МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Н.Ф. Ржевська
«___» _____ 2020 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

ЗА СПЕЦІАЛЬНІСТЮ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ «МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «Darknet як інструмент криміналізації політичного процесу: міжнародна та вітчизняна практика»

Виконавець: студент 2 курсу, 208 групи, Бурдін Петро Петрович

Керівник: доцент кафедри міжнародних відносин, інформації та регіональних студій Боротканич Наталія Петрівна

Нормоконтролер: _____ _____
(підпис) (П.І.Б.)

КИЇВ 2020

ЗМІСТ

ВСТУП

Даркнет - це накладання мереж, яке потребує спеціальних інструментів та програмного забезпечення для отримання доступу. Історія даркнета передує 1980-м, і спочатку цей термін використовувався для опису комп'ютерів на ARPANET, які були приховані та запрограмовані на отримання повідомлень, але які нічого не реагували та не визнавали, залишаючись, таким чином, невидимими або в темряві. З тих пір «даркнет» перетворився на загальний термін, який описує частини Інтернету, цілеспрямовано не відкриті для загального огляду або приховані мережі, архітектура яких накладається на Інтернет

Даркнет використовується майже так само широко і настільки ж різноманітно, як Інтернет: від електронної пошти та соціальних мереж до розміщення та обміну файлами, веб-сайтів новин та електронної комерції. Для доступу до нього потрібно спеціальне програмне забезпечення, конфігурації або авторизація, часто використовуючи нестандартні протоколи зв'язку та порти. В даний час два найпопулярніші способи доступу до даркнета це дві накладені мережі такі як Tor та I2P.

Браузер Tor живе на межі Інтернету і служить основною технологією темної мережі - колекція прихованих сайтів, недоступних через звичайний браузер і не індексованих пошуковими системами, такими як Google.

Правда про темну павутину полягає в тому, що окрім надзвичайної конфіденційності та захисту від нагляду авторитарних урядів, вона сприяє зростанню підпільного ринку, який досвідчені злочинці використовують для торгівлі наркотиками, викраденими особами та іншими незаконними продуктами та послугами.

Для людей, які живуть під гнітючими режимами, які блокують значну частину Інтернету або карають за політичні погляди, темна павутина - це рятівний круг, який забезпечує доступ до інформації та захист від переслідування. Крім того, він може просто забезпечити конфіденційність та

анонімність для тих, хто насторожено ставиться до того, як корпорації та уряди відстежують, використовують та потенційно монетизують свої дані.

Сьогодні багато організацій ведуть прихований веб-сайт на Tor, включаючи майже всі великі газети, Facebook і навіть Центральне розвідувальне управління США. Це тому, що веб-сайт Tor демонструє прихильність до конфіденційності. Наприклад, «Нью-Йорк Таймс» та «ЦРУ» сподіваються полегшити спілкування з людьми, які можуть надати конфіденційну інформацію. З іншого боку, та сама конфіденційність та анонімність, які забезпечують захист від тиранів та цільової реклами, також роблять темну павутину плацдармом для злочинів.

Поєднання темних веб-сервісів з криптовалютами призвело до очікувань буму злочинності. Десять років тому невідомий фахівець з криптографії який використовував псевдонім Сатоші Накамото, розробив першу у світі валютно-платіжну мережу, яка не контролюється національним урядом: біткойн. Спочатку біткойн став нішевим середовищем обміну для технологічного співтовариства у 2011 році валютою вибору для наркоторговців, які проводять операції на веб-сайті, відомій як Шовковий шлях. Протягом останніх п’яти років поєднання зашифрованої мережі, прихованої від більшості світу, та валюти транзакцій, яка майже не піддається контролю за правоохоронними органами, призвело до невеликого, але значного ринку незаконних продавців, які продавали нелегальні товари.

Незважаючи на те, що загальний економічний обсяг незаконної темної веб-діяльності залишається відносно невеликим, багато найбільш агресивних загроз для суспільства сьогодні діють у тіні мережі Tor і, отже, заслуговують на увагу міжнародних регуляторів, фінансових установ та правоохоронних органів.

Темна павутина використовувалася для боротьби з урядовою цензурою та допомоги політичним активістам у поширенні їхніх повідомлень.

Майбутнє темної павутини непевне. Оскільки уряди продовжують жорсткі дії на його використання, а незаконна діяльність відлякує нешкідливих користувачів, ми можемо побачити серйозні зрушення в темній мережі в найближчі роки.

Актуальність теми дослідження. Інтернет за останні два десятиліття став невід'ємним елементом людського життя і новим (зручним і оперативним) інструментом комунікації в суспільстві. Поза всяким сумнівом, в цифрову епоху значна частина економічної, політичної і культурного життя протікає саме в інтернеті. Даркнет виступає одним з рівнів інтернету.

Перший рівень інтернету включає в себе сукупність індексованих сайтів, користувачів яких можна визначити на основі IP адреси. Другий рівень - глибинний інтернет «Deep Internet» - являє собою набір неіндексованих сторінок інтернету, які не можуть бути знайдені по пошуковим системам, але користувачі яких можуть бути ідентифіковані. Відмітна риса даркнета полягає в тому, що його користувачі завдяки браузеру і системі шифрування зберігають свою анонімність і не можуть бути ідентифіковані. Виникнення даркнета пов'язують з першої інтернет-мережею APRANET в 1970-х рр., Коли інтернет був субкультурою, не мав масового поширення і служив інструментом спілкування вчених. У 2002 р термін Даркнет був використаний вперше в книзі співробітників Microsoft «Даркнет і майбутнє поширення інформації», в якій автори виступили за ідею свободи і конфіденційності в Інтернеті.

Така технологія збереження конфіденційності користувачів сама по собі нейтральна, але може використовуватися як на благо - для розвитку креативних форм спілкування, так і для суспільно небезпечних діянь - торгівля наркотичними засобами, тероризм,інформаційні злочини політичного характеру, продаж зброї, пошук вбивць за наймом, порушення прав на інтелектуальну власність, віртуальна валюта та ін.

Таким чином, актуальність теми дослідження обумовлюється наростанням кіберзлочинів політичного характеру в інтернет-просторі, що

мають не тільки міжнародно-політичні наслідки, формуючи регіональні конфлікти та фінансові кризи, а й навіть здатні вплинути на баланс сил між глобальними гравцями міжнародної арени

Метою виконання дипломної роботи є дослідження та розкриття сутності використання мережі Даркнет в міжнародно-політичних процессах

Завданнями роботи є:

- Розкрити процес становлення та історію винекнення мережі Darknet;
- Проаналізувати вплив мережі Darknet на міжнародні політичні процеси;
- Дослідити специфіку та особливості роботи мережі Darknet та TOR;
- Розглянути та порівняти правову базу України та США протидії кіберзлочиності.

Об'єктом дослідження є криміналізація міжнародно-політичних процесів, яка діє за допомогою використання сучасних інструментів інформації.

Предметом дослідження є мережа Даркнет та її інструменти інформаційного простору.

Методологія дослідження: Для досягнення поставленої мети та спішного вирішення завдань дипломної роботи було використано низку загальнонаукових методів дослідження. Методологічною основою дипломної роботи є теоретико-методологічний арсенал, зумовлений метою й предметом дослідження, що аналізується, – Мережа Даркнет .

Застосування методів і прийомів наукового пізнання спрямовується **системним підходом**, що дає можливість досліджувати історію винекнення та особливості мережі Darknet, аналізувати сучасний інтернет простір та способи подання інформації.

(підрозділи 1.1,1.2,1.3).

Логіко-семантичний метод сприяв поглибленню понятійного апарату (підрозділ 2.1).

Використання **статистичного методу** дослідження дозволило визначити тенденції розвитку Darknet на сучасному етапі та вплив інформаційних злочинів політичного характеру в мережі Darknet на світові політичні процеси.

(підрозділ 2.3,3.1,2.2).

За допомогою **порівняльного методу** було здійснено порівняльний аналіз правової бази протидії кіберзлочиності на прикладі України та США.

(підрозділ 3.2).

РОЗДІЛ 1. ІНТЕРНЕТ ЯК ДЖЕРЕЛО ТА ЗАСІБ ПОШИРЕННЯ МАСОВОЇ ІНФОРМАЦІЇ В XXI СТОРІЧЧІ

1.1 Історія виникнення та особливості мережі Darknet

Darknet - це накладена мережа інтернету, доступ до якої можна отримати лише за допомогою спеціалізованого програмного забезпечення, конфігурацій та спеціальних авторизацій, і часто використовує нестандартні протоколи зв'язку, щоб Інтернет навмисно був недоступним. Darknet стосується мереж, які не індексуються пошуковими системами, такими як Google, Yahoo або Bing. Це мережі, які доступні лише для вибраної групи людей, а не для широкої громадськості в Інтернеті, і доступні лише через авторизацію, певне програмне забезпечення та конфігурації. Це включає нешкідливі місця, такі як академічні бази даних та корпоративні сайти, а також ті, що мають більш темні теми, такі як чорні ринки, фетиш-спільноти, хакерство та піратство.[77]

Darknet - відрізняється від інших розподілених мереж P2P, оскільки обмін даними є анонімним, і тому користувачі можуть спілкуватися, не боячись урядового чи корпоративного втручання. З цієї причини Даркнет часто асоціюється з політичними комунікаціями дисидентів та незаконною діяльністю.[91] У більш загальному плані термін «даркнет» може бути використаний для опису всіх некомерційних веб-сайтів в Інтернеті або для позначення всіх «підпільних» веб-комунікацій та технологій, найчастіше пов'язаних з незаконною діяльністю або інша думка. [59]

Технічно даркнет це різновид віртуальної приватної мережі (VPN) з додатковими заходами, що забезпечують неможливість виявлення мережі та IP-адрес учасників. Мета полягає в тому, щоб приховати не тільки самі повідомлення, але і сам факт обміну інформацією. Учасники приєднуються з надією на можливість обмінюватися інформацією або файлами з невеликим ризиком виявлення.[2]

Даркнет може бути використаний для таких цілей, як:

- Забезпечення приватності та захист від політичних репресій;

- Злочини у сфері інформаційних технологій;
- Розповсюдження файлів, захищених авторськими правами;
- Тероризм;
- Кіберрозвідка.

Darknet і Dark Web часто використовуються як синоніми, що є неправильним. Ці два терміни відрізняються, оскільки darknet позначає мережу (наприклад, спільноту комп'ютерів), тоді як Dark Web - веб-сайти в darknet. Доступ до Dark Web можна отримати лише за допомогою протоколів darknet, таких як The Onion Router [88] Tor. Tor теж став майже синонімом Dark Web, але є й інші протоколи darknet, за допомогою яких ви можете отримати до нього доступ. Деякі альтернативи Tor - це Invisible Internet Project I2P, Freepto та Freenet.[22]

Freenet це підмережа в Інтернеті, яка використовується для публікації суперечливих та незаконних матеріалів. Включаючи веб-сторінки, форуми, сайти чату та функцію пошуку, це розподілена мережа, доступ до якої здійснюється через програмне забезпечення Freenet. Усі користувачі вносять частину своєї пропускної здатності та дискового простору, і насправді не знають про природу зашифрованих даних, які в будь-який момент знаходяться на їх дисках. Популярні темні мережі включають Tor, Freenet і I2P. Такі мережі зазвичай децентралізовані, і трафік маршрутизируется через широко розповсюджену систему серверів, які часто надаються добровольцями. Складна система маршрутизації ускладнює відстеження комунікацій.[38]

Freepto це ОС на базі Linux, яку можна завантажити за допомогою USB-диска на будь-якому комп'ютері. Дані, які ви зберігаєте на USB-диску, будуть механічно зашифровані. Він пропонує хактивістам простий спосіб спілкування без зусиль, як Tor. Це простий у використанні та найшвидший спосіб збереження зашифрованих даних.[39] Спеціальні темні мережі найчастіше використовуються для незаконного обміну файлами, що включає

захищені авторським правом носії, піратське програмне забезпечення, шкідливі програми.

Darknet використовуються при тестуванні мережевої безпеки. Адміністратор виділяє частину невикористаного простору IP-адрес для даркнета і налаштовує пристрій мережевого моніторингу для виявлення будь-якого трафіку, що направляється на IP-адресу в цьому діапазоні.

Оскільки в Darknet не працюють легітимні системи, будь-який трафік для адреси в ньому виходить від зловмисної або неправильно налаштованої системи. Темні мережі особливо корисні для виявлення систем, заражених вірусами або іншими шкідливими програмами, які намагаються поширитися в мережі.[2] Ідея анонімної мережі Інтернет-комунікацій, яка є стрижнем того, що є темною павутиною, сягає аж до 1960-х років із створенням ARPANET. Мережа Агентства перспективних дослідницьких проектів також відома як ARPANET, була експериментальною комп'ютерною мережею, створеною в 1960-х роках, яка була попередницею Інтернету, а згодом і темної Мережі. Ідея ARPANET виникла з бажання ділитися інформацією на великі відстані без необхідності телефонних зв'язків між кожним комп'ютером у мережі. ARPANET була комп'ютерною системою зв'язку, яка пізніше набула щупалеподібну структуру, що зробила можливим спілкування між пристроями. ARPANET починався як винахід для світу академічних кіл, військові, які мали справу з холодною війною в цей час, швидко знайшли для нього користь.[37]

Історія даркнета починається з 1969 року, коли Чарлі Клайн, студент Каліфорнійського університету в Лос-Анджелесі, друкує перше повідомлення і відправляє його між комп'ютерами, підключеними до ARPANET, інтернет-попереднику, розробленим Агентством перспективних дослідницьких проектів оборони Пентагону. Всього через кілька років поруч з ARPANET починає з'являтися ряд ізольованих секретних мереж. Деякі в кінцевому підсумку стали відомі як Даркнет. ARPANET в 1969 році не був побудований з урахуванням безпеки. Швидке зростання мережі зробив її

небезпечною. Згідно з технічними характеристиками інформації, що зберігається в цифровому вигляді, зловмисник може затримувати, порушувати, пошкоджувати, використовувати, знищувати, викрадати і змінювати цифрові дані. Залежно від цінності інформації такі дії матимуть різні наслідки з різним ступенем шкоди.

З появою сучасної мережі, яка, ймовірно, відзначена стандартизацією пакету протоколів Інтернету в 1982 році, проблема зберігання конфіденційних або незаконних даних стає все більш гострою. Ранні рішення включають фізичні "притулку даних" - Інформаційні аналоги податкових притулків-в Карибському басейні, які обіцяють розмістити все, від азартних ігор до незаконної порнографії.

У міру того, як Інтернет стає все більш популярним, зниження витрат на зберігання в поєднанні з досягненнями в області стиснення файлів викликало вибух активності даркнета, коли користувачі почали обмінюватися захищеними авторським правом матеріалами. Незабаром в тимчасовій передачі даних через Інтернет народжуються децентралізовані концентратори даних, деякі з яких, наприклад, так звані топ-сайти, на яких відбувається більшість нелегальних музичних і кіно-файлів, захищені паролем і відомі тільки інсайдерам. Інші, такі як Napster, працюють відкрито і забезпечують мільйони передач файлів в день.

У березні 2000 року, розробник програмного забезпечення Ян Кларк, випускає Freenet, революційне програмне забезпечення, яке пропонує анонімний прохід в мережі Даркнет, де можна отримати доступ до заборонених матеріалів: від дитячої порнографії до інструкцій про те, як створити вибухові речовини.[38]

У вересні 2002 року, дослідники з Військово-морської дослідницької лабораторії США випускають ранню версію Tor («Цибулевий маршрутизатор»), яка приховує місце розташування і IP-адреса користувачів, що завантажують програмне забезпечення. Спочатку розроблений для захисту особистості американських бойовиків і дисидентів в репресивних

країнах, таких як Китай, Tor також має ще один природний електорат: мешканці даркнета.[6]

У 2010 році кількість екстремістських сайтів в даркнета досягло 50 000, а терористичних форумів - понад 300. Незаконний продаж піратського цифрового контенту служить джерелом фінансування терористичних операцій. До цього дня Даркнет є відкритим питанням для великої кількості держав, так як злочинці використовують найголовнішу ідею даркнета - анонімність. Щоб розуміти загальну картину актуального стану даркнета, необхідно розібратися і проаналізувати інтерпретацію даного терміну.

Даркнет, темна мережу (англ. Darknet) - це загальний термін, що описує частини Інтернету, умисно не відкриті для публічного перегляду або прихованих мереж, архітектура яких накладена на архітектуру Інтернету. Термін спочатку описував комп'ютери в ARPANET, які були приховані, запрограмовані для отримання повідомлень, але не реагували на і не підтверджували що-небудь, таким чином залишаючись невидимими для загальної мережі.[2]

До того, як була винайдена криптовалюта, нелегальні транзакції в темній павутині було важко здійснити, оскільки клієнти потенційно могли знаходитись за тисячі миль від них, і жодна зі сторін не хотіла ризикувати використанням кредитних карток або PayPal для транзакцій, оскільки вони залишають паперові сліди.[85] Криптовалюта, форма цифрової валюти, яка сприяє анонімному здійсненню транзакцій, стала відповіддю на цю постійну проблему. Хоча різні форми криптовалют розроблялися з 1990-х років, жодна з них не набула такої популярності та масового використання як Bitcoin винайдений у 2009 році. Сатоші Накамото "видобув" перший біткойн, фактично започаткувавши революцію в незаконних транзакціях в Інтернеті. Біткойн вирішив проблему, яку попередні версії криптовалюти не могли - у неї була спеціальна цифрова бухгалтерська книга, яка заважала користувачам копіювати гроші. З вирішенням проблеми анонімних транзакцій зросли нелегальні продажі в темній мережі.[41]

Випуск браузера Tor зробив його більш доступним як для користувачів, так і для активістів, яким він потрібен був у цей час. Tor не тільки захищав особисті дані людей в Інтернеті, але й дозволяв їм отримувати доступ до важливих ресурсів, соціальних мереж та заблокованих веб-сайтів. В даний час Інтернет домінує у всіх аспектах нашого повсякденного, звичного життя. Важливо пам'ятати, що він існує лише кілька десятиліть. Хоча це відносно короткий проміжок часу в порівнянні з ходом людської історії, інтернет є надзвичайно великим простором, що складається з мільярдів окремих сайтів, які пов'язані один з одним в складній комбінації. Існує величезна кількість відомих сайтів в усьому світі, однак за їх межами ховається величезна кіберзлочинністю межа - за деякими оцінками, в сотні разів перевищує Всесвітню павутину.

Даркнет зараз - це це оверлейная мережу будь-якого типу, для доступу до якої потрібна певна авторизація або інструменти. Причини роботи в даркнета зазвичай пов'язані з різними функціями. Вони можуть бути використані для здійснення ряду злочинів, включаючи незаконний обмін файлами, чорні ринки, а також як засіб обміну нелегальними товарами або послугами. Це часто найпопулярніші види використання темної мережі. Але вони також використовуються для безлічі інших причин.

