-ботів зі ШІ– аналогів загальновідомого ChatGPT, але призначених для допомоги хакерам. Часом такі боти мають вельми промовисті назви «BadGPT» і «FraudGPT». [11]

Хакери використовують ШІ для розробки складних алгоритмів, які можуть обходити системи виявлення вторгнень та інші захисні механізми. ШІ може допомогти у створенні шкідливого програмного забезпечення, яке адаптується до середовища та уникає виявлення. На сьогоднішній день найбільшим успіхом зловмисників, які використовують хакерські ШІ-інструменти, є створення Morris II – комп'ютерного «хробака», тобто вірусу, здатного до самопоширення. Цей вірус здатен на основі запропонованих йому підказок самовідтворююватися. В цьому випадку зловмисники можуть вставляти такі підказки у вхідні дані, які під час обробки моделями генеративного ШІ спонукають модель відтворювати вхідні дані (реплікація) і брати участь у зловмисних діях (корисне навантаження). [11]

ШІ може бути використаний для аналізу соціальних мереж та інших відкритих джерел інформації, щоб створювати детальні профілі потенційних жертв. Ця інформація може бути використана для більш ефективних атак соціальної інженерії. Технології глибокого навчання дозволяють створювати реалістичні підробки голосу та відео (діпфейки). Це може бути використано для обману систем голосової автентифікації або для створення фальшивого компрометуючого контенту. Алекс Голден, засновник кіберрозвідувальної компанії Hold Security, розповів, що «любовні шахраї» вже починають теж використовувати ChatGPT, щоб створити переконливих підставних осіб. [12]

ШІ може бути інтегрований в існуючі системи правоохоронних органів для покращення ефективності їхньої роботи. ШІ може автоматизувати багато рутинних завдань, таких як збір даних, класифікація доказів, що дозволить слідчим зосередитися на більш складних аспектах розслідування. ШІ може автоматизувати обмін інформацією між різними правоохоронними органами, що дозволить швидше реагувати на транснаціональні злочини.

Прикладом позитивного застосування ШІ для протидії кримінальним правопорушенням у сфері комп'ютерних мереж є штучний інтелект DarkBERT. Вчені вже випробували новий ШІ в роботі. Вони підключили його до мережі Tor, яка використовується для доступу до dark web. Перші результати роботи свідчать про те, що DarkBERT набагато ефективніше справляється зі своїм завданням, ніж інші мовні моделі. У майбутньому з його допомогою можна буде «виявляти» неіндексовані сайти і перевіряти вміст форумів у dark web'і. [13]

Висновки. Розвиток інформаційно-комунікаційних технологій, від телеграфу до комп'ютера, заклав фундамент для створення глобальної мережі Інтернет. Темпи його розповсюдження значно перевершили початкові прогнози, досягнувши 5,16 мільярда користувачів у 2024 році, що становить 64,4% світового населення.

Структура сучасного інтернету поділяється на три основні рівні: поверхнева мережа (Clearnet), глибинна мережа (Deepnet) та темна мережа (Darknet). Особливу увагу привертає Darknet, який забезпечує високий рівень анонімності користувачів через використання спеціальних технологій, таких як Tor. Технології анонімізації, такі як Tor, створюють серйозні виклики для правоохоронних органів, роблячи традиційні методи відстеження та збору доказів малоефективними. Це піднімає важливі питання щодо балансу між захистом приватності та необхідністю боротьби зі злочинністю в кіберпросторі.

Зроблено висновок, що темна мережа (Darknet) є складним технологічним та соціальним феноменом, що має подвійну природу. З технологічного боку, це накладена мережа в Інтернеті, що забезпечує анонімність користувачів через шифрування, децентралізацію та спеціалізоване програмне забезпечення. З криміногенного боку, Darknet як частина кіберпростору виступає як місце та інструмент для здійснення протиправної діяльності, характеризуючись анонімними транзакціями, зашифрованими комунікаціями та прихованими сервісами.

Розвиток інформаційних технологій призвів до виникнення нового виду злочинності - кіберзлочинності, яка становить серйозну загрозу національній та міжнародній безпеці. Кіберзлочини характеризуються підвищеною прихованістю, трансграничним характером, високим рівнем технічної підготовки злочинців та складністю виявлення і розслідування.

Darknet та його сучасні аналоги, такі як певні функції месенджера Telegram, становлять серйозну загрозу для суспільства, надаючи платформу для різноманітної незаконної діяльності. Особливу небезпеку представляє легкість доступу до забороненого контенту, включаючи дитячу порнографію, наркотики, зброю та інші нелегальні товари і послуги. Особливо небезпечним є використання цієї мережі терористичними та екстремістськими групами для обміну інформацією, вербування, навчання та координації злочинних дій

Darknet являє собою багатогранну загрозу для суспільства та національної безпеки, надаючи платформу для широкого спектру незаконної діяльності.