Темні мережі часто називають засобом захисту політичних дисидентів від репресій або засобом, що дозволяє людям обходити мережі цензури. Вони можуть сприяти інформуванню про порушення і витоку новин, а також допомагають захистити людей від стеження. Як такі, і через безліч додатків темної мережі, вони є гаряче оспорюваної проблемою

Крім незаконних покупок і продажів, існують інші, легальні причини, за якими можна зацікавитися використанням темної мережі. Люди в закритих суспільствах, що зіштовхуються з крайньої цензурою, можуть використовувати темну мережу для спілкування з іншими людьми за межами своєї громади. Навіть люди в відкритих суспільствах можуть бути зацікавлені у використанні темної мережі, особливо в зв'язку з тим, що

стурбованість з приводу відстеження дій уряду і збору даних продовжує зростати в усьому світі.

Проте, велика частина діяльності, яка відбувається в темній мережі, є незаконною. Неважко здогадатися, чому це може мати місце: темна мережа пропонує такий рівень захисту ідентичності, якого немає на поверхні. Злочинці, які прагнуть захистити свою особистість, щоб уникнути виявлення і захоплення, залучені до цього аспекту темної мережі.

Інша мета darknet - надати місце для приватного спілкування, коли публічне спілкування небажано, небезпечно або заборонено. Наприклад, коли режим Мубарака в Єгипті відключив Інтернет в цій країні, політичні дисиденти використовували даркнет Tor для підтримки зв'язку з рештою світу.

1.2 Сучасний Інтернет-простір: характерні особливості

Сучасна епоха характеризується як епоха глобального інформаційного суспільства, зміст якої становить експоненціальне зростання інформаційних технологій і глобалізація інформаційних процесів. Одним з головних проявів цих процесів є виникнення глобальної мережі Інтернет, стрімке і неухильне розширення її використання у всіх сферах життя суспільства.

Інтернет, який ми використовуємо сьогодні - тобто мережа комп’ютерних мереж, що базуються на наборі протоколів Протоколу управління передачею (TCP) / Інтернет-протоколу (IP) (Postel 1981) - на сьогодні відносно стара технологія. [74] Дослідження його проекту почалися в 1973 р., А мережа запрацювала в січні 1983 р. Протягом перших двох десятиліть свого існування вона була заповідником технологічної, академічної та дослідницької еліти. З початку 1990-х років він почав проникати в основне суспільство і зараз широко розглядається як технологія загального призначення GPT, без якої сучасне суспільство не може функціонувати. Тож за відносно короткий період технологія перетворилася з

чогось, що вважається екзотичним, на очевидно буденну комунальну послугу, на зразок мережевої електрики.[12]

Інтернет зробив революцію у світі комп'ютерів та комунікацій. Винахід телеграфа, телефону, радіо та комп'ютера створив основу для цієї безпрецедентної інтеграції можливостей. Інтернет - це одночасно всесвітня можливість мовлення, механізм розповсюдження інформації та засіб співпраці та взаємодії між людьми та їхніми комп'ютерами, не враховуючи географічного розташування. [93] Інтернет є одним із найуспішніших прикладів переваг стійких інвестицій та прихильності до досліджень та розвитку інформаційної інфраструктури. Починаючи з перших досліджень комутації пакетів, уряд, промисловість та наукові кола стали партнерами у розробці та впровадженні цієї захоплюючої нової технології.[3]

Сьогодні Інтернет є широко розповсюдженою інформаційною інфраструктурою, початковим прототипом того, що часто називають Національною «Глобальною або Галактичною» Інформаційною Інфраструктурою. Його історія складна і включає багато аспектів - технологічний, організаційний та спільний. І його вплив сягає не лише технічних областей комп'ютерних комунікацій, але й усього суспільства, коли ми рухаємось до все більшого використання Інтернет-інструментів для здійснення електронної комерції, збору інформації та діяльності громад.

Сам Інтернет трансформувався. У перші дні - з історичного погляду все ще відносно недавно - це була статична мережа, призначена для передачі невеликої кількості байтів або короткого повідомлення між двома терміналами; це було сховище інформації, де вміст публікували та підтримували лише спеціалісти-кодери. У 1980-х і 1990-х роках Інтернет розширився, охопивши IT-можливості університетів та дослідницьких центрів, а згодом і державних установ та приватних підприємств з усього світу. Інтернет зазнав величезного зростання; це вже не був підконтрольний державі проект, а найбільша комп'ютерна мережа у світі, що включала понад 50 000 підмереж, 4 мільйони систем та 70 мільйонів користувачів.[4]

Поява веб 2.0 у першому десятилітті XXI століття саме по собі стало революцією в короткій історії Інтернету, сприяючи зростанню соціальних медіа та інших інтерактивних інструментів комунікації на основі натовпу.

Інтернет більше не займався лише обміном інформацією: це був складний мультидисциплінарний інструмент, що дозволяє людям створювати вміст та спілкуватися між собою. Сьогодні ми можемо надсилати дані з одного кінця світу на інший за лічені секунди, робити онлайн-презентації, жити в паралельних «ігрових світах» і використовувати картинки, відео, звук та текст, щоб ділитися своїм реальним життям. Особисті історії виходять на публіку; місцеві проблеми стають глобальними.

Підйом Інтернету спричинив дискусію про те, як спілкування в Інтернеті впливає на соціальні відносини. Інтернет звільняє нас від географічних пут і об’єднує в тематичні спільноти, які не прив’язані до якогось конкретного місця. Наше - це мережеве, глобалізоване суспільство, пов’язане новими технологіями.[4]

Інтернет - це інструмент, який ми використовуємо для взаємодії один з одним, і відповідно ставить нові виклики конфіденційності та безпеці.

Зміни в соціальній комунікації мають особливе значення. Хоча аналогові інструменти все ще мають своє місце в деяких секторах, нові технології продовжують завойовуватись щодня, трансформуючи наші комунікаційні практики та можливості - особливо серед молодих людей. Інтернет усунув усі комунікативні бар’єри. В Інтернеті звичайні обмеження простору та часу зникають, і існує запаморочливо широкий діапазон комунікативних можливостей. Вплив додатків у соціальних мережах викликав дискусію про «нову комунікаційну демократію».

Розвиток Інтернету сьогодні формується переважно за допомогою миттєвого мобільного зв'язку. Мобільний Інтернет - це нова революція за допомоги якого підключення до Інтернету на смартфоні чи планшеті веде до дедалі мобільнішої реальності: ми не прив'язані до жодного конкретного пристрою, і все знаходиться в хмарі.[4]

У 1995 році, за оцінками, 16 мільйонів людей у всьому світі мали доступ до Інтернету. Поточна кількість користувачів, за оцінками, становить близько 3,5 мільярдів. У 1995 році всі користувачі отримали доступ до мережі через фіксовані зв'язки; в даний час більше половини всіх користувачів отримують до нього доступ через мобільні пристрої. І більшість програм, які користуються популярністю серед сучасних користувачів, не існували - і справді не були б здійсненними - в мережі, як це було в 1995 році. Чудовим в Інтернеті є те, що, хоча його інфраструктура повинна була докорінно розвиватися протягом цих двох десятиліть, щоб задовольнити постійно мінливі вимоги своїх користувачів, він все ще залишається вірним своїм основним архітектурним принципам.[12]

Оскільки Інтернет, в принципі, дозволяє кожному, хто має мережевий зв'язок, стати глобальним видавцем, він спочатку розглядався як кардинально інший вид засобів масової інформації, що домінував у друкованому та ефірному світі.

Тоді як ті попередні засоби масової інформації були системами «мало-до-багатьох» , Інтернет може бути засобом «багато-до-багатьох» ; його користувачі можуть бути активними творцями вмісту, а не пасивними споживачами вмісту, створеного іншими. Але оскільки мережа еволюціонувала, щоб об'єднати мільярди користувачів, це раннє бачення її потенціалу як засобу комунікації пом'якшилось досвідом. Аналіз трафіку даних у мережі свідчить про те, що пасивне споживання, що характеризує ефірну епоху, повертається. Наприклад, на наземні стаціонарні зв'язки в Північній Америці Netflix - послуга потокової передачі фільмів - займає 36,5% трафіку в нижній частині потоку в пікові вечірні години . Мережа все ще пропонує великі творчі можливості для своїх користувачів, але шанси на її перетворення на „мільярдне телебачення" можуть скорочуватися.

Одним із визначальних явищ сучасності, що змінює світ таким, яким ми його знаємо, є доступність Інтернету у всьому світі. Однією з особливостей сучасного інтернет простору є є соціальні медіа, які існують у

багатьох формах, включаючи блоги, форуми, ділові мережі, платформи обміну фотографіями, соціальні ігри, мікроблоги, чат-програми та не в останню чергу соціальні мережі. У 2020 році рівень глобального соціального проникнення досяг 49 відсотків, причому Східна Азія та Північна Америка мали найвищий рівень проникнення відповідно 71 та 69 відсотків, а потім Північна Європа - 67 відсотків.[49]

Facebook із 2,3 мільярдами користувачів сьогодні є найпопулярнішою платформою соціальних мереж за ним слідують YouTube, Instagram та WeChat, у яких понад мільярд користувачів. Наступними є Tumblr і TikTok, у яких понад півмільярда користувачів.

Характерною особливістю сучасного інтернет простіру є кібер злочиність. Кіберзлочинність це злочинна діяльність, яка спрямована або використовує комп'ютер, комп'ютерну мережу або мережевий пристрій. Більшість, але не всі, кіберзлочинності здійснюють кіберзлочинці або хакери, які хочуть заробити гроші. Кіберзлочинність здійснюється приватними особами або організаціями. Деякі кіберзлочинці організовані, використовують передові технології та мають високу технічну кваліфікацію. Рідко кіберзлочинність має на меті пошкодити комп'ютери з інших причин, крім прибутку. Вони можуть бути політичними чи особистими.[13]

Види кіберзлочинності:

- Шахрайство з електронною поштою та Інтернетом;
- Шахрайство з особистими даними (де викрадається та використовується особиста інформація);
- Викрадення даних про фінансові або карткові платежі;
- Викрадення та продаж корпоративних даних;
- Кіберектор (вимагання грошей для запобігання нападу, що загрожує);
- Вимагальні програми (тип кіберектори);

- Криптоджекінг (хакери видобувають криптовалюту, використовуючи ресурси, якими вони не володіють);
- Кібершпіонаж (де хакери отримують доступ до даних уряду або компанії);
- Кібертерроризм.

Більшість кіберзлочинів підпадає під дві основні категорії:

- Злочинна діяльність, яка націлена;
- Злочинна діяльність, яка використовує комп’ютери для вчинення інших злочинів.

Кіберзлочинність, орієнтована на комп’ютери, часто включає віруси та інші типи шкідливих програм. Кіберзлочинці можуть заражати комп’ютери вірусами та шкідливим програмним забезпеченням, щоб пошкодити пристрої або зупинити їх роботу. Вони також можуть використовувати шкідливе програмне забезпечення для видалення або викрадення даних.[13]

В сучасний час інформаційні технології входять в усі сфери людської діяльності. Інтернет дозволяє людям знаходити інформацію будь-якого виду, бути на зв'язку з усім світом і користуватися різними ресурсами.

Стрімкий розвиток Інтернету та інформаційних технологій призвело до появи нових видів злочинів. В наші дні користувачі все більше і більше замислюються над комп'ютерною безпекою. Загроза в мережі в основному виникає від людини або організованою групи людей, чиї дії в мережі спрямовані на злом і розкрадання даних користувачів, підприємств та шкільних установ.

Термін хакер позначає комп'ютерного професіонала високого рівня, людина яка розуміє основи роботи комп'ютерних систем. Хакером так само називають фахівця, який незвичайним способом вирішує комп'ютерні проблеми. Це свого роду комп'ютерний геній, який творчо підходить до вирішення комп'ютерних задач, виправляє помилки в програмах

нестандартним чином. На западесуществует відмінність між терміном хакер як комп'ютерного професіонала, не залученого в протиправну діяльність, і крекерів - хакера, що застосовує свої знання і навички для злому комп'ютерних систем.

Хакерів можна віднести до різних категорій, до таких як:

1. «білі» хакери (whitehat) звичайні програмісти, системні адміністратори забезпечують нормальне функціонування і безпеку комп'ютерів;

2. «чорні» хакери (blackhat) власне займаються зломом баз даних, інформаційних мереж, завдають шкоди в роботі системи;

3. «скриптер» - звичайні користувачі готових скриптів, і часто навіть не уявляють, як вони працюють.

Комп'ютерне хакерство - це злом програмного забезпечення комп'ютерів найчастіше з метою вилучення або зараження вірусом комп'ютерної системи, з метою розкрадання секретної інформації, нанесення шкоди в роботі системи і т.д[93]

1.3 Інтернет-інформація як джерело формування політичних поглядів суспільства

Інформаційні технології, зокрема Інтернет, широко впроваджуються в усі сфери життєдіяльності сучасного суспільства. Інтернет сприяє розвитку зв'язків і комунікацій між політичними партіями і суспільством, ведення політичної дискусії і політичної боротьби

У наш час інформаційна технологія проникає в усі сфери людської життєдіяльності, в тому числі і в політику.[58] Політичну діяльність умовно можна розділити на державно-політичну і суспільно-політичну. Що стосується сфери державної діяльності, то інформаційна техніка все ширше використовуються, з одного боку, для інформації громадян про проведені державних заходах, з іншого - з метою збору інформації про діяльність і інтересах громадян.

Суспільно-політична сфера - це функціонування політичних партій і громадських організацій, в яких громадяни проявляють свою громадянську активність. У цій сфері політичного життя суспільства особливу роль відіграє система Інтернет. Повсюдна доступність Інтернет в поєднанні з потужними обчислювальними і комунікаційними засобами (ПКблокноти, двонаправлені пейджери, персональні цифрові секретарі, стільникові телефони і т.п.) дозволяє широко використовувати Інтернет в суспільно-політичній діяльності.[16]

Інтернет є вирішальною технологією Інформаційної ери, оскільки електричний двигун був вектором технологічної трансформації Індустріальної ери. Ця глобальна мережа комп'ютерних мереж, в основному заснована сьогодні на платформах бездротового зв'язку, забезпечує повсюдну потужність мультимодального, інтерактивного спілкування у вибраний час, що перевищує простір. Інтернет насправді не є новою технологією: його предок, Arpanet, був вперше застосований у 1969 році (Abbate 1999). Але саме в 1990-х роках, коли він був приватизований і звільнений з-під контролю Міністерства торгівлі США, він розповсюдився по всьому світу з надзвичайною швидкістю: у 1996 році перше опитування користувачів Інтернету нарахувало близько 40 мільйонів; у 2013 р. вони перевищують 2,5 млрд., причому на Китай припадає найбільша кількість користувачів Інтернету. Крім того, деякий час розповсюдження Інтернету було обмежене складнощами щодо створення наземної телекомунікаційної інфраструктури в країнах, що розвиваються. Це змінилося з вибухом бездротового зв'язку на початку двадцять першого століття. Дійсно, у 1991 р. У світі було близько 16 млн. Абонентів бездротових пристроїв, у 2013 р. - близько 7 млрд. (На планеті 7,7 млрд. Людей). Розраховуючи на сімейне та сільське використання мобільних телефонів та беручи до уваги обмежене використання цих пристроїв серед дітей віком до п'яти років, ми можемо сказати, що людство зараз майже повністю пов'язане, хоча і з великим рівнем нерівності в пропускній здатності, оскільки а також в ефективності та ціні послуги.

В основі цих мереж зв'язку Інтернет забезпечує виробництво, розповсюдження та використання оцифрованої інформації у всіх форматах. Швидкість та масштаби трансформації нашого середовища спілкування за допомогою Інтернету та бездротового зв'язку спричинили всілякі утопічні та дистопічні сприйняття у всьому світі.[17]

Наповнення Інтернету політичною інформацією практично не піддається контролю, що надає можливість реалізації свободи слова, але, разом з тим, дозволяє поширювати непідтверджену, неточну інформацію, а іноді і просто компромат. Важливо також врахувати, що джерела Інтернету надають можливість скрупульозно відстежувати тему, що представляє інтерес для користувача, швидко дізнаватися про зміни і можливості реагування за допомогою розміщення необхідної інформації або висловлювання власної думки, якщо тема обговорюється на форумі або конференції. Нарешті, можливість отримання самої різної інформації сприяє задоволенню запитів будь-якій аудиторії, а багато індивіди просто не можуть обходитися без використання Інтернету при виконанні своїх професійних обов'язків (наприклад, фінансова діяльність, наукова і т.д.)

Очікується, що Інтернет матиме значний вплив на багато аспектів нашого життя в майбутньому. Засоби, пропоновані Інтернет-технологіями, вже дають можливість людям у всьому світі отримати доступ до величезної кількості інформації майже з будь-якої мислимої теми, знайти інших, що мають подібні інтереси, обговорити відповідні питання, а також зробити інформацію доступною для інших людей за мінімальні витрати. Це революціонізує способи, яким люди навчаються, здійснюють покупки, займаються дозвіллям, не відстають від поточних справ, ведуть бізнес та підтримують почуття спільності. Подібним чином Інтернет може також мати зростаючий, але непередбачуваний вплив на спосіб, яким політичні організації та особи передають свої повідомлення громадянам, і може глибоко змінити спосіб участі громадян у політичному процесі.[11]

Цифрові медіа стали невід'ємною частиною політичного життя окремих громадян, оскільки все більше людей у всьому світі використовують цифрові медіа-технології для інформації та комунікації. У сукупності цифрові медіа також становлять важливу платформу, яку люди можуть використовувати для координації та мобілізації серед однодумців. Тим не менше, поширюючи інформативні та мобілізуючі повідомлення, цифрові засоби масової інформації також сприяють соціально-політичним чинникам, які викликають занепокоєння щодо поширення дезінформації, інформаційних розбіжностей та політичної поляризації. [12]

На сучасному этапі розвитку інтернет простору, розвитку цифрових видань та подання інформації в електроному форматі інтернет користувачам фейкові новини мають великий вплив на свідомість громодян. Зростаюча кількість людей використовує Інтернет, щоб бути в курсі події та обмінюватися мільйонами публікацій, статей та відео на таких платформах, як Facebook, Twitter і YouTube. Швидке прийняття соціальних медіа призвело до зростання обміну інформацією серед користувачів, а фальшиві новини стали складовою наших цифрових щоденних процедур. Поширення дезінформації частково пояснюється тим, що соціальні мережі не підтверджують справжність новин . Це дозволяє легко ділитися, здавалося б, реальними зображеннями та відео, якими вміло маніпулювали. Дезінформація має значний вплив на громадську думку та дискурс.[14]

Термін фейкові новини вислизає від звітів, зображень та відеозаписів, які спільно використовуються для цілеспрямованого поширення дезінформації, тобто інформації, яка фактично є неправильною . Спочатку ці новини можуть виглядати автентичними та намагатись привернути увагу, шокувати чи сформувати думки. Фейкові новини можуть створювати особи чи групи, які діють у своїх інтересах або інтересах третіх сторін. Створення дезінформації зазвичай мотивується особистими**,** політичними чи економічними програмами .[84]

Поширення сфабрикованих новин для формування громадської думки щодо певних тем - явище недавнього часу. Сенсаційні заголовки або політичні статті, що використовуються для поширення брехні та пропаганди, існують з часу появи друкованих ЗМІ. За часів обміну цифровою інформацією фальшиві новини стали більше мережевим явищем, яке важко контролювати. Фейкові новини можуть досягти високого рівня видимості за короткий проміжок часу, оскільки ними легко ділитися через соціальні мережі та соціальні боти.[14]

Інтернет інформація може мати важливий вплив на громадську думку кількома способами:

- Встановлення порядку денного новин, що формує погляд громадськості на те, що є гідними новин та важливим;
- Обрамлення деталей історії;
- Повідомлення соціальної бажаності певних видів ідей.

Формування громадської думки починається з встановлення порядку денного провідними ЗМІ у всьому світі. Цей порядок денний диктує, що заслуговує на новини, а також як і коли про це буде повідомлено. Порядок денний ЗМІ визначається різноманітними факторами навколишнього середовища та роботи з новинами, що визначає, які історії будуть гідними новин.

Ще однією ключовою складовою формування громадської думки є обрамлення. Фреймінг - це коли історія чи новина змальовується певним чином і має на меті змінити ставлення споживачів так чи інакше. Більшість політичних питань важко розроблені для того, щоб переконати виборців проголосувати за конкретного кандидата. Наприклад, якби кандидат Х одного разу проголосував за законопроект, який підвищував податки на прибуток середнього класу, у заголовку, що міститься в рамці, було б написано "Кандидат Х не дбає про середній клас". Це ставить кандидата Х у негативний фрейм для читача новин.[46]

Соціальна бажаність - ще одна ключова складова формування громадської думки. Соціальна бажаність - це думка, що люди загалом формують свої думки на основі того, що, на їхню думку, є популярною. На основі встановлення порядку денного ЗМІ та обрамлення ЗМІ, найчастіше певна думка повторюється в різних засобах масової інформації та на сайтах соціальних мереж, поки не створюється хибне бачення, де сприймана істина насправді дуже далека від фактичної істини.[45]

На громадську думку можуть впливати зв'язки з громадськістю та політичні ЗМІ. Крім того, засоби масової інформації застосовують широкий спектр рекламних методів, щоб висвітлити свої повідомлення та змінити думку людей. З 1950-х років телебачення було основним засобом формування громадської думки, хоча Інтернет стає все більш важливим у цій сфері. Зростання висвітлення скандалів, а також сенсаційне висвітлення засобів масової інформації, спричинене прибутком, призвело до того, що населення отримує більш негативних та недовірливих поглядів на владу, ніж попередні покоління.[48]

Лідер громадських думок - це активний користувач ЗМІ, який інтерпретує значення медіа-повідомлень для менш обізнаних про політичні події. Лідерство думок - це концепція, що випливає з теорії двоступеневого потоку комунікацій, висунутої Полом Лазарсфельдом та Еліху Кацом. Значними розробниками цієї теорії були Роберт К. Мертон, К. Райт Міллс та Бернард Берельсон. Ця теорія є однією з декількох моделей, які намагаються пояснити поширення інновацій, ідей або комерційних продуктів.

Лідер думок - це агент, який є активним медіа-користувачем і який інтерпретує значення медіа-повідомлень або контенту для медіа-користувачів нижчого класу. Зазвичай лідер думок високо поважається тими, хто приймає його думки. Мертон розрізняє два типи лідерської думки: мономорфну та поліморфну. Як правило, лідерство думок розглядається як мономорфна міра індивідуальних відмінностей, що залежить від сфери діяльності, тобто людина, яка є лідером думок в одній галузі, може бути послідовником в

іншій галузі. Прикладом мономорфного лідера думок у галузі комп'ютерних технологій може бути технік із сусідніх комп'ютерних служб. Технік має доступ до набагато більше інформації на цю тему, ніж пересічний споживач, і має необхідний досвід, щоб зрозуміти інформацію, хоча одна і та ж людина може бути послідовником в іншій галузі (наприклад, спорту) і просити інших радитись. На відміну від них, поліморфні лідери думок здатні впливати на інших у широкому діапазоні доменів. Варіанти поліморфного лідерства думок включають ринковий мавенізм, силу особистості та узагальнене лідерство думок.[75]

Лідери громадської думки - це особи, які отримують більше висвітлення у ЗМІ, ніж інші, і мають особливу освіту з певного питання. Вони прагнуть прийняти інших, і їх особливо спонукає підвищити свій соціальний статус.[47]

РОЗДІЛ 2. DARKNET ЯК КРИМІНАЛЬНИЙ ЦИФРОВИЙ ПРОСТІР МЕРЕЖІ ІНТЕРНЕТ

2.1 Програмне забезпечення та інструменти Darknet

Оригінальна пропозиція анонімності та відсутність належності до реальної організації темної павутини робить її вигідним місцем для діяльності, яка в іншому випадку перешкоджатиме державному контролю.

Існування цифрового простору, який охоплює вищезазначені функції, людей та технології, може припустити, що темна павутина є не просто технологічним продуктом, а явищем, що виникає внаслідок потреби в секретності та анонімності між членами спільноти, подібно до чорного ринку фізичного світу, який існує через потребу в нерегульованому обміні товарами та послугами між фізичними особами.[97] До програмного забезпечення та інстументів darknet можно віднести:

Браузер TOR (onion routing) - це веб-браузер, призначений для анонімного веб-серфінгу та захисту від аналізу трафіку. Незважаючи на те, що Tor часто асоціюється з даркнетом та злочинною діяльністю, браузер із законних причин часто використовується представниками правоохоронних органів, репортерами, активістами, викривачами та звичайними особами, які переймаються за безпеку в інтернеті. Спочатку TOR був розроблений ВМС США для захисту вразливих комунікацій уряду США. Хоча Tor і надалі використовується урядом, зараз він є багатоплатформеним браузером із відкритим кодом, який доступний для загального користування. Браузер використовує вихідні ретранслятори та зашифровані тунелі, щоб приховати користувальницький трафік усередині мережі, але залишає кінцеві точки легшими для спостереження і не робить ефекту поза межами мережі.[5]

Мережа TOR - один із багатьох прикладів нових технологій, які намагаються заповнити порожнечу конфіденційності даних у цифровому просторі, що страждає від проблем кібербезпеки. Його функція з відкритим кодом означає, що його вихідний код доступний будь-якому користувачеві для оновлення або вдосконалення.[6] Однак за допомогою Tor мережа Tor

перехоплює трафік з вашого браузера і відхиляє запит користувача від випадкової кількості IP-адресу інших користувачів (комп'ютерів), перш ніж передавати запит користувача в кінцевий пункт призначення. Мережа надсилає інформацію на IP-адресу користувача A, яка зашифровує інформацію та передає її на адресу користувача B, який виконує інше шифрування та передає її на адресу користувача C, яка є останньою адресою, відомою як вузол виходу. Цей останній вузол розшифровує зашифровані дані і, нарешті, передає запит до кінцевого пункту призначення. Ця остання адреса вважає, що запит надійшов із вихідного вузла, і надає доступ до нього. Процес шифрування на кількох комп'ютерах повторюється від вихідного вузла до початкового користувача.[6] Мережа Tor заважає IP-адресам користувачів від небажаного спостереження, зберігаючи запити користувачів, зв'язок, транзакції та ідентифікаційні дані, які не підлягають відстеженню та є приватними, але не обов'язково захищеними.

Bitmessage - це протокол зв'язку P2P, який використовується для надсилання зашифрованих повідомлень іншій особі або багатьом передплатникам. Він децентралізований і недовірливий, що означає, що вам не потрібно - по суті довіряти будь-яким особистостям, таким як органи кореневих сертифікатів. Він використовує надійну аутентифікацію, що означає, що відправник повідомлення не може бути підроблений, і він має на меті приховати дані, що не містять вмісту, такі як відправник та одержувач повідомлень, від пасивних підслуховувачів, таких як ті, хто запускає беззаконні програми прослуховування. [7]

VPN - Віртуальна приватна мережа дає конфіденційність і анонімність шляху створення приватної мережі з підключення до Інтернету в громадському місцях. VPN маскують вашу адресу інтернет-протоколу (IP), тому ваші дії в Інтернеті практично неможливо простежити. Найголовніше, що служби VPN встановлюють безпечні та зашифровані з'єднання, щоб забезпечити більшу конфіденційність, ніж навіть захищена точка доступу Wi-Fi. Серфінг в Інтернеті або здійснення транзакцій у незахищеній мережі

Wi-Fi означає, що ви можете розкрити свою приватну інформацію та звички перегляду. Ось чому віртуальна приватна мережа, більш відома як VPN, повинна бути обов'язковою для всіх, кого турбує їхня безпека та конфіденційність в Інтернеті. Шифрування та анонімність, які надає VPN, допомагають захистити ваші дії в Інтернеті: надсилання електронних листів, покупки в Інтернеті або оплата рахунків. VPN також допомагають залишати анонімним веб-перегляд.[15]

VPS - це сервер, створений за допомогою програмної віртуалізації . Він функціонує як фізичний сервер, але це віртуалізований екземпляр, створений на сервері. На одній фізичній машині може розміщуватися кілька віртуальних приватних серверів. А хмарні VPS можуть бути розміщені на кілька серверів. Управління як VS-системами на одній машині, так і в хмарі здійснюється за допомогою програмного забезпечення, що називається гіпервізор. Машина, яка запускає гіпервізор, називається хост- машиною, а окремі віртуальні приватні сервери - гостьовими машинами або гостьовими екземплярами. Гіпервізор може запускати та зупиняти віртуальні машини та розподіляє системні ресурси , такі як ЦП , пам'ять та пам'ять на диску, для кожного VPS. Віртуальні приватні сервери стали популярним вибором для веб-хостингу, оскільки вони пропонують багато переваг виділених серверів за нижчою вартістю. Вони також забезпечують додаткову перевагу простої масштабованості . Оскільки кожен VPS віртуалізований, конфігурацію можна оновити за допомогою модифікації програмного забезпечення, а не оновлення апаратного забезпечення. Тим не менше, виділені сервери часто забезпечують кращу продуктивність, оскільки всі ресурси фізичної машини присвячені одному серверу. [86] Найпоширеніший тип VPS - це веб-хост . Багато веб-хостингових компаній пропонують рішення для хостингу VPS як альтернативу спільному хостингу та спеціальному хостингу. VPS розміщується між двома варіантами, як правило, як за продуктивністю, так і за ціною. Як і загальний хост, VPS може ділитися ресурсами фізичної машини з іншими обліковими записами хостингу. Однак VPS можна

налаштувати на замовлення, як спеціальне хостингове рішення, яке воно ізольоване «приватне» від інших облікових записів.

KeePassX - це програма для людей з надзвичайно високими вимогами до безпечного управління персональними даними. Він має легкий інтерфейс, є крос-платформним та публікується на умовах Загальної публічної ліцензії GNU. KeePassX зберігає багато різної інформації, наприклад імена користувачів, паролі, URL-адреси, вкладення та коментарі в одній базі даних. Для кращого управління для кожного окремого запису можна вказати визначені користувачем заголовки та значки. Крім того, записи сортуються за групами, які також можна налаштувати. Вбудована функція пошуку дозволяє здійснювати пошук в одній групі або в повній базі даних. [8] KeePassX пропонує невелику програму для безпечного створення паролів. Генератор паролів дуже настроюваний, швидкий і простий у використанні. Особливо той, хто часто генерує паролі, оцінить цю функцію. Повна база даних завжди шифрується або за допомогою AES (псевдонім Rijndael), або алгоритму шифрування Twofish, використовуючи 256-бітний ключ. Тому збережену інформацію можна вважати цілком безпечною. KeePassX використовує формат бази даних, сумісний з KeePass Password Safe. Це робить використання цієї програми ще вигіднішим.[8]

Криптовалюта - це цифрові гроші. Це означає, що немає фізичної монети або купюри - все це в інтернеті. Ви можете переказувати криптовалюту комусь в Інтернеті без посередниць, як банк. Біткойн та ефір - добре відомі криптовалюти, але нові криптовалюти продовжують створюватися. Люди можуть використовувати криптовалюти для швидких платежів та уникнення комісій за транзакції. Деякі можуть отримати криптовалюти як інвестицію, сподіваючись, що вартість зросте. Ви можете придбати криптовалюту за допомогою кредитної картки або, в деяких випадках, отримати її за допомогою процесу, який називається « майнінг ». Криптовалюта зберігається в цифровому гаманці або в Інтернеті, і на вашому комп’ютері, або на іншому обладнанні.[26]

Bitcoin - це валюта цифрових платежів, яка використовує криптовалюту (цифровий засіб обміну), технологію блокчейну та мережу однорангових (P2P) на відміну від центрального органу (наприклад, банку) для створення та управління грошовими операціями. Мережа біткойнів P2P з відкритим кодом сприяє створенню всіх біткойнів та керує всіма операціями з біткойнами. [9] Біткойн, який часто називають «готівкою для Інтернету», є однією з декількох популярних валют цифрових платежів поряд із Litecoin, Peercoin та Namecoin. Коли слово Біткойн пишеться з великої літери, воно, як правило, відноситься до програмного забезпечення та систем, що використовуються для біткойнів (у нижчих регістрах воно стосується фактичної валюти) Хоча біткойни фізично не існують, їх «відкривають» кодери-добровольці, які називаються майнерами.[89] Ці майнери використовують високопродуктивні комп'ютери для вирішення складних обчислювальних задач та обробки транзакцій. Цей процес створює (або «видобуває») поодинокі блоки, які потім додаються до загальнодоступного запису, який називається блокчейн. Оскільки блокчейн є загальнодоступним, суть біткойнів децентралізована.[9]

Незалежно від того, скільки майнерів одночасно обробляє транзакції, протокол Bitcoin диктує, скільки часу потрібно для видобутку одного біткойна. Це забезпечує створення нових біткойнів за фіксованою ставкою, хоча вартість майнінгу зазначеного біткойна є змінною величиною, що призводить до інтенсивної конкуренції серед майнерів біткойнів. Варто також зазначити, що вихідний код біткойнів диктує, що пожиткова пропозиція біткойнів обмежена 21 мільйоном.

Біткойн-міксери - це рішення (програмне забезпечення або послуги), які дозволяють користувачам змішувати свої монети з іншими користувачами, щоб зберегти свою приватність. Хоча адреси біткойнів є «псевдонімами» - тобто вони самі по собі не розкривають особистість власника - їх часто все одно можна пов'язати з реальними особами. Наприклад, якщо ви виводите біткойн з біржі, де ви ідентифікували себе,

біржа знає, що адреса виведення коштів - ваша. Існують також більш досконалі методи, такі як аналіз блокчейнів, для прив’язки біткойн-адрес до реальних даних. Наступного разу, коли монети перемістяться з цих адрес, користувачі ризикують розкрити всіляку особисту інформацію. Залежно від того, як вони витрачають монети, вони можуть виявити, скільки монет їм належить (навіть за іншими адресами), на що вони витрачають свої гроші тощо.[10] Змішуючи свої монети, користувачі можуть приховати зв’язок між своїми біткойн-адресами та реальними даними. Це дозволяє їм використовувати Біткойн більш приватно.

Блокчейн - це цифровий запис транзакцій. Назва походить від його структури, в якій окремі записи, звані блоками, пов'язані між собою в єдиний список, який називається ланцюжком. Блокчейни використовуються для запису транзакцій, здійснених з такими криптовалютами, як біткойн , і мають багато інших додатків.[76]

Кожна транзакція, додана до блокчейну, перевіряється декількома комп'ютерами в Інтернеті . Ці системи, які налаштовані на моніторинг певних типів транзакцій блокчейну, утворюють однорангову мережу. Вони працюють разом, щоб гарантувати, що кожна транзакція є дійсною, перш ніж вона буде додана до блокчейну. Ця децентралізована мережа комп’ютерів гарантує, що одна система не може додавати неприпустимі блоки в ланцюг. Коли новий блок додається до блокчейну, він зв’язується з попереднім блоком за допомогою криптографічного хешу, сформованого із вмісту попереднього блоку. Це гарантує, що ланцюг ніколи не розірветься і що кожен блок буде постійно записаний. Також навмисно важко змінити минулі транзакції в блокчейні, оскільки спочатку слід змінити всі наступні блоки.[18] Хоча блокчейн широко відомий своїм використанням у таких криптовалютах, як біткойн, лайткойн та ефір, ця технологія має кілька інших застосувань. Наприклад, це дозволяє «розумні контракти», які виконуються при дотриманні певних умов. Це забезпечує автоматизовану систему ескроу для транзакцій між двома сторонами. Блокчейн потенційно може бути

використаний, щоб дозволити особам платити один одному без центрального пункту клірингу, який необхідний для АСН та банківських переказів. Це може значно підвищити ефективність біржової торгівлі, дозволяючи операціям здійснювати розрахунки майже миттєво, замість того, щоб вимагати трьох і більше днів для кожної транзакції.

Технологію блокчейн також можна використовувати в нефінансових цілях. Наприклад, Міжпланетна файлова система (IFPS) використовує блокчейн для децентралізації зберігання файлів, пов'язуючи файли разом через Інтернет. Деякі платформи цифрового підпису зараз використовують блокчейн для запису підписів та перевірки цифрових підписів. Блокчейн можна навіть використовувати для захисту інтелектуальної власності , пов'язуючи розподіл вмісту з першоджерелом.[18]

Hidden Wiki - це вікі, стійка до цензури, що працює як прихована послуга, яку кожен може анонімно редагувати. Головна сторінка служить каталогом для деяких сайтів .onion. До прихованої Вікі, яка також має псевдодомен верхнього рівня .onion, можна отримати доступ лише за допомогою Onion Routers . На перший погляд це дуже схоже на Вікіпедію. Однак на прихованій Вікі ви знайдете посилання на темні веб-сторінки, які були згруповані в різні категорії. Це допомагає людям орієнтуватися в темній мережі.

Прихована Вікі - це один із найпоширеніших способів для користувачів розпочати навігацію по Глибокій Мережі.[19]

Ботнет - це сукупність підключених до Інтернету пристроїв, заражених шкідливим програмним забезпеченням, які дозволяють хакерам керувати ними. Кіберзлочинці використовують бот-мережі для підбурювання бот-мережних атак, які включають шкідливу діяльність, таку як витік облікових даних, несанкціонований доступ, викрадення даних та DDoS-атаки. Власники ботнетів можуть одночасно мати доступ до кількох тисяч комп'ютерів і можуть наказувати їм здійснювати шкідливі дії. Спочатку кіберзлочинці отримують доступ до цих пристроїв за допомогою спеціальних

троянських вірусів для нападу на системи безпеки комп'ютерів, перш ніж впроваджувати програмне забезпечення управління та управління, щоб дозволити їм здійснювати зловмисні дії у великих масштабах. Ці дії можна автоматизувати, щоб заохотити якомога більше одночасних атак. Наслідки ботнет-атаки можуть бути руйнівними - від повільної роботи пристрою до величезних рахунків в Інтернеті та викрадених персональних даних. Є також юридичні наслідки, які слід враховувати, наприклад, якщо ваш комп'ютер використовується як частина ботнет-атаки, ви можете нести юридичну відповідальність за наслідки будь-якої зловмисної діяльності, яка походить від вашого пристрою

Різні типи ботнет-атак можуть включати:

- Розподілені атаки відмови в обслуговуванні (DDoS), які спричиняють незаплановані простої додатків; [51]
- Перевірка списків витоків облікових даних (атак заповнення облікових даних), що призводять до поглинань облікових записів;
- Атаки веб-додатків для викрадення даних;
- Надання зловмиснику доступу до пристрою та його підключення до мережі.

В інших випадках кіберзлочинці продаватимуть доступ до мережі ботнетів, яку іноді називають мережею "зомбі", щоб інші кіберзлочинці могли використовувати мережу для власної шкідливої діяльності, наприклад, активації спам-кампанії.[20]

I2P - це безкоштовна технологія з відкритим кодом. Багато додатків, такі як пошта, IRC-чат, однорангові програми, обмін файлами та програма обміну миттєвими повідомленнями, використовують інтерфейс I2P, щоб дозволити анонімне спілкування та роботу як для окремих користувачів, так і для організацій. I2P має власну базу даних внутрішньої мережі, яка використовується для надійного розподілу інформації про контакти та маршрутизацію.[21]

DDoS - Розподілені атаки на відмову в обслуговуванні це підклас атак на відмову в обслуговуванні DoS. DDoS-атака включає кілька підключених мережевих пристроїв, спільно відомих як ботнет, які використовуються для переповнення цільового веб-сайту підробленим трафіком.[51]

На відміну від інших видів кібератак, DDoS-атаки не намагаються порушити ваш периметр безпеки. Швидше, DDoS-атака має на меті зробити ваш веб-сайт та сервери недоступними для законних користувачів. DDoS також можна використовувати як димову завісу для інших зловмисних дій та для знесення охоронних пристроїв, порушуючи периметр безпеки цілі. Успішна розподілена атака відмови в обслуговуванні - це дуже помітна подія, що впливає на всю базу користувачів в Інтернеті. Це робить його популярною зброєю вибору для хаквістів, кібер-вандалів, вимагачів та всіх інших, хто прагне висловити бажання або відстояти свою справу.

DDoS-атаки можуть відбуватися короткими спалахами або повторними нападами, але в будь-якому випадку вплив на веб-сайт або бізнес може тривати дні, тижні і навіть місяці, оскільки організація намагається відновити. Це може зробити DDoS надзвичайно руйнівним для будь-якої онлайн-організації. Крім усього іншого, DDoS-атаки можуть призвести до втрати доходів, погіршити довіру споживачів, змусити підприємства витратити статки на компенсації та завдати довгострокової шкоди репутації.[51]

2.2 Месенджер Telegram як спиятливе середовище розвитку Darknet

Програми обміну повідомленнями стали улюбленим способом спілкування, що дає нам можливість спілкуватися з друзями в будь-який час і в будь-якому місці. І хоча Facebook Messenger, WhatsApp та Viber є найвідомішими з них, є одна програма, яка нещодавно з’явилася заявивши, що є найбільш безпечною з них усіх. Ця програма називається Telegram Messenger . Telegram, запущений у 2013 році, є зашифрованою програмою обміну миттєвими повідомленнями, щомісяця використовує 200 мільйонів активних користувачів. Подібно до WhatsApp, користувачі Telegram можуть

спілкуватися як з окремими людьми, так і з групами. Будь-який злочинець, котрий починає тіньову пропозицію або розмову, може насолоджуватися приватними та наскрізними зашифрованими чатами замість відкритих тем, які можна побачити на форумах в Інтернеті. Раніше для забезпечення анонімного підключення до Dark Web через платформу TOR було потрібно кілька кроків. Але сьогодні будь-який користувач Telegram може легко приєднатися до каналів одним натисканням на своєму телефоні, зберігаючи при цьому свою особистість прихованою.

Telegram - це програма для обміну повідомленнями в Інтернеті, яка працює так само, як популярні програми обміну повідомленнями WhatsApp та Facebook Messenger. Це означає, що ви можете використовувати його для надсилання повідомлень друзям при підключенні до Wi-Fi або мобільних даних. Telegram заснований на хмарі і стверджує, що він надає пріоритет безпеці та швидкості, що робить його хорошою альтернативою іншим популярним програмам обміну повідомленнями. Послуга запущена в 2013 році, і з тих пір вона охопила 200 мільйонів активних користувачів щомісяця.[24] Заснований росіянином Павлом Дуровим, який також стоїть за найбільшою в Росії соціальною мережею ВКонтакте (VK), Telegram стверджує, що поєднує швидкість WhatApp із швидкоплинністю Snapchat. Як і WhatsApp, Telegram також має можливість показувати статус друга в Інтернеті та додавати та ділитися фотографіями, відео, місцезнаходженням, контактами та документами.[23]

Відмінною рисою Telegram є безпека. Вся його діяльність, включаючи чати, групи та засоби масової інформації, якими обмінюються учасники, зашифрована. Це означає, що їх не буде видно без попередньої розшифровки. Додаток також дозволяє встановлювати таймери самознищення для повідомлень та носіїв, якими ви ділитесь, які можуть складати від двох секунд до одного тижня завдяки вбудованій функції "Секретний чат". Він також пропонує наскрізне шифрування, не залишаючи слідів на серверах Telegram. Також є можливість перевірити безпеку своїх "таємних чатів",

використовуючи зображення, яке служить ключем шифрування. Порівнюючи свій ключ шифрування з ключем друга, ви можете ефективно переконатися, що ваша розмова безпечна та менш вразлива до атак.

Функція секретних чатів Telegram використовує наскрізне шифрування, що означає, що вона не залишає слідів на серверах, підтримує самознищення повідомлень і не дозволяє переадресацію. Голосові дзвінки також наскрізні зашифровані. Це навіть дозволяє налаштовувати ботів для конкретних завдань. Завдяки своєму багатому набору функцій та швидкому прийняттю, Telegram став затребуваним інструментом на сцені шахрайства. Згідно з веб-сайтом Telegram, додаток дозволяє користувачам створювати приватні групи, що містять до 200 000 учасників, а також публічні канали, доступ до яких має кожен, хто має програму.

Ті сайти, що ми бачимо відкриваючи посилання в браузері є частиною Мережі. Вона працює на основі стека (групи) протоколів TCP / IP. Серед них найбільш важливими є Transmission Control Protocol (протокол управління передачею, TCP), Internet Protocol (протокол інтернету або міжмережевий, IP) і HyperText Transfer Protocol (протокол передачі гіпертексту, HTTP, останнім часом, частіше захищений, S). Перший відповідає за надійну передачу потоку байтів від одного комп'ютера до іншого, а другий за маршрутизацію пакетів даних, тобто визначення всіх пунктів передачі даних. HTTP працює на рівень вище і дозволяє кодувати інформацію у вигляді документів (сайтів).

На основі цих протоколів можуть бути створені оверлейні мережі, такі як TOR або I2P, а також VPN і багато інших. Більшість з них призначені для усунення головних недоліків Інтернету - низьку безпеку і практичного повної відсутності анонімності. Команда Telegram запропонувала ще один варіант - TON Sites. Технічно, сайти, створені в мережі TON будуть схожі на звичайні веб-сторінки. Різниця полягає в тому, що вміст таких сайтів не буде зберігатися на якомусь одному сервері, а буде рівномірно розподілено по вузлах мережі і користувачам. Замість IP-адрес в цій мережі будуть ADNL,

плюс цей протокол за умовчанням забезпечує шифрування. Доступ до звичайних HTTP-сайтів і назад можливий через шлюзи.[24]

На даний момент доступна інструкція по компіляції проксі (шлюзу), а також створення сайту. Вона розміщена на ресурсі для розробників TON і дозволяє почати бажаючим експериментувати з новим інструментарієм.

«Відкрита мережа Telegram» (TON - Telegram Open Network) була анонсована в 2017 році Павлом Дуров. За задумом цього всесвітньо відомого ексцентричного розробника і колишнього генерального директора «ВКонтакте» проект повинен буде стати новим стандартом онлайн-торгівлі, а також основою інфраструктури безпечного обміну даних. На поточний момент, за словами самого Павла і даними обізнаних джерел, платформа знаходиться в кінцевій стадії розробки.[24]

В першу чергу TON має на увазі під собою зручність для користувача. Транзакції, які будуть проходити на цьому блокчейні, не вимагають очікування і великий комісії, і виконуються так само швидко, як Visa і Mastercard. Блокчейн працює за принципом Proof-of-stake протоколу, що робить транзакції безпечними. Архітектура складається з одного блокчейна і 292 додаткових мереж. Блокчейн буде підтримувати технологію шардінга, яка прискорить генерацію нових блоків і збільшить швидкість транзакцій.[25]

Блокчейн TON складається з безлічі блокчейнов, які діляться на:

- Головний блокчейн, який буде зберігати ключову інформацію про протокол, таку, як хеш, інформацію про валідаторах і їх «балансів»;
- Безліч «робочих» блокчейнов, що дозволяють виконувати смарт-контракти. Такі блокчейни TOH можуть бути створені у відповідності з різними правилами і використовувати різні Віртуальні Машини для виконання смарт-контрактів;
- Повну структуру блокчнйна TON: мастерчейн воркчейн, шардчейн, блоки, де блоки також є деякою різновидом блокчейна, що дозволяє їх переписувати і відмовитися від хардфорков мережі.

TON буде використовувати протокол ADNL (256 біт ідентифікатора каналу + вміст пакета) який дає можливість будь-яким вузлам обмінюватися інформацією один з одним. Можна сказати, що завдяки ADNL все вузли утворюють глобальний граф TON. Але додатково передбачена можливість створювати оверлейні мережі - підграфи всередині цього графа. Оверлейні мережі можуть бути публічними і приватними. Стати учасником публічної мережі нескладно - потрібно знайти TL-структуру, що описує її (вона може бути публічною - або доступна за певним ключу в DHT). У випадку з приватної мережею ця структура повинна бути відома вузлу заздалегідь.

Telegram Open Network включає в себе наступні продукти:

- TON Storage. Система зберігання, яка подібна до роздільного аналогу Dropbox;
- TON Proxy. Децентралізований VPN сервіс, заснований на блокчейне, який являє собою середовище для безпечного використання TON. Являє собою анонимайзер, аналогічний TOR;
- TON Services & DNS. Платформа для надання сторонніх сервісів, що дозволяє використовувати призначені для користувача інтерфейси і сервіси доменних імен.[73]
- TON Payments. Платформа для проведення мікроплатежів і P2P транзакцій.[25]

Gram - внутрішня криптовалюта платформи TON. Розробники криптовалюта бачать в ній аналог Visa і Mastercard: всередині мережі будуть відбуватися миттєві транзакції. Gram заснований на протоколі Proof-of-Stake і буде забезпечений завдяки роботі смарт-контрактів. Це допоможе проводити до 10 млн транзакцій / сек. У Gram передбачається Майнінг. Істинність транзакцій забезпечують "валідатори", які отримують за це комісію. Це робить криптовалюта схожою на Ripple.[53]

Зловмисники перебираються до Telegram, оскільки останнім часом правоохоронні органи успішно руйнують ринки та форуми Dark Web, такі як Hansa Market та AlphaBay. До Telegram легко отримати доступ і пропонує

хороші можливості безпеки, тому деякі з розміщених груп чату стали корисною альтернативою форумам Dark Web.

Прикладами каналів чату є "DarkWork", "Blacmarket". Повідомлення про них включають рекламу, яка прагне наймати працівників компаній чи банків, отримувати внутрішню інформацію та конфіденційні дані. Ця внутрішня інформація може бути продана або використана для проведення кібератаки всередині компанії. Інші незаконні послуги в деяких більш кривих каналах Telegram включають підробку юридичних документів. Підроблені документи включають посвідчення особи, паспорти, банківські документи тощо. Автор одного з дописів стверджував, що має зв’язки всередині російського управління дорожньої поліції і що він може видавати водійські посвідчення всіх категорій.[52]

Зручність каналів Telegram дозволяє учасникам загроз та тим, хто прагне взяти участь у кіберзлочинах, спілкуватися в більш безпечній та легкодоступній формі. Хоча програми обміну повідомленнями стали невід’ємною частиною сучасного життя та вдосконалювались з роками, щоб забезпечити безпеку інформації своїх користувачів, ними також користуються ті, хто тікає від сторонніх очей, а законодавство - піддаючи особисту та фінансову інформацію ризику .

2.3 Інформаційні злочини політичного характеру в мережі Darknet

Стрімкий розвиток технологій, розвиток інформаційних технологій і широке використання Інтернету привели до революційних змін у всіх сферах повсякденної діяльності, в процесі виробництва, в торгівлі, освіті, розвагах, і навіть спосіб мислення сучасної людини. Поряд з цими змінами, які в цілому поліпшили якість нашого життя, з'явилися умови, які сприяють розвитку нових форм злочинності.[94] Ці нові форми злочинності в цілому називаються «Злочини у сфері інформаційних технологій».

Інформаційні технології зробили можливим вчинення широкого кола злочинів, які вимагають знань і високої професійної підготовки. Так

«злочином в сфері інформаційних технологій», вважаються карані злочинні дії, вчинені з використанням обчислювальної техніки та систем обробки даних, за вчинення яких грецьке законодавство передбачає конкретне покарання.

Основна відмінність електронних злочинів полягає в тому, одні з них відбуваються з використанням комп'ютера (комп'ютерні злочини), а інші з через Інтернет (кіберзлочини). Варто відзначити, що в грецькому законодавстві поки що не існує закону, який би стосувався виключно питань Інтернету та регулював поведінку користувачів Інтернету з точки зору кримінального права. Форми електронних злочинів різноманітні і з безперервним розвитком технології та Інтернету з'являються все в більшій кількості. Для усунення цієї небезпеки необхідні міждержавні консультації і розробка комплексної та ефективної стратегії.[50]

Електронним злочинів відноситься: незаконне копіювання або зміна конфіденційних даних, несанкціоноване використання або доступ до програм або даними комп'ютера, включаючи хакерство, розповсюдження вірусів, підроблення та шахрайство. Злочин в кіберпросторі має характеристики, які необхідно враховувати для того, щоб краще зрозуміти. Воно відбувається швидко, за лічені секунди, може трапитися з ким завгодно, хто підключений до Інтернету, і з будь-якого місця на планеті.

У першому випадку мова йде про людей, які не обов'язково мають спеціальні навички використання комп'ютера, в той час як питання юрисдикції (наприклад, зв'язку грецької влади з Facebook) в деякій мірі регулюється. Дуже часто, однак, кіберзлочинці, що створюють найсерйозніші проблеми країнам, організаціям і приватним особам, особливо розумні, мають спеціальні знання і обладнання, і їх надзвичайно важко ідентифікувати.

Не випадково в Англії з лютого 2001 року хакерів, в залежності від важливості атаки, можуть вважати терористами. Точно так же в США, будь-який акт несанкціонованого доступу до PC вважається терористичною

атакою і карається в залежності від важливості вторгнення, аж до довічного ув'язнення без можливості скорочення терміну.

Навіть якщо ці особи і будуть ідентифіковані, їх арешт часто залежить від співпраці між країнами, де була виявлена їх діяльність, і країною, в якій вони знаходяться. Насправді це одна з найбільших перешкод, які можуть бути вирішені тільки на основі партнерства і розробки спільних дій.

Однією з серйозних проблем кіберзлочинності є визначення місця скоєння злочину. Простий приклад: сервер, де розміщений веб-сайт знайомств інтернет-шахраїв знаходиться в США, управляється сайт з Румунії, а його діяльність охоплює багато країн.

На конференції по електронній злочинності в 2001 році в Будапешті була підписана Конвенція про кіберзлочинність. Відповідно до Конвенції, кожна держава-учасниця зобов'язана створити необхідні правові умови для надання наступних прав і обов'язків компетентним органам по боротьбі з кіберзлочинністю: виїмка комп'ютерної системи, її частини або носіїв; виготовлення та конфіскація копій комп'ютерних даних; забезпечення цілісності і збереження комп'ютерних даних, які, що стосуються справи; знищення або блокування комп'ютерних даних, що знаходяться в комп'ютерній системі.

Конвенція також вимагає створити необхідні правові умови для того, щоб зобов'язати Інтернет-провайдерів проводити збір і фіксацію або перехоплення необхідної інформації за допомогою наявних технічних засобів, а також сприяти в цьому правоохоронним органам. При цьому рекомендується зобов'язати провайдерів зберігати повну конфіденційність про факти подібного співробітництва.

На початку 2002 був прийнятий Протокол №1 до Конвенції про кіберзлочинність, який додає до переліку злочинів поширення інформації расистського та іншого характеру, підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовому, національному, релігійному або етнічної приналежності.[72]

До інформаційних злочинів політичнго характеру в мережі даркнет можно віднести:

- хактивізм;
- кібершпіонаж;
- кібертероризм.

Хактивізм - це методологія використання хакерства як форми політичної чи соціальної активності. Хактівізм передбачає розбіжності проти дій чи організацій у формі цифрових процесів та \ або цифрових носіїв для просування політичного порядку денного. Інше визначення - використання технологічних хаків чи громадянська непокора шляхом прямої дії проти організацій електронними засобами. Найпростішою визначальною характеристикою є активізм, який є руйнівним.[57]

Хактивісти атакують і зламують захищені комп'ютерні системи. Об’єктом хактивістів часто є великі корпорації або державні органи. Оскільки хактивісти діють з почуттям політичної совісті, вони можуть також атакувати менші корпорації та організації. Хакери мають на меті отримати фінансову вигоду, і тому вони в основному націлені на більші організації, проте хактивісти не прагнуть отримати грошову вигоду, тому майже будь-яка організація, незалежно від їх розміру, може стати об'єктом хактивізму.

Хаквісти використовують точно такі ж інструменти, методи та програмне забезпечення, як і хакери: шкідливе програмне забезпечення, віруси, троянські програми, комп'ютерні хробаки, фішинг та інше зловмисне програмне забезпечення на додаток до DDoS-атак, атак грубої сили та подібних методів.

Оскільки хактивізм є більш новим поняттям, важливо виявити деякі більші випадки хактивізму та визначити причини, що ці випадки мали місце. Це допоможе допомогти організаціям зрозуміти деякі поштовхи до хактивізму та, можливо, проаналізувати методи, які вони можуть використовувати, щоб не стати жертвою хактивізму.

Операція Туніс. У 2011 році на Міністерство промисловості Тунісу та на біржу напала кібергрупа Anonymous. Причиною нападу була цензура та напади уряду на тих, хто намагався опублікувати свободу слова через веб-сайт WikiLeaks. Напади носили помстивий характер і складалися з декількох розподілених процесів відмови в обслуговуванні, щоб вивести з ладу урядові сайти. DDoS атака просто бомбардують законний сайт з такою кількістю даних і інформації запиту він більше не може приймати легітимні запити сторінок. Вони також отримали доступ до урядових веб-сайтів і зневажили їх листами, що вислали уряд Тунісу за пригнічення мови та цензуру.

OpVenezuela. У 2014 році внутрішні повстання на знак протесту проти репресій та цензури уряду Венесуели спричинили напад груп «Анонім», «Лулсек» та «Бінарні опікуни». Ця широко розповсюджена кампанія нападів на DDoS та викривлення урядових веб-сайтів цими кібер-учасниками мала протестувати проти уряду Мадуро. Крім того, активісти змогли отримати доступ до офіційного акаунта президента Мадуро у Twitter і розмістили твіти, в яких говорилося: «No se metan con los mejores», зламаний @LulzSecPeru» або «Не сперечайся з найкращими». Основні міркування цих хакерів були безпосередньо пов'язані з неможливістю подати скарги та політичним опозиціями проти цензури та державного насильства.

Боротьба з хактивізмом - дуже складна перспектива. По-перше, багато хактивістських організацій борються лише з гнобленням та привласненням коштів та просувають кілька гуманітарних причин. Якщо ви подивитесь на основні перспективи, це соціальна несправедливість, яка давно залишилась без відповіді у багатьох із цих країн. По суті, це низові зусилля, спрямовані на досягнення політичних результатів за допомогою асоціальних методів та засобів. Крім того, групи не мають центральної ідентичності. Вони працюють на електронних дошках оголошень та інших форумах, публікуючи свої загадкові повідомлення в соціальних мережах, щоб викликати інтерес. Це означає, що організаціям доведеться застосовувати захисні засоби всередині, щоб гарантувати, що вони не стануть жертвами хакерської діяльності.

Кібершпигунство - використання комп'ютерних мереж для отримання незаконного доступу до конфіденційної інформації, як правило, такої, що зберігається урядом чи іншою організацією.[83]

Кібертероризм - передбачає використання комп'ютерів та супутніх технологій з метою заподіяння шкоди чи збитку з метою примушення цивільного населення та впливу на політику цільового уряду або іншим чином вплинути на його поведінку. Крім того, кібертероризм, який слід диференціювати від хактивізму та кібервійни, передбачає націлювання на критичні інфраструктури.[56]

До інформаційних злочинів політичного характеру можно віднести втручання Росії у вибори у США 2016 року замах на основи американської демократії. Від витончених зусиль у соціальних мережах та традиційних інформаційних операцій до спроб злому списків виборців та державних виборчих систем, росіяни взяли участь у спільній кампанії з метою підірвати американську демократію та послабити довіру до демократичного процесу та інституцій.

Це не єдиний раз, коли росіяни займаються цим видом діяльності. У таких країнах, як Нідерланди, Україна та Франція, росіяни використовували операції впливу, щоб впливати на політичні кампанії, кандидатів і дискурс, щоб атакувати сприйнятих противників путінської Росії та підтримувати тих, хто симпатизує російським інтересам. Росіяни вирішили використовувати інформацію та впливати на операції та кіберінструменти для досягнення трьох важливих і доповнюючих цілей:

Ці типи атак, спрямовані на США та інші країни, безумовно, виявляють сучасну небезпеку та вразливість для відкритих демократичних процесів, систем та даних. Росія інвестує у узгоджені та складні стратегії для послаблення країн-конкурентів та послаблення союзів, таких як НАТО або всередині Європи, які, як вважають, відповідають російським інтересам. Як зазначив у своєму недавньому зверненні директор ЦРУ Майк Помпео,

зусилля Росії по підриву американської демократії еволюціонували і становлять "серйозну загрозу".

Більш принципово, вони розкривають нову форму комбінованого, асиметричного впливу та кібератак, спрямованих на демократичні держави та інституції. США та їхні демократичні союзники у всьому світі тепер повинні розглядати такі кампанії як основоположні, наполегливі та стратегічні загрози цілісності демократичної політичної системи. Вони також повинні усвідомити, що російський ігровий збірник може бути скопійований та розгорнутий іншими державними та недержавними суб'єктами, які намагаються вплинути на курс демократичного суспільства по всьому світу. Деталі кампанії 2016 року є важливими і продовжують розкриватися в міру розслідування в Конгресі та у Федеральному бюро розслідувань, в тому числі за допомогою висновків розвідувального співтовариства та аналізів Департаменту національної безпеки. Розкрита тактика викриває російську книгу ігор.

Російська кампанія, яка використовувала державні та недержавні довірені особи, передбачала повномасштабні інформаційні операції за допомогою використання традиційних та соціальних медіа, кіберзломів електронних листів політичних партій та продавців, пов'язаних з виборами, а також перевірки державних виборчих систем та виборців валки. Як частина цієї кампанії, до двадцяти однієї державної мережі, пов'язаної з виборами, " потенційно була націлена на російських урядових кібер-суб'єктів", згідно зі свідченнями двох службовців Міністерства національної безпеки цього літа.

Нещодавні розкриття спонсорованих Росією кампаній у соціальних мережах за допомогою облікових записів Facebook та Twitter (ботів (автоматизованого програмного забезпечення для полегшення обміну повідомленнями в Інтернеті)) є частиною ширшої кампанії Росії з метою вплинути на політичний дискурс у Сполучених Штатах, посіяти соціальні розбіжності. і вплинути на виборчий процес. У міру того, як з’являються деталі, масштаби спотворень стають чіткішими. За однією оцінкою, кількість

Twitter-ботів становила 400 000 за місяці до виборів. Facebook нещодавно передав Конгресу деталі понад 3000 оголошень, придбаних компанією, пов’язаною з Кремлем. Хоча, схоже, фактичних кібер- чи інших збоїв в системах голосування в день виборів 2016 року не було, були напади на державні системи голосування, як, наприклад, при злому постачальника виборчих послуг та доступу до списків для голосування, як в Іллінойсі. Небезпека в таких випадках полягає в здатності іноземних суб'єктів маніпулювати, спотворювати або навіть знищувати дані про голосування, доступ або системи. Це суть цілісності виборчого процесу.[98]

РОЗДІЛ 3. МІЖНАРОРДНА ТА ВІТЧИЗНЯНА ПРАКТИКА КІБЕРЗЛОЧИННОСТІ

3.1 Міжнародні актори в мережі Darknet. Вплив Darknet на світові політичні процеси

Протягом останніх кількох років національні держави все частіше використовують темну павутину як інформаційне поле бою для різноманітних ключових розвідувальних та кібер-військових кампаній. В епоху цифрових інформаційних операцій Сполучені Штати, Росія та Китай є основними суб'єктами національних держав, які обговорюються у засобах масової інформації та звітності з відкритим кодом. Сполучені Штати, Росія та Китай все ще чітко лідирують у кібер-орієнтованих фінансових ресурсах та робочій силі, відбувся значний ріст менш відомих національних держав через випуск прогресивних подвигів, що просочилися в останні роки та доступні зворотні машинобудування.

Темна павутина забезпечує анонімне середовище, в якому може працювати кожен. Важливість та значущість для національних держав, низка ключових цілей може бути досягнута під цим пластом анонімності. Кібер-діячі національних держав використовуватимуть темну мережу для збору розвідувальних даних та розробки джерел, урядового та корпоративного шпигунства, експлуатації та тестування, операцій з дезінформації для геополітичного впливу, порушення інфраструктури та отримання фінансової вигоди.[64]

- **Розвідка та шпигунство** - Ранній початок інформаційних операцій, заснованих на кіберпрограмі, проводили Агентство національної безпеки США (АНБ) та Народно-визвольна армія Китаю (НВАК). Хоча АНБ використовувала інформаційні операції для негласного збору розвідувальних даних від іноземних супротивників, Китай добре відомий своєю великою діяльні у шпигунстві та розкраданні інтелектуальної власності з великим успіхом. Це включає нагляд за власними громадянами та використання ними темної павутини для спроби обійти державний контроль.

- **Порушення інфраструктури** - Інтернет-кампанії, що фінансуються державою, проти інших національних держав набули широкого розповсюдження, головним чином націлені на мережі, що містять конфіденційну урядову або корпоративну інформацію та стратегічні плани. Наприкінці 2015 року Росія продемонструвала, як кінетичні атаки, що проводяться на критичну інфраструктуру та інформаційні пункти, можуть калічити національну державу , хакуючи Україну під час поточних конфліктів за Крим. Міністерство національної безпеки США та багато дослідників кібербезпеки виявили та повідомили про додаткові спроби проникнення в ключову американську комунальну інфраструктуру на основі кібер.

- **Активізм та пропаганда** - будь то релігійні розбіжності на Близькому Сході чи ідеологічні розбіжності в Південно-Китайському морі, політичний активізм та пропаганда є ефективною зброєю національних держав протягом десятиліть. Враховуючи перехід суспільства до стійких цифрових комунікацій, кібер став найкращим середовищем для цього виду діяльності. Національні держави, як великі, так і малі, використовували кібердіяльність, щоб робити все, починаючи від просування своїх програм денного життя , до підкріплення держав-проксі як у темній мережі, так і на соціальних медіа-платформах.

- **Еквайлайт Придбання та розробка** - багато експлойтів чорних шапок обговорюються на темних веб-форумах та в зашифрованих чатах. Системні вразливості деталізовані та спільно використовуються для всіх типів критичних операційних систем та дистрибутивів Unix. Темна мережа забезпечує цінний ресурс для анонімного дослідження та тестування вихідного коду.

- **Прибутковість** - країни, які стикаються з екстремальними економічними санкціями США та ООН, звертаються до темної мережі з метою отримання фінансової вигоди. В останні роки Північна Корея успішно

розпочала хакерські операції з банківською системою в масштабах усієї Східної Азії.

Як можна було б підозрювати, актори національних держав не виявляються відразу в темній мережі. Коли національна держава здійснює оперативну атаку на організацію або викрадає важливу інформацію, вона мало потребує або бажає виставляти ці дані на продаж або іншим способом скидати їх через анонімні мережі. Подібним чином уряди не повідомлятимуть про збір розвідувальних даних або заходи збору правоохоронних органів, окрім як єдиною метою психологічної диверсії.

Провівши останні п’ять років, архівуючи анонімні сервіси темної мережі та взаємодіючи із спільнотою темної мережі, аналітики виявили низку «відбитків пальців» акторів національної держави. Ми бачимо в темній павутині ці відбитки пальців як ознаки та спонукальні фактори, пов’язані з використанням анонімними мережами акторів національної держави.

Актори національної держави в темній мережі мають кілька ключових відбитків пальців, які відповідають їх мотиваційному використанню для темної мережі.

- **Актори національних держав використовують темну павутину для придбання та викрадення кібер-подвигів**

Актори національних держав отримують кібер-експлойти з відкритим кодом з підземних ринків, щоб здійснити зворотний інжиніринг - часто для успішного побудови програмного забезпечення для протидії будь-яким атакам, коли такий експлойт використовується проти уряду або критичної мережі. Ключовим ідентифікатором актора національної держави, який видається покупцем експлуатуючої діяльності, є наявність значного бюджету та фінансових ресурсів для придбання пропонованих товарів. Регулярні темні користувачі Інтернету регулярно обговорюють "розповіді" для виявлення правоохоронних та / або розвідувальних агентів у мережі.

- **Актори національних держав отримують грамоти ворожих урядів та інших суб'єктів, що мають геополітичний чи військовий інтерес** .

Наприклад, темна мережа рясніє адресами електронної пошти US * .gov, які можна використовувати для грубого втручання в мережу або цільових фішингових кампаній. Виявив понад 550 000 темних веб-сторінок з обліковими даними, включаючи електронну адресу .gov.

Іран також має значний урядовий слід витоків вірчих даних та мережевої інформації, але не можна легко визначити, чи ця інформація просочилася іншим актором національної держави або командою пильних хакерів. Наприклад, хакер IranDokht, швидше за все, пов'язаний з недавньою глибокою веб-пастою користувача slntar, яка включала кілька десятків адміністративних панелей веб-сайту уряду Ірану для зловмисного націлювання.

- **Розроблені кампанії для фішинг-фішингу використовуються не лише злочинцями, націленими на корпоративні мережі, але й актори національних держав використовують їх для своїх політичних та мілітаристських програм**.

Північна Корея успішно використовувала фішинг для отримання доступу до численних наукових дослідницьких організацій та критичних аналітичних центрів США, використовуючи китайську модель для технологічного прогресу за допомогою цифрового шпигунства. Під час операції «ВТАРЕНИЙ ПЕНСІЛ» Північна Корея націлилась на групу ядерних програм, розповсюдження зброї та поліції Стенфордського університету. Інфраструктура операцій накладалася на інші кампанії, проведені Північною Кореєю. Одна з IP-адрес, що використовуються в цій кампанії (157.7.184.15), також розмістила домен bigwnet [.] Com, який використовувався як інфраструктура управління та керування шкідливим програмним забезпеченням «BabyShark».

Раніше цього року було виявивлено, що IP-адреса (5.160.246.99), що базується на Ірані, була пов’язана зі списком доменів уряду Великобританії, зокрема доходу та митниці Її Величності «HMRC» у цільовій фішинг-кампанії.

- **Актори національних держав використовували темну павутину для проведення кінетичних атак на інфраструктуру супротивника.**

У 2017 році Іран здійснив кібератаки на системи безпеки на саудівській Аравії Aramco, одному з найбільших виробників нафти у світі. Хакери використовували шкідливе програмне забезпечення Triton, щоб змінити один із контролерів безпеки цих об'єктів, в результаті чого контролер зупинив невизначений промисловий процес.

У 2015 році Росія успішно продемонструвала вимкнення українських електромереж під час політичних протестів. Також вважається, що Росія стоїть за низкою атак на енергетичні мережі Ірландії , можливо, полігоном для розробки експлоата, який планується використовувати проти більш грізних противників.

Нещодавно випущений американським КІБЕРКОМ припущення про те, що США успішно встановили приховане зловмисне програмне забезпечення в російській електромережі, щоб кінетично перервати російську інфраструктуру у випадку майбутньої атаки, наприклад, президентські вибори 2020 року у відповідь на доступ Росії до ключових систем ядерної безпеки в 2018 році.

Влітку 2019 року, незадовго до Black Hat 2019, у квітні Microsoft повідомила, що Центр розвідки загроз виявив цілеспрямовану атаку на пристрої **IoT** [90], включаючи: телефон із передачею голосу за IP «VOIP», принтер та відеодекодер. Атака вразила кілька локацій, використовуючи пристрої як м'які точки доступу до більш широких корпоративних мереж. Два з трьох пристроїв все ще мали заводські налаштування безпеки, програмне забезпечення третього не було оновлено. Microsoft приписує атаку

російській групі, яку вона називає Strontium, альтернативною назвою групи Fancy Bear.[68] Дослідники кібербезпеки визначили цю групу як APT28. Тиждень тому була пов’язана та сама група, яка фінансується державоюзлом захищених акаунтів електронної пошти дослідників, які розслідують злочини, які, як стверджується, були скоєні російською державою. Fancy Bear / APT28, Fancy Bear також є ключовим фактором для злому IoT за даними Microsoft.

- **Національні держави використовують темну павутину для здобуття політичного впливу шляхом доксингу політичних опонентів.**

Згідно з доповіддю Мюллера, Guccifer 2.0 успішно порушив DNC під час кампанії 2016 року, а отримана інформація була обережно оприлюднена, щоб вплинути на вибори в США. Численні докси різних ключових міжнародних діячів на Tor's DoxBin. doxbwurbe475dm5i [.] onion. Крім того, Президент Трамп багато наповнений численними прикладами з темних веб-сервісів Cebolla та DoxBin.

- **Пропаганда Dark Web.**

Ефективне використання пропаганди є ключовою рисою успішного проведення інформаційних операцій. Шкідлива інформація про політичного чи військового опонента може просочуватися в критичні моменти, щоб вплинути на результат та громадську думку. Темна мережа містить численні приклади, коли урядові дані країн потрапляли на приховані форуми та сайти з метою політичної вигоди та міжнародного впливу.[99]

Подібним чином «Гардіан» повідомляв, що саме підрозділу з кібербезпеки Саудівської Аравії було наказано «зламати» його комп'ютерні мережі через критичне повідомлення «Гардіан» про відкрите вбивство KSA журналіста Washington Post Джамаля Хашоггі.

- **Одним з найосновніших відбитків пальців акторів національної держави в темній павутині є збір інформації .**

Широко відомий «секрет», що збір ключових HUMINT «людський інтелект» [65] проводиться ізраїльським Моссадом та американським ЦРУ на

темних веб-форумах, чатах та в Інтернет-ретрансляційних чатах. Агентів регулярно закликають і дражнять за відкриту присутність у деяких популярних темних веб-кімнатах.

Критична оборонна технологія США була випущена в темну павутину і доступна для збору розвідувальних даних та зворотного проектування іноземними противниками. Наприклад, минулого року американські військові специфікації для безпілотника MQ-9 Reaper з'явились у темній мережі для продажу та широко поширилися. Конфіденційну інформацію за участю безпілотника MQ-9 Reaper та інших військових документів було викрадено з комп'ютера капітана ВПС США.

Звітність із відкритим кодом показала, що ізраїльський інструмент збору розвідки Whatsapp Peagsus [67] був розгорнутий у 45 різних країнах для збору мобільних телефонів і навіть проданий Саудівській Аравії для спостереження за потенційними дисидентами в країні в більш прихованих засобах збору розвідувальних даних. Нещодавно зламаний російський підрядник SyTech обговорив спроби зневірити Tor, потенційно розкривши справжню ідентифікацію відвідувачів та хостів прихованих служб у темній мережі.

З огляду на цей постійно мінливий ландшафт загрози в темній павутині, національні держави звертаються до довірених осіб та використовують терористичний сегмент темної павутини для запуску атак та уникнення приписування. Замість того, щоб використовувати кімнату, повну кібер-солдатів у Китаї, націлену на кімнату, повну хакерів у Форт-Мід (NSA) у темній мережі, деякі держави-країни вирішили залучити приватних «підрядників» для проведення інформаційних операцій від їх імені.

Росія має найширшу колекцію кібер-найманців та приватних підрядників для їх порядку денного національної держави. Наприкінці жовтня британські звіти з відкритим кодом припускають, що Національний центр кібербезпеки виявив, що група Turla, кіберзлочинна група, що охороняється урядом Росії, захопила передбачувану державою іранську

хакерську групу , відому як OilRig або APT34, і згодом здійснив напади на 35 країн. У липні хакерська група активно націлювалась на політичні групи США, використовуючи кодовий рядок «TrumpTower», який у поєднанні з вищезазначеними даними міг зробити висновок, що вони можуть бути пов'язані з передбачуваною іранською групою фософорів.

Російські підрядники також активно працюють і в Tor. На початку цього року хакери, приховуючись під ім'ям ov1Ru $, порушили російського підрядника розвідки, SyTech розкривши низку секретних програм, спрямованих на програми анонімності Tor. Виглядаючи як зловмисний вузол виходу в анонімній мережі Tor, програма підрядника під назвою Nautilus-S була спеціально налаштована на деанонімізацію трафіку Tor. Підрядник, тісно співпрацюючи з російською службою ВПС та FSB 71330, також мав ще одну програму в 2010 році, яку називали Nautilus, яка збирала дані соціальних мереж від користувачів Facebook, Twitter, LinkedIn та інших.

Можливо, Росія намагається моделювати свою поведінку після відносин Агентства національної безпеки США з комерційними підрядниками. Наприклад, Буз Аллен Гамілітон (BAH) має цілісний союз із розвідувальним співтовариством, де поряд із АНБ працюють сотні, якщо не тисячі фахівців з розвідки та кібербезпеки. Значним витокам розвідки з АНБ за недавню історію сприяли такі підрядники, як Едвард Сноуден та Реаліті Віннер, обидва мали делікатний доступ до інформації та діяли від імені уряду США під час перебування в BAH. АНБ та інші важливі організації розвідувального співтовариства продовжуватимуть вимагати підтримки у підрядників, які не входять до складу відомства, для досягнення своїх цілей розвідки над національними загрозами.

Глобальний тероризм, який часто підживлюється фінансово та політично деякими державами, має постійний та часто реагуючий слід у темній павутині, що реагує на геополітичні події та політику, а також на зміну технологій. Багато великомасштабних екстремістських організацій, таких як ІДІЛ, «Аль-Каїда» та ліванська «Хезболла», оголосили себе

«національними державами», наповненими військовими ресурсами, такими як кіберармії та тактичні хакерські групи, які прагнуть виконати свої програми. На заході існує широко суперечливий звіт із відкритим кодом щодо справжньої діяльності таких квазінаціональних держав у темній мережі. Кілька років тому, за оцінками, ІДІЛ широко використовував анонімні мережі, щоб закрити місцезнаходження та особисті дані своїх членів та новобранців. Також існувала низка легкодоступних прихованих служб, що рекламують пов’язаний з Даєшем вміст - арабська мовна абревіатура ІДІЛ, включаючи вербування та пропагандистські матеріали. Темні анонімні мережі, такі як Tor, матимуть обмежене майбутнє використання для відкритого вербування терористів та розповсюдження пропаганди, але натомість терористи демонструють перевагу зашифрованим мобільним додаткам, таким як Whatsapp та Telegram, для організаційної координації та зв'язку.[96]

Терористи використовують темну павутину, щоб приховувати широкий моніторинг поверхневої павутини компаніями соціальних мереж та представниками служби безпеки призвів до швидшого вилучення екстремістського контенту з платформ соціальних медіа. З цим пов'язано посилене використання терористичними мережами темної мережі для спілкування, радикалізації та планування атак. Також терористи використовують темну павутину для вербування. Хоча початковий контакт можна встановити на поверхневих веб-платформах, часто даються подальші вказівки щодо наскрізних програм шифрування, таких як Telegram, про те, як отримати доступ до веб-сайтів, пов'язаних з джихадистами, у темній павутині.

Терористи використовують темну павутину як резервуар пропаганди, видалення екстремістського та терористичного вмісту з поверхневої мережі збільшує ризик втрати матеріалів терористичних організацій. Значна частина цього вмісту згодом з’являється на темній павутині.

Терористи використовують віртуальні криптовалюти, щоб уникнути виявлення та збору коштів. Терористи, як і злочинці, використовують криптовалюту, оскільки вона забезпечує таку ж форму анонімності у фінансовій ситуації, що і шифрування для систем зв'язку. Згідно з інформаційною інформаційною інформацією, наприкінці 2017 року дослідники спостерігали сплеск збору коштів ІДІЛ, зокрема спеціальних сайтів, що заохочують пожертви біткойнів, підтверджуючи, що кібертерористи ІДІЛ знають про ризики моніторингу фінансових операцій.[63]

В даний час існує дуже обмежена кількість легко виявлених ІДІЛ або формалізація прихованих служб терористичної групи в темній мережі. Прикладом є «Кібер-Кахілафа», ефективна хакерська організація "Ісламської держави", яка у 2016 році була надзвичайно активною в темній мережі, розміщуючи вміст, пов'язаний з ІДІЛ, наприклад відео та пропагандистські навчальні матеріали. Деякі темні веб-форуми припускали, що це західний уряд, який знаходиться в державному управлінні

Завдяки великим зусиллям міжнародних альянсів у «війні проти тероризму» існує кілька терористичних груп, що мають інфраструктуру та організаційну силу для широкої координації через анонімні мережі. У 2016 році міжнародна хакерська група «Анонім» здійснила напади на підозрюваних членів ІДІЛ у темній мережі, розмістивши контактну інформацію для своїх членів (адреси електронної пошти в соціальних мережах) та поверхневі веб-сайти своїх прихильників, зокрема «Ісламська держава» (@ nashirislamicstateEN). Анонімні атаки на ІДІЛ продовжувались і в 2019 році, коли більше соціальних медіа та особиста інформація члена Даїш / ІДІЛ обмінювалася між багатьма сервісами глибокої веб-пасти.

Такі незалежні націлювання на терористів у темній мережі продовжуються, і вміст, опублікований наприкінці вересня 2019 року, детально описує можливі координати геолокації підозрюваного лідера ІДІЛ Абу Бакра аль-Багдаді. Темний веб-пост закрився написом "ENJOY CIA",

ніби тоді така інформація може бути використана для оперативного націлювання розвідувальним співтовариством США. Абу Бакр аль-Багдаді був убитий в операції спецназу під проводом США рівно через місяць після розміщення інформації в темній мережі. Координати, вклеєні в темну павутину, не співвідносяться з Ідлібом, місцем розташування комплексу лідера ІДІЛ та подальшою смертю з боку сил безпеки США.

В умовах триваючих конфліктів проти тероризму в таких країнах, як Сирія, Ірак, Афганістан, Ємен та сектор Газа, кількість "розколених" груп зростає , особливо з урахуванням недавніх розрахованих атак, які Туреччина проводила проти курдів вздовж сирійсько-турецького кордону. На Tor існують різні зображення, включаючи відеозаписи відстрілів голови та страт, які проводили в Ємені солдати ІДІЛ. Такі конфлікти змусили більшість терористів, пов'язаних з ІДІЛ, перейти на зашифровані протоколи зв'язку, такі як WhatsApp та Telegram. Глибокий веб-допис від липня 2019 року також натякнув на те, що вербування ІДІЛ навіть відбувалося в приватних каналах Discord; Discord - це власна платформа комунікацій VoIP, яку підтримують спільнота відеоігор та глибокі веб-злочинці.[69]

Після придбання Facebook популярного мобільного додатка WhatsApp відбувся злагоджений рух до мобільного додатку Telegram. ISIS на Telegram зростає в популярності із регулярними відео, зображеннями, посиланнями та пропагандистським контентом, незважаючи на уявлення громади, що Telegram суворо ставиться до публікацій про дитячу порнографію та терористичний контент.

- США

США мають чималу робочу силу, навички, фінанси та міжнародний вплив. Загальна кількість кібервійськів, зайнятих у США, становить близько десятків, можливо сотень тисяч, завдяки недавньому від'єднанню Американського кіберкомандування (КІБЕРКОМ) від АНБ [70] та створенню пов'язаних з ним відділів Міністерства оборони (МО), таких як кіберармія (ARCYBER) та ВМС FCC (Кіберкомандування флоту). США також

лідирують у розвитку технічних навичок та міжнародному впливі, очолюючи численні глобальні кібер-ініціативи як у темряві, так і над поверхнею. Цього тижня громадськість дізналася, що США звернулись за допомогою до Чорногорії, залучивши елітну кібергрупу для співпраці та координації з метою прогнозування неминучого впливу Росії на президентські вибори в США 2020 року.

- Китай

Китай широко використовує глибоку мережу для шпигунства та збору розвідувальних даних. Поки Китай блокує використання Tor для своїх громадян, уряд регулярно використовує анонімність цієї технології для свого вдосконаленого підрозділу НОАК 61398 [71] для орієнтації на військові оборонні технології США та інтелектуальну власність. Китай також досить кмітливий, щоб визначити ключових військових підрядників оборонної промисловості для цілеспрямованих мережевих атак для збору конструкцій, документів та адміністративних деталей критично важливих технологій, контрольованих експортом. Цього літа були виявлені хакери, що базуються в Китаї, що керують широкомасштабною кампанією шпигунства у клітинкахнацілена на 10 різних операторів мобільного зв'язку по всьому світу. Реалізований доступ може бути використаний для здійснення майбутньої широкомасштабної атаки на стільниковий телефон та інфраструктуру даних. Розгорнута кампанія могла бути організована як помста за триваючі глобальні перегони озброєнь 5G та жорсткі реакції США на китайського постачальника телекомунікаційних послуг, Huawei, обмежуючи діяльність із розвитку 5G на Заході. З 2015 року підрозділ 78020, що фінансується державою, також бере участь у широкомасштабному військовому, політичному та економічному шпигунстві в багатому ресурсами районі Південно-Китайського моря. Розроблена шпигунська кампанія включає складну мережеву мережу ресурсів, включаючи IP-адреси, розташовані в Денвері, штат Колорадо, згідно з поглибленим звітом розвідки, опублікованим Threat Connect, Inc.

- Росія

Як видно з численних зауважень ЗМІ та ФБР за останні роки, російський уряд та спецслужби глибоко проникли в темну павутину, проводячи численні масштабні кампанії національних держав проти цілей у всьому світі. Атаки регулярно включають США та їх західних союзників у те, що можна було сприймати як повну кібервійну, демонструючи широкий спектр передових технічних кібер-можливостей. Дослідники Міністерства оборонної кіберстратегії намагаються визначити точну кількість кібер-спеціалістів, доступних для російських кібер-кампаній, але є повідомлення про низку елітних спеціальних підрозділів хакерського злому., в тому числі 26165 та його сестринський підрозділ 74455, пов'язаний з хакерством проти Національної конвенції Демократичної Республіки та детальною хакерською кампанією ГРУ для впливу на вибори в США. Росія також сумно відома своїм використанням кібер-довірених осіб, наймаючи прогресивні неурядові кіберзлочинні організації, які проводять теракти від їх імені.

- Ізраїль

Ізраїль є надзвичайно закритим і впливовим актором національної держави. Підрозділ 8200, елітна організація кібершпигунів Ізраїлю, порівнянна з АНБ з більш цілеспрямованою та продуманою оперативною програмою. Підрозділ 8200 доповнено низкою інших високотехнологічних підрозділів із ізраїльськими силами оборони (ІДФ). Конфліктні джерела повідомлень вислизають від потенційного спеціального ізраїльського кіберкомандування, але ці можливості могли бути розподілені між різними підрозділами телекомунікацій ІДФ в даний час. Колишній персонал підрозділу 8200 також був найнятий ізраїльськими кіберкорпораціями для здійснення спонсорованої Ізраїлем негласної діяльності у темних веб-операціях, що вимагає більшої юридичної свободи та меншої міжнародної перевірки.

- Німеччина

Німеччина, Великобританія та Франція мають ускладнені кібернетичні можливості. Нещодавно Німеччина створила власне Командування кібер- та інформаційного простору (CIR) із понад 13 000 співробітників, призначених для запобігання атакам втручання в мережі та кампаніям дезінформації. Правоохоронні органи Німеччини також займають лідируючі позиції у сфері темних веб-мереж на державному рівні, беручи активну участь у знищенні кількох відомих криптомаркетів та продавців наркотиків за останні роки.

- Великобританія

Недавні повідомлення про те, що хакери з Великобританії проникли в російську групу "Турла", підкреслюють витонченість можливостей Великобританії. GHCQ[66] удвічі збільшив свої можливості з 2014 року, надаючи можливості повного спектру від тактичних до найвищих кінцевих наступальних кібер операцій. Зважаючи на те, що NHS Великобританії є основною жертвою WannaCry[62] у 2017 році, Великобританія має можливість не тільки захищатись від майбутніх атак, але й контратакувати за необхідності.

- Україна

Спочатку Україну не вважали видатним актором національної держави. Раніше кібер-можливості України були зосереджені навколо організованої злочинності та темної спільноти веб-кардингу. З огляду на найновіші повідомлення в ЗМІ, в яких висвітлюються українські уряди та бізнесмени, що їх цікавлять, та їхній вплив на виборчу політику США, «вплив» України на міжнародній арені є помітним. Цей "вплив", в поєднанні з постійною війною України з Росією за анексію Криму, включаючи захист від російської кібератаки на українську електроенергетичну інфраструктуру, ставить Україну до перших 10 державних акторів в кібердомені. Розгляд України в останню хвилину також демонструє, наскільки швидко та різко можуть змінитися умови в цьому середовищі.

- Франція

На початку 2019 року Франція опублікувала свою нову французьку військову кібер-стратегію, що складається з двох окремих документів: Міністерської політики щодо оборонної кібервійни (далі - Міністерська політика) та Публічних елементів доктрини військової кібервійни (далі - Публічні елементи). Франція має значний вплив в організаціях ЄС та НАТО, компенсуючи те, чого їй не вистачає в людському капіталі.

- Іран

Іран лідирує в країнах Близького Сходу (крім Ізраїлю) як головний кібер-учасник національної держави. Кіберармія Ірану вже більше десятиліття є грізною загрозою для цілей різноманітних західних оборонних та комерційних мереж. Після того, як Сполучені Штати успішно проникли та зупинили свою систему ядерних центрифуг за допомогою вірусу Stuxnet, Іран вклав значні кошти у розвиток навичок та ресурсів, щоб забезпечити себе на міжнародній кібер-сцені. Вони також активно працюють у "проксі" конфігурації, де співпрацюють з іншими меншими національними державами для обміну технологіями та ресурсами. За оцінками, будь-яка кібератака на рівні національної держави з боку Ірану може бути здійснена за допомогою таких країн, як Північна Корея, Сирія та Ємен.

Також відомо, що Іран змовляється з терористичними організаціями, такими як "Хезболла" та приватними хакерськими групами. Навчаючи приватних хакерів і грубих терористів, можливо, без чітких вказівок та оперативних меж, Іран міг би стати ключовим у організації наступної глобальної кібервійни.

- Північна Корея

Північна Корея взяла на себе відповідальність за низку широкомасштабних атак на міжнародну хлібопекарську інфраструктуру у відповідь на міжнародні економічні санкції, накладені на них за опір припиненню ядерних програм. Згідно з повідомленнями розвідки з відкритим кодом, північнокорейські хакери успішно розгорнули нову шкідливу програму банкоматів під назвою ATMDTrack, яка реєструє та краде

банківські дані з карток, вставлених у вразливі банкомати в Індії. Оцінюється, що ATMDTrack[61] є компонентом набагато більшого сімейства шкідливих програм DTrack, що включає не тільки програмне забезпечення троянських команд і управління віддаленим доступом (RAT), але і кейлоггінг, отримання історії браузера, збір IP-адрес хостів, інформацію про доступні мережі та активні з'єднання, перелік усі запущені процеси та перерахування всіх файлів на всіх доступних дискових томах машини-жертви.

- Індія

У 2018 році Індія створила Національну організацію технічних досліджень як головне відомство для захисту національної критичної інфраструктури та для врегулювання всіх випадків кібербезпеки у критично важливих секторах країни. Окрім кібератак з боку Пакистану, Індія стикається з атаками інших ключових зловмисних акторів національних держав, як уже згадувалося вище, атак Північної Кореї на банківську інфраструктуру Індії. Недавні конфлікти в Кашмірі посилюють потребу в захисній позиції з боку пильних хакерів, які підтримують народ Кашміру.

- Канада

У 2018 році Канада ухвалила всеохоплюючий законодавчий орган, щоб надати Канаді Службу безпеки в галузі зв'язку (CSE) для ефективних наступальних кібер операцій. Широкий законопроект C-59 позиціонує CSE (канадську АНБ) на більш "активну кібер" позицію , на відміну від попередньої оборонної та реактивної позиції. Законодавство закликає CSE " здійснювати діяльність на глобальній інформаційній інфраструктурі або через неї з метою погіршення стану, порушення, впливу, реагування або втручання у можливості, наміри або діяльність іноземної особи, держави, організації або терористичної групи, коли вони стосуються до міжнародних справ, оборони або безпеки ". Канада не буде самотньою на світовій арені в кібер-галузі, але матиме ресурси та підтримку парламенту для впливу,

захисту та захисту канадської інфраструктури від нападів національних держав.

3.2 Порівняльний аналіз правової бази протидії кіберзлочиності на прикладі України та США

Сьогодні, в умовах глобалізації, інтелектуалізації злочинності, охоплення інформатизацією всіх суспільних відносин, міжнародна спільнота усвідомлює необхідність удосконалення чинних і розробки уніфікованих нормативно-правових актів щодо регулювання міжнародної інформаційної безпеки. Однією з важливіших умов побудови в Україні суспільства сталого розвитку, згідно з вимогами ЮНЕСКО, є створення відкритого інформаційного суспільства. Але реалізація ідей інформаційного суспільства як наслідку цифрової революції, на шляху до євроатлантичної інтеграції України, можлива лише за умов забезпечення сталої системи забезпечення інформаційної безпеки. Ефективність, сталість і захищеність державного інформаційного простору є важливим чинником надійного забезпечення національної безпеки, передумовою переходу українського суспільства на більш високу ступінь сталого розвитку. Інформаційно-телекомунікаційна складова стає одним із найважливіших елементів інформаційної безпеки суспільства і держави. Телекомунікаційні технологій підвищують ефективність управління силами оборони, бойові можливості техніки і озброєння. Але, поряд з якісними позитивними зрушеннями, розвиток цифрового світу зумовив виникнення нових небезпек, поширення випадків незаконного збирання, зберігання, використання, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність набула транснаціонального характеру та здатності завдати значної шкоди інтересам особи, суспільства і держави. На погляд дослідників і експертів, кіберпростір залишається критично слабкою складовою національної безпеки та зберігає певний ступінь уразливості до кіберзагроз.

Об’єктами кібератак і кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Джерелом таких загроз стають іноземні спеціальні структури, організовані злочинні хакерські групи, терористичні та екстремістські організації. В умовах проведення операції об’єднаних сил, розв’язання проблеми вдосконалення національної системи кібербезпеки, надійного захисту національного кіберпростору, постає найактуальнішим завданням теорії і практики державотворення.

Отже, необхідність побудови сталої та надійної системи забезпечення кібербезпеки України в умовах інтернаціоналізації кіберзлочинності, розповсюдження кібертероризму та інформаційної експансії в кіберпросторі, в першу чергу, потребує з’ясування теоретичних засад її відокремлення від системи інформаційної безпеки України як підсистемного утворення

Активне зростання кіберзагроз в сучасному суспільстві ставить перед кожною державою надзвичайно актуальне завдання - необхідність забезпечення інформаційної безпеки. Світова щорічна оцінка стану даного виду злочинності, викликає побоювання у зв'язку з низьким рівнем захищеності громадян сучасного інформаційного суспільства, при цьому спектр проблем досить широкий - від технічної незахищеності до уразливості систем забезпечення роботи, призначених для проведення операцій з грошовими коштами. Не дивлячись на те, що вивчення даної проблеми ведеться не одне десятиліття, тим не менш не досить повно сформовано поняття покарання, що дозволяє широко «розгортатися» злочинним угрупуванням.[42]

Кіберзлочинність визначається як злочин, який вчиняється за допомогою підключеного до мережі пристрою, такого як комп’ютер або мобільний телефон. Ті, хто здійснює кіберзлочини , відомі як кіберзлочинці або кібер-шахраї. Зі зростаючою цифровізацією злочини в Інтернеті також зростають швидшими темпами.

У вузькому сенсі «комп'ютерна злочинність» являє собою сукупність злочинів, де в якості безпосереднього основного об'єкта злочинного посягання виступають охоронювані законом суспільні відносини в сфері безпечного створення, зберігання, обробки і передачі комп'ютерної інформації, а предметом злочину є комп'ютерна інформація, засоби захисту комп'ютерної інформації, інформаційно-телекомунікаційні мережі, засоби зберігання, обробки і передачі комп'ютерної інформації ». У широкому сенсі визначення «комп'ютерна злочинність» дається наступне трактування: «комп'ютерна злочинність являє собою сукупність злочинів, де основним безпосереднім об'єктом злочинного зазіхання виступають суспільні відносини в сфері комп'ютерної інформації та інформаційних технологій, безпечного функціонування засобів створення, зберігання, обробки, передачі, захисту комп'ютерної інформації, але при цьому комп'ютерна інформація, інформаційно-телекомунікаційні мережі; засоби створення, зберігання, обробки, передачі комп'ютерної інформації (комп'ютери, смартфони, айфони, касові апарати, банкомати, платіжні термінали та інші комп'ютерні пристрої) є не тільки предметами злочинного діяння, а й використовуються як засіб і знаряддя вчинення злочину.

Кіберзлочинність для України є порівняльно новим видом злочинності. На сьогоднішній день в Україні є низка нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави.[42]

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету

Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.[43]

Сучасний світ вже не перший рік говорить про можливість ведення бойових дій у кіберпросторі. Це сталося після 2010 року, коли на прикладі Ірану світ побачив, що шкідливе програмне забезпечення може мати значний вплив на реальність і зупинити процеси, що відбуваються в реальному світі. На даний момент розроблено навіть положення про те, як повинні відбуватися ці кібер-конфронтації та про те, які правила мають відбуватися (маються на увазі теоретичні розробки, викладені в першому та другому Таллінських посібниках).

В Україні процес правового регулювання забезпечення кібербезпеки країни є саме цим питанням, яке почало досліджуватись досить пізно у 2015 році, коли була прийнята Стратегія кібербезпеки України. Розробка питань, що регулюються цією Стратегією, здійснювалась у ряді законів та інших нормативно-правових актів. Але, на жаль, чинне законодавче регулювання не дає відповіді на багато питань, з якими може зіткнутися українське суспільство у сфері домінування інформаційних технологій та Інтернету речей. З 2014 року Україна перебуває у стані збройного конфлікту з агресором - Російською Федерацією. За ці роки українська армія навчилася стабільно захищати кордони та стримувати атаку агресора, але є нове, поки невідоме поле бою - кіберпростір. У зв'язку з цим питання про те, як протистояти будь-якому агресору в кіберпросторі, є актуальним і потребує вивчення.

Ще зовсім недавно в Україні не було всеосяжного спеціального закону про кібербезпеку. Поки кіберзлочинність процвітала в Україні вже багато років, розвиток стійкої політики кібербезпеки відставав. Українське законодавство щодо боротьби зі злочинністю в кіберпросторі лише частково задовольняло потреби країни і не завжди охоплювало ключові елементи, необхідні для забезпечення ефективності. Таким чином, до жовтня 2017 року законодавча база в цій галузі включала наступні загальні законодавчі акти:

- Закон України Про Державну службу спеціального зв’язку та захисту інформації України від 23 лютого 2006 року No 3475-IV;
- Закон України "Про захист інформації в телекомунікаційних системах" No 80/94-ВР від 5 липня 1994 року;
- Закон України Про інформацію No 2657-XII від 2 жовтня 1992 року;
- Закон України Про телекомунікації No 1280-IV від 18 листопада 2003 р .;
- Закон України "Про державну таємницю" No 3855-XII від 21 січня 1994 року;
- Закон України «Про захист персональних даних» No2297-VI від 1 червня 2010 року; і
- Кримінальний кодекс України No 2341-III від 5 квітня 2001 року.

Також парламент України ратифікував Будапештську конвенцію про кіберзлочинність (Будапештська конвенція) ще в 2006 році.[43]

Забезпечення кібербезпеки в Україні ґрунтується на принципах:

- верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;
- забезпечення національних інтересів України;
- відкритості, доступності, стабільності та захищеності кіберпростору, розвиткок мережі Інтернет та відповідальних дій у кіберпросторі;
- державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;
- пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист

відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

- пріоритетності запобіжних заходів;
- невідворотності покарання за вчинення кіберзлочинів;
- пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
- міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;
- забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

На даний час законопроекти відпрацьовуються фахівцями зацікавлених органів (СБУ, МВС, НБУ, МО, ДССЗЗІ та інші), якими у тому числі пропонуються термін «кіберзлочин» узгодити із положенням України про кримінальну відповідальність. Законопроект № 2133а розроблено у зв'язку з необхідністю підвищення ефективності заходів спрямованих на протидію кіберзлочинності. У ньому пропонується внести зміни до низки законодавчих актів, а також запропоновано внести терміни «кіберпростір» та «кібербезпека» до закону України «Про основи національної безпеки».[43]

Основою кіберзлочинів, згідно чинного законодавства України є передбачені Кримінальним кодексом України суспільно небезпечні діяння і закріпленні в окремому Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинів відносяться тільки злочини, передбачені розділом XVI КК України, а в рамках криміналістики доцільно включити до даного поняття інші злочини, для скоєння яких застосовується

комп’ютер та використовується Інтернет. Проте у розділі зовсім відсутні поняття пов’язані з кібербезпекою, натоміть є лише деякі поняття злочинів, які вчиняються за допомогою електронно-обчислюваних машин (комп’ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв’язку.

Розділ складається з трьох статей:

- ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв’язку»;
- ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
- ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерів), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації»;
- ст. 362 «Викрадання, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем»;
- ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем»;
- ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку».[44]

З розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» та законопроектом «Про основні засади забезпечення кібербезпеки України» одним з військових формувань, яке займається питаннями кібербезпеки є

Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язок).

Закони та положення про кібербезпеку - США висвітлює загальні питання в законах та нормативних актах про кібербезпеку, включаючи кіберзлочинність, чинне законодавство, запобігання атакам, конкретні сектори, корпоративне управління, судовий процес, страхування та слідчі та поліцейські повноваження у 26 юрисдикціях.

Федеральний Закон про комп’ютерне шахрайство та зловживання “CFAA”, 18 USC § 1030, є основним законодавчим механізмом переслідування кіберзлочинності, і він передбачає як кримінальне, так і цивільне покарання. CFAA забороняє: [78]

- несанкціонований доступ (або перевищення дозволеного доступу) до комп'ютера та отримання інформації про національну безпеку;
- несанкціонований доступ (або перевищення дозволеного доступу) до комп’ютера, який використовується в міждержавній або іноземній торгівлі, та отримання інформації;
- несанкціонований доступ до непублічного комп’ютера, що використовується урядом США;
- свідомий доступ до захищеного комп’ютера без дозволу з метою обману;
- пошкодження комп’ютера навмисно або необдумано;
- торгівля паролями;
- передача погрози вимагання, зокрема погрози пошкодити захищений комп’ютер та погрози отримання інформації або компрометації конфіденційності інформації;
- кібер-вимагання, пов'язане з вимогами грошей або майна.

Залежно від конкретного правопорушення, покарання може становити від одного до 20 років ув'язнення.

Інші відповідні закони включають Закон про захист електронних комунікацій “Закон про захист електронних комунікацій”, який передбачає захист засобів зв'язку у місцях зберігання та транзиті. Відповідно до Закону про збережений зв’язок (Розділ II ЄКПА), 18 USC § 2702, передбачається кримінальне порушення навмисного доступу без дозволу (або перевищення дозволеного доступу) до об’єкта, що надає послугу електронного зв’язку („ECS”), який може включають, серед інших, постачальників послуг електронної пошти або навіть роботодавців, які надають адреси електронної пошти своїм працівникам. Персональні комп’ютери не вважаються засобами, що забезпечують ECS. За порушення передбачено покарання від одного року до перших порушень без неналежної мети (тобто порушень, не вчинених з комерційною перевагою, спричинити зловмисне знищення або пошкодження тощо) до 10 років за повторні порушення з неналежною метою.[78]

Навмисне перехоплення електронних комунікацій під час транзиту заборонено Законом про підслуховування (Розділ I ЄСПЗ), 18 USC § 2511, за винятком правоохоронних органів, деяких постачальників послуг та інших у тому числі, потенційно роботодавців. Покарання за порушення може передбачати позбавлення волі на строк до п’яти років.

На додаток до федеральних законів, численні штати прийняли закони, що забороняють злом та інші комп'ютерні злочини, деякі з яких є ширшими, ніж федеральний закон. Наприклад, Нью-Йорк забороняє навчитися користуватися комп’ютером з наміром отримати доступ до комп’ютерних матеріалів (комп’ютерний проступ),

Закон про кримінальне право Нью-Йорка, § 156.10, із штрафами до чотирьох років позбавлення волі та знати несанкціоноване використання комп’ютера ,

Закон про кримінальну відповідальність штату Нью-Йорк, § 156.05, 156.20 та наступні. , із покаранням різного діапазону до 15 років позбавлення волі, залежно від тяжкості правопорушення.

Специфікація, який закон застосовується, залежить від кількох факторів. Хакерство може порушити, серед інших статутів, CFAA, 18 USC § 1030 (a)

- інформація про національну безпеку, позбавлення волі на строк до 10 років,
- отримання інформації, позбавлення волі на термін до одного року або п’ять, якщо обтяжує ситуацію) чинники,
- державні комп’ютери, позбавлення волі до одного року та
- доступ до шахрайства, позбавлення волі до п’яти років.

Численні федеральні та державні закони включають вимоги щодо кібербезпеки. Федеральна торгова комісія «FTC» проявляла особливу активність у цьому напрямку та тлумачила свої повноваження щодо виконання закону відповідно до 5 (a) Закону про FTC, застосовуючи несправедливі та оманливі практики, як засіб вимагати від компаній вжиття заходів безпеки. Починаючи з 2002 року, FTC розпочав понад 80 заходів щодо примусового виконання рішень щодо компаній, які, за її твердженнями, не здійснили розумні заходи безпеки. Закон про обмін інформацією про кібербезпеку «CISA» має два основних наслідки.

По-перше, це дозволяє компаніям контролювати мережевий трафік, включаючи вжиття захисних заходів у власних системах.

По-друге, це заохочує обмін інформацією про кіберзагрози між компаніями та урядом. Однак деякі федеральні закони є галузевими або поширюються лише на державні компанії.

Наприклад, Закон Гремма-Ліча-Блілі «GLBA» та його імплементаційні норми вимагають від "фінансових установ" застосовувати письмові політики та процедури, які "розумно розроблені" для забезпечення безпеки та конфіденційності записів клієнтів та захисту від очікуваних погрози та несанкціонований доступ та використання.[80] Закон про переносимість медичної страховки та відповідальність за їх відповідальність «HIPAA» [81] включає вимоги щодо кібербезпеки, що застосовуються до

охоронюваної медичної інформації, якою володіють певні «охоплені організації» та їх «ділові партнери».

На державному рівні кілька штатів прийняли закони, що встановлюють вимоги безпеки. Більшість із цих статутів вимагають певної форми «розумної безпеки». Правила штату Массачусетс встановлюють особливі вимоги до безпеки компаній, які володіють або мають ліцензію на особисту інформацію, включаючи реалізацію письмової програми безпеки та шифрування даних при транзиті через загальнодоступні мережі та на всіх портативних пристроях. [78]

Нещодавно Нью-Йорк ухвалив Закон про ЩИТ, який вимагає розумної безпеки особистої інформації та визначає конкретні заходи, які можуть відповідати цьому стандарту. Закон про конфіденційність споживачів у Каліфорнії створює право на порушення даних щодо жителів Каліфорнії із встановленими законом штрафами від 100 до 750 доларів США за споживача та за інцидент, якщо позивачі докажуть, що зазначений бізнес не здійснив та не підтримував розумні процедури безпеки та практики, що відповідають характеру інформації, для захисту особистої інформації.

Закон про Агентство з питань кібербезпеки та безпеки інфраструктури створив CISA, що входить до складу Міністерства національної безпеки, і федеральне відомство, відповідальне за захист критичної інфраструктури в США. CISA координує між урядом та організаціями приватного сектору щодо захисту критичної інфраструктури. Федеральний уряд видав спеціальні вказівки для операторів критичної інфраструктури, а атомна, хімічна, електрична, державна підрядна організація, транспорт та інші галузі мають детальні статутні та нормативні вимоги.

Закони США про кібербезпеку існують як на федеральному рівні, так і на рівні штатів і різняться залежно від комерційного сектору. Наприклад, кілька федеральних законів мають положення про повідомлення про порушення даних, але кожен штат і чотири території також мають закони про порушення даних. Багато регуляторів очікують, що регульовані компанії

запровадили «розумні» заходи безпеки з урахуванням таких факторів, як чутливість захищених даних. У світлі розповсюдження стандартів багато компаній покладаються на загальноосвітні системи кібербезпеки, такі як NIST Cybersecurity Framework[82], що рекомендує компаніям вживати заходів для виявлення та оцінки суттєвих передбачуваних ризиків (у тому числі з постачальниками), розробляти та впроваджувати політику та засоби контролю для організації у світлі цих ризиків відстежуйте та виявляйте аномалії та реалізовані ризики, оперативно та адекватно реагуйте на інциденти, а потім оживайте від будь-якого інциденту. На додаток до загальних розумних вимог безпеки, деякі закони США набагато більш припустимі. Наприклад, положення штату Массачусетс щодо кібербезпеки та Нью-Йоркський закон про ЩИТ містять детальні вимоги щодо захисту інформації на рівні штату, а департамент фінансових послуг Нью-Йорка (який регулює такі організації, як банки та страхові компанії) має додаткові додаткові вимоги.

Усі штати та чотири території мають вимоги щодо повідомлення про інциденти, і більшість із цих статутів вимагають звітування перед державними регуляторами. Характер та обсяг інформації, яку потрібно повідомляти, різниться залежно від держави чи території. Наприклад, штат Массачусетс вимагає, щоб організації, що повідомляють про порушення державним регуляторам, повинні містити інформацію про:

- характер порушень безпеки або несанкціоноване придбання чи використання;
- кількість жителів штату Массачусетс, що постраждали від інциденту;
- кроки вжиті для усунення інциденту;
- назва організації, яка повідомляє та зазнала порушення;
- відповідальна особа, якщо вона відома;
- тип персональної інформації, яка потенційно може бути скомпрометована;

- чи зберігала організація письмова програма інформаційної безпеки, як того вимагають правила штату Массачусетс, та чи оновлює організація цю програму у відповідь на інцидент.

Ці державні вимоги доповнюють федеральні вимоги, що стосуються конкретних галузей. Наприклад, Управління з питань цивільних прав Міністерства охорони здоров'я та соціальних служб «HHS» вимагає від охоплених організацій та бізнес-партнерів повідомляти про певні випадки, пов'язані із захищеною інформацією про здоров'я «PH». Часові рамки складання звітів залежать від штату чи установи, і більшість з них вимагає повідомлення приблизно в той самий час, коли особи отримують повідомлення. Вермонт вимагає надсилання будь-якого повідомлення своєму Генеральному прокурору протягом 15 днів. Фінансові установи, що охоплюються, зобов’язані повідомити про порушення у Нью-Йоркському департаменті фінансових послуг протягом 72 годин. Однак на запит правоохоронних органів деякі повідомлення можуть затримуватися.[78]

Інформація про кіберзагрози, як правило, не повинна повідомлятися, хоча федеральний уряд заохочує участь у Центрах обміну та аналізі інформації або Організаціях обміну та аналізі інформації, де інформація про загрози обмінюється в межах сектору групи компаній.

Усі 50 штатів США та чотири території прийняли статут повідомлень про порушення з різними вимогами. Звичайно, статути повідомлень про порушення вимагають надсилання повідомлень особам, чия електронна Персональна інформація, як визначено в ній, була отримана в результаті інциденту, хоча деякі держави вимагають повідомлення лише на основі доступу до такої інформації. Державні визначення Особистої інформації, що ініціюють повідомлення про порушення даних, як правило, застосовуються до імені або першого початкового та прізвища в поєднанні з іншим ідентифікатором, коли вони не зашифровані або не відредаговані, наприклад, номер соціального страхування, номер посвідчення водія чи ідентифікаційної картки або номер рахунку, або номер кредитної картки або дебетової картки

в поєднанні з будь-яким необхідним кодом безпеки, кодом доступу або паролем, що дозволить отримати доступ до облікового запису особи.

Все частіше, Штати також включають у визначення Особистої інформації інформацію про здоров'я та біометричну інформацію, а також імена користувачів та паролі, що забезпечують доступ до онлайнового облікового запису. Багато штатів також вимагають надсилати повідомлення генеральним прокурорам або іншим державним установам, часто залежно від кількості осіб, які зазнали впливу. Більшість штатів дозволяють врахувати, чи існує ризик заподіяння шкоди суб'єктам даних, але деякі штати не дозволяють такого розгляду. Часові рамки сповіщення залежать від штату; однак 30 днів - загальноприйнятий стандарт.Крім того, деякі секторні закони передбачають вимоги щодо сповіщення. Правило HIPAA про повідомлення про порушення, 45 CFR §§ 164.400–414, вимагає від суб’єктів господарювання та ділових партнерів, що охоплюються HIPAA, подавати повідомлення у разі виникнення певних інцидентів, що впливають на ІМЗ.[81]

3.3 Кібербезпека та інформаційна безпека в інтернеті: практичні рекомендації

У сучасному світі, де організації комерційної, фінансової, медичних, переробних і енергетичних сфері, в тому числі всі урядові структури - організовують збір, зберігання і обробку всієї необхідної в роботі інформації, а також персональні дані співробітників, користувачів, клієнтів і відвідувачів. В основному вся ця інформація потребує захисту, оскільки є конфіденційною, а втрати води в системі її, втрати або розкрадання можуть мати непередбачувані (негативні) наслідки для людей і організацій (держав).

Інформаційна безпека - це набір інструментів та практик, які можна використовувати для захисту цифрової та аналогової інформації. InfoSec охоплює цілий ряд IT-доменів, включаючи безпеку інфраструктури та мережі, аудит та тестування. Він використовує такі інструменти, як

автентифікація та дозволи, щоб обмежити несанкціонованим користувачам доступ до приватної інформації. Ці заходи допомагають запобігти шкоді, пов’язаній з крадіжкою інформації, її зміною або втратою.[32]

Кібербезпека - це практика захисту комп’ютерів, серверів, мобільних пристроїв, електронних систем, мереж та даних від зловмисних атак. Це також відомо як безпека інформаційних технологій або електронна інформаційна безпека. Цей термін застосовується в різних контекстах - від бізнесу до мобільних обчислень, і його можна розділити на кілька загальних категорій:[33]

- Мережева безпека - це практика захисту комп’ютерної мережі від зловмисників, будь то цільові зловмисники чи умовно-шкідливі програми.[55]
- Безпека програм зосереджена на захисті програмного забезпечення та пристроїв від загроз. Компрометована програма може надати доступ до даних, які вона призначена для захисту. Успішна безпека починається на стадії проектування, задовго до розгортання програми чи пристрою.
- Інформаційна безпека захищає цілісність і конфіденційність даних як при зберіганні, так і під час передачі.
- Операційна безпека включає процеси та рішення щодо обробки та захисту активів даних. Дозволи, які користувачі мають при доступі до мережі, і процедури, що визначають, як і де дані можуть зберігатися або ділитися всіма, потрапляють під цю парасольку.
- Відновлення після катастрофи та безперервність бізнесу визначають, як організація реагує на інцидент з кібербезпекою або будь-яку іншу подію, що спричиняє втрату операцій або даних. Політика відновлення після стихійних лих диктує, як організація відновлює свою діяльність та інформацію, щоб повернутися до тієї ж робочої потужності, що і до події. Безперервність бізнесу - це план, на якому організація відмовляється, намагаючись працювати без певних ресурсів.

- Навчання кінцевих користувачів стосується найбільш непередбачуваного фактора кібербезпеки: людей. Будь-хто може випадково ввести вірус в іншу безпечну систему, не дотримуючись належних практик безпеки. Навчити користувачів видаляти підозрілі вкладення електронної пошти, не підключати невідомі USB-накопичувачі та різні інші важливі уроки є життєво важливим для безпеки будь-якої організації.

Хоча кібербезпека та інформаційна безпека охоплюють різні цілі та сфери застосування з деяким перекриттям. Інформаційна безпека - це ширша категорія захисту, яка охоплює криптографію, мобільні обчислення та соціальні медіа. Це пов’язано із забезпеченням інформації, що використовується для захисту інформації від несуспільних загроз, таких як відмови серверів або стихійні лиха. Для порівняння, кібербезпека охоплює лише Інтернет-загрози та цифрові дані. Крім того, кібербезпека забезпечує покриття необроблених, некласифікованих даних, тоді як інформаційна безпека цього не робить.[27]

Інтернет-безпека складається з ряду тактик безпеки для захисту діяльності та транзакцій, що проводяться в Інтернеті через Інтернет. Ця тактика призначена для захисту користувачів від загроз, таких як злом комп’ютерних систем, електронних адрес або веб-сайтів; шкідливе програмне забезпечення, яке може заразити та по суті пошкодити системи; та викрадення особистих даних хакерами, які викрадають особисті дані, такі як дані банківських рахунків та номери кредитних карток. Інтернет-безпека є специфічним аспектом більш широких концепцій, таких як кібербезпека та комп'ютерна безпека, зосереджена на конкретних загрозах та вразливостях Інтернет-доступу та використання Інтернету. У сучасному цифровому середовищі багато наших щоденних дій покладаються на Інтернет. Різні форми спілкування, розваги, а також фінансові та робочі завдання виконуються в Інтернеті. Це означає, що тони даних та конфіденційної інформації постійно передаються через Інтернет. Інтернет в основному є приватним та безпечним, але він також може бути небезпечним каналом для

обміну інформацією. З високим ризиком вторгнення з боку хакерів та кіберзлочинців, безпека Інтернету є головним пріоритетом як для приватних осіб, так і для бізнесу.[27]

Незважаючи на те, що Інтернет представляє користувачам багато інформації та послуг, він також включає кілька ризиків. Кібератаки лише збільшуються у вишуканості та обсязі, оскільки багато кіберзлочинці використовують комбінацію різних типів атак для досягнення однієї мети. Незважаючи на те, що перелік потенційних загроз великий, ось декілька найпоширеніших загроз безпеці в Інтернеті:

Шкідливе програмне забезпечення - скорочення від "зловмисне програмне забезпечення", шкідливе програмне забезпечення має кілька видів, включаючи комп'ютерні віруси, хробаків, троянські програми та нечесне шпигунське програмне забезпечення.[31]

Комп’ютерний хробак - це програма, яка копіює себе з одного комп’ютера на інший. Для створення цих копій не потрібна взаємодія людини, і вона може поширюватися швидко та у великих обсягах.[29]

Спам - це небажані повідомлення у вашій поштовій скриньці. У деяких випадках спам може просто включати небажану пошту, яка рекламує товари чи послуги, які вас не цікавлять. Зазвичай вони вважаються нешкідливими, але деякі можуть містити посилання, які встановлюватимуть шкідливе програмне забезпечення на ваш комп’ютер, якщо на них натискатимуть.[28]

Фішинг - шахрайство створюється кіберзлочинцями, які намагаються отримати приватну або конфіденційну інформацію. Вони можуть виступати за ваш банк або веб-службу і заманювати вас на клацання посилань, щоб перевірити деталі, такі як інформація про рахунок або паролі.[30]

Ботнет - це мережа приватних комп’ютерів, які були скомпрометовані. Заражені шкідливим програмним забезпеченням, ці комп’ютери контролюються одним користувачем, і їх часто спонукають

брати участь у таких недоброзичливих діях, як відправлення спаму чи атаки на відмову в обслуговуванні DoS.[20]

Інтернет-безпека вимагає поєднання декількох продуктів та технологій для належного захисту даних. Важливо враховувати кілька типів стратегій безпеки в Інтернеті, коли вживаєте належних заходів, щоб захистити свою мережу.[87] Ці тактики можуть включати:

- Вибір браузера: Кожен браузер має власні заходи безпеки, але деякі можуть мати серйозні недоліки, які дозволяють хакерам та кіберзлочинцям експлуатувати та вторгуватися. Переконайтеся, що ви використовуєте захищений веб-переглядач, щоб зменшити ризик пошкодження комп'ютера чи мережі.
- Багатофакторна автентифікація MFA: MFA - це метод контролю доступу до комп'ютера, який вимагає декількох окремих доказів для механізму автентифікації. Веб-сайти та облікові записи електронної пошти можна зробити більш безпечними, вимагаючи принаймні двох факторів автентифікації користувача.[54]
- Безпека електронної пошти: Електронна пошта створює хвилю можливостей для вірусів, хробаків, троянських програм та інших небажаних програм. Встановлення багатошарової та всебічної стратегії безпеки електронної пошти допоможе значно зменшити вплив нових загроз. Повідомлення електронної пошти також можна захистити за допомогою криптографії, наприклад підписання електронного листа, зашифрування тіла повідомлення електронної пошти та зашифрування зв'язку між поштовими серверами.[60]
- Брандмауери: Брандмауери діють як фільтри, що захищають пристрої, дозволяючи або забороняючи доступ до мережі. Застосовуючи конкретний набір правил, щоб визначити, чи є щось безпечним чи шкідливим, брандмауери можуть запобігти викраденню конфіденційної інформації та утримати зловмисний код у мережах.[27]

Кібербезпека постійно розвивається, що може ускладнити постійне оновлення інформації. Залишатися в курсі уваги та бути обережними в Інтернеті - це два найкращих способи захистити себе, свої мережі та пристрої та свій бізнес.[95]

1. Використовуйте лише довірені сайти, надаючи свою особисту інформацію. Хорошим правилом є перевірка URL-адреси. Якщо сайт містить «https: //», то це безпечний сайт. Якщо URL-адреса містить «http: //», - зауважте відсутні «s» - уникайте введення конфіденційної інформації, наприклад даних вашої кредитної картки або номера соціального страхування.

2. Не відкривайте вкладення електронної пошти та не клацайте посилання в електронних листах з невідомих джерел. Одним з найпоширеніших способів впливу мереж та користувачів на зловмисне програмне забезпечення та віруси є електронні листи, замасковані як відправлені кимось, кому ви довіряєте.

3. Завжди оновлюйте свої пристрої. Оновлення програмного забезпечення містять важливі виправлення для усунення вразливостей системи безпеки. Кібер-зловмисники також можуть націлювати застарілі пристрої, на яких може не працювати найновіше програмне забезпечення безпеки.

4. Регулярно створюйте резервні копії своїх файлів для додаткового захисту в разі атак кібербезпеки. Якщо вам потрібно очистити пристрій від кібератаки, це допоможе зберігати ваші файли в безпечному, окремому місці.

Поки тактика кіберзахисту розвивається, розвивається і загроза кібербезпеки, зловмисне програмне забезпечення та інші загрози набувають нових форм. І загрози кібербезпеки не дискримінують. Усі особи та організації, які використовують мережі, є потенційними цілями. Щоб захистити себе, важливо знати три різні типи загроз кібербезпеці: кіберзлочинність, кібератаки та кібертероризм.[35]

- Кіберзлочинність здійснюється однією або кількома особами, які націлені на вашу систему, щоб спричинити хаос або заради отримання фінансової вигоди.
- Кібератаки часто здійснюються з політичних причин і можуть бути призначені для збору та поширення вашої конфіденційної інформації.
- Кібертероризм призначений для порушення електронних систем, щоб вселити паніку і страх у своїх жертв.

У міру дедалі більшої залежності від технологій стає все більш важливим забезпечення кожного аспекту онлайн-інформації та даних. У міру зростання Інтернету та збільшення комп'ютерних мереж.[36]

Попереджувальні заходи, які ви можете вжити для запобігання фінансовим наслідкам або викраденню особистої інформації:

1. Утримайтеся від введення конфіденційної інформації на загальнодоступних комп'ютерах.
2. Бережіть паролі та часто їх міняйте.
3. Ніколи не надсилайте по електронній пошті конфіденційну інформацію, таку як номери соціального страхування, номери кредитних карток або банківських рахунків та дані водійських прав.
4. Тримайтеся подалі від незахищених сайтів, таких як ті, що не мають захищеного рівня сокета (SSL), особливо якщо сайт продає товари та послуги або запитує фінансову інформацію.
5. Ви можете перевірити, чи використовує веб-сайт SSL-сертифікат, переглянувши URL-адресу веб-сайту. Якщо він починається з «https» замість «http», це означає, що сайт захищений за допомогою сертифіката SSL («s» означає безпечний).
6. Не відповідайте на небажані повідомлення електронної пошти.
7. Переконайтесь, що ви знаєте всіх одержувачів, коли відповідаєте на повідомлення електронної пошти або надсилаєте його.
8. Використовуйте подарункові картки або інші безпечні способи оплати, не прикріплені до вашого банківського рахунку.

9. Використовуйте обчислювальні та веб-переглядачі, які мають поточний захист від зловмисного програмного забезпечення та брандмауер.

10. Утримайтеся від публікації особистої інформації в соціальних мережах.[79]

Безпека мережі - це один з найважливіших аспектів, який слід враховувати при роботі через Інтернет, локальну мережу чи іншим способом. Хоча немає мережі, яка захищена від атак, стабільна та ефективна система мережевої безпеки має важливе значення для захисту даних. Хороша система мережевої безпеки допомагає зменшити ризик стати жертвою викрадення та саботажу даних. Безпека мережі допомагає захистити ваші робочі станції від шкідливого шпигунського програмного забезпечення. Це також гарантує захист спільних даних. Інфраструктура мережевої безпеки забезпечує кілька рівнів захисту для запобігання атакам MiM , розбиваючи інформацію на численні частини, шифруючи ці частини та передаючи їх незалежними шляхами, таким чином запобігаючи таким випадкам, як прослуховування.[36]

ВИСНОВКИ

Darknet - це спеціальна прихована сетьінтернет-з'єднань, яка має захищене з'єднання, що встановлюються між довіреними бенкетами і дозволяє анонімно обмінюватися інформацією і файлами.

Особлива риса ресурсу - це анонімність. Цей ресурс часто застосовують у випадках, коли потрібно додати секретну інформацію, здобувати нелегальний товар або контент. У цій мережі так здійснюється будь-яка незаконна діяльність. Darknet є некомерційної мережею і пов'язаний з «підпільним» спілкуванням і технологіями. Більшість звичайних користувачів пов'язують Darknet з DeepWeb. DeepWeb - це явище, яке описує безліч веб-сторінок, які не скануються пошуковою системою.

В межах дослідження була поставлена загальна мета – дослідити сутність використання мережі Даркнет в міжнародно-політичних процесах, а також визначити особливості використання мережі Даркнет як інструменту криміналізації політичного процесу, що було здійснено шляхом вивчення:

по-перше, історії винекнення та особливловостей мережі Даркнет, сутності та змісту цього явища, його класифікації на види, його ролі та значення в сучасному світі;

по-друге, сутності та принципу роботи Даркнет, особливості роботи програмного забеспечення та інструментів, інформаційних злочинів політичнго характеру;

по-третє, особливостей розвитку та правової бази протидії кіберзлочиності в Україні та США, впливу Даркнет на міжнародні політичні процеси, кібербезпеки та інформаційної безпеки в інтернеті.

У дипломній роботі було висвітлено теоретичні підходи до визначення мережі Darknet, його етапи становлення як інструменту криміналізації політичного процесу та основні складові.

Стрімкий розвиток технологій, розвиток інформаційних технологій і широке використання інтернету привели до революційних змін у всіх сферах

повсякденної діяльності, в процесі виробництва, в торгівлі, освіті, розвагах і, навіть, способах мислення сучасної людини. Поряд з цими змінами, які в цілому поліпшили якість нашого життя, з'явилися умови, які сприяють розвитку нових форм злочинності.

У результаті проведеного дослідження, підтвердилась думка про те, що держави використовують темну мережу для збору розвідувальних даних та розробки джерел, урядового та корпоративного шпигунства, експлуатації та тестування, операцій з дезінформації для геополітичного впливу, порушення інфраструктури та отримання фінансової вигоди.

Результатами дослідження встановлено, що активісти і революціонери давно використовують DarkNet для самоорганізації, не побоюючись відкрити свою позицію уряду, проти якого вони виступають. Зрозуміло, це означає, що з тих же причин DarkNet використовується терористами, екстремістами і іншими небажаними організаціями та угрупуваннями. Будь-яка людина може отримати доступ до прихованого сегменту Інтернету дуже легко. Існує безліч сумнівних матеріалів, а також велика кількість злочинців.

Хакерство виникло і розвивалося протягом багатьох років як спосіб соціального протесту і відходу від реального світу в світ кіберпростору. Якщо раніше хакери були затребувані як професіонали в області інформаційних технологій, що допомагають вирішити проблеми з інформаційними системами, то в останні роки хакерство все більше йде в бік кібертероризму. Хакери, як явище офіційно вважається поза законом, але фактично це одна з рушійних сил нашого суспільства по шляху науково-технічного прогресу.

Завдяки тісній співпраці хакерів між собою і інформаційної відкритості і безкорисливості в процесі творчої діяльності, відбувається удосконалення програмного забезпечення та широке впровадження їх досягнень у повсякденну практику користувачів.

Розглянуті принципи відкритої моделі, цінності свободи, культ творчості дозволяють виділити хакерської співтовариство як значущу і

соціально безпечну групу, на відміну від фрікерові кібертерористів, які переступають закон, діють антисоціально і вводять в оману інших, зараховуючи себе до товариства хакерів. Таким чином, хакери, як члени організованого співтовариства, чия діяльність спрямована на розвиток інформаційного суспільства (як з технічної, так і з соціального боку), абсолютно не співвідносяться з тими характеристиками, якими їх наділяють засоби масової інформації.

Було встановлено, що мережа DarkNet широко використовується серед журналістів та політичних блогерів, особливо тих, хто живе в країнах, де жорстка цензура і тюремне ув'язнення в якості покарання за її порушення є звичайним явищем. Інтернет-анонімність дозволяє цим людям, а також інформаторам спілкуватися з джерелами і вільно публікувати інформацію, не побоюючись покарання. Така ж анонімність може використовуватися читачами новин для доступу до інформації на поверхневій мережі, яка зазвичай блокується національними брандмауерами.

Інтернет має багато таємниць і невідомості. Їли звичайні люди користуються з "світлої" частиною, то існує його "темна" частина, які забезпечую анонімність дій і повну свободу в мережі. Найчастіше люди проникають в DarkNet через своєї цікавості, але деякі мають на меті пов'язані з кіберзлочинністю. Тому звичайні користувачі заходять в DarkNet на свій страх і ризик. Однак проникнути на цю "темну" сторону не так, то просто, доступ можливий тільки через спеціальні браузери, що забезпечують анонімність. Однак маленький шанс стеження є, можливість бути розкритим підвищується, якщо робити необдумані дії.

У ході дослідження було визначено, що глобальний тероризм, який часто підживлюється фінансово та політично окремими державами, має непередбачуваний та часто реактивний слід у темній павутині, що реагує на геополітичні події та політику, а також на зміну технологій. Адаптивність терористів змушує їх переходити від темної павутини до наскрізних зашифрованих власних протоколів, таких як Whatsapp та Telegram, де вони

можуть