Різноманітність незаконних послуг, доступних у Darknet, створює серйозні виклики для правоохоронних органів та законодавців. Анонімність мережі ускладнює виявлення та притягнення до відповідальності злочинців. Ця ситуація вимагає розробки нових підходів до боротьби з кіберзлочинністю, посилення міжнародного співробітництва та вдосконалення законодавства для ефективного протистояння загрозам, які виникають у цифровому просторі.

Динамічність темної мережі (Darknet) полягає в тому, що деякі месенджери, як ось всім відомий Telegram, через певну анонімізацію користувачів деградують до Darknet. Telegram надає можливості для анонімної

комунікації та створення автоматизованих маркетплейсів, які можуть бути використані злочинцями. Ця ситуація нагадує початкову концепцію Darknet, яка з часом перетворилася на середовище для незаконної діяльності. Telegram швидко став важливим осередком інтернет злочинності через свою простоту використання, сприйняття анонімності та нижчі ризики шахрайства. Оскільки правоохоронні органи продовжують посилювати контроль над Tor, ймовірно, що злочинці продовжуватимуть мігрувати на більш доступні платформи, такі як Telegram. Моніторинг цих каналів є вирішальним для випередження еволюціонуючих інтернет загроз.

Інтеграція штучного інтелекту (ШІ) в екосистему Даркнету також є проявом її динамічності. ШІ значно розширює можливості зловмисників, дозволяючи їм автоматизувати та оптимізувати свої атаки, створювати більш переконливі фішингові схеми, обходити системи безпеки та проводити масштабні операції з безпрецедентною ефективністю.

Поява спеціалізованих ШІ-ботів для хакерів, таких як "BadGPT" і "FraudGPT", свідчить про зростаючу динамічність кіберзлочинного світу. Особливо тривожним є розвиток самовідтворюваних вірусів на основі ШІ, як-от Morris II, що демонструє потенціал для створення більш адаптивних і стійких форм шкідливого програмного забезпечення.

Штучний інтелект може бути потужним інструментом у боротьбі зі злочинністю в Darknet, але його використання має супроводжуватися ретельним аналізом потенційних ризиків та розробкою відповідних заходів безпеки. Важливо розуміти, що ШІ не є панацеєю від усіх проблем, а лише одним з інструментів у комплексному підході до боротьби з кіберзлочинністю.

ЛІТЕРАТУРА

1. Визначення кіберпростору
2. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/cyberspace (Дата звернення: 14.04.2024).
3. The Size of the World Wide Web URL: WorldWideWebSize.com (Дата звернення: 20.05.2024).
4. Deep web vs. dark web: What’s the difference? URL: http://surl.li/khfequ (Дата звернення: 24.05.2024).
5. Даркнет URL: https://ru.wikipedia.org/wiki/Даркнет (Дата звернення: 24.05.2024).
6. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Головна - Офіс Генерального прокурора. URL: http://surl.li/lwspen (дата звернення: 30.05.2024).
7. Доповідь X Конгресу Організації Об’єднаних Націй по попередженню злочинності і поведінці із злочинцями // Десятий Конгрес ООН по попередженню злочинності і поведінці із злочинцями. URL: http://surl.li/trrfzk (дата звернення: 01.06.2024).
8. Буз С.І. Кіберзлочини: поняття, сутність та загальна характеристика // Юрист-Правознавець. 2019. № 4 (91). С. 78–82, с.81.

9. Yotam Rosner, Aviad Mendelbaum, Sean London, and Yoram Schweitzer Backdoor Plots: The Darknet as a Field for Terrorism URL: https://www.files.ethz.ch/isn/170411/INSSInsights464.pdf (дата звернення: 12.06.2024).
10. Дуров “Telegram став другим месенджером у світі після WhatsApp” URL: https://dev.ua/news/durov-telegram-stav-druhym-mesendzherom-u-sviti-pislia-whatsapp-1676803994 (дата звернення: 12.06.2024).
11. Використовується як легалізований Даркнет. У ГУР пояснили, чи заборонять Telegram в Україні та в чому його небезпека URL: http://surl.li/gikvqu (дата звернення: 13.06.2024).
12. Після ChatGPT в інтернеті наступає ера BadGPT. Як штучний інтелект допомагає хакерам. Інтернет Свобода. URL: http://surl.li/nxnlya (дата звернення: 19.10.2024).
13. Брюстер Т. Фейкові дівчата і викрадення особистих даних. Кіберзлочинці підхопили штучний інтелект ChatGPT для злочинів. Що у них виходить? – Forbes.ua. Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії. URL: http://surl.li/pgnhtu (дата звернення: 19.10.2024).
14. Штучний інтелект DarkBERT почне виявляти кібер-злочинців - NoWorries. NoWorries. URL: http://surl.li/nsupet (дата звернення: 19.10.2024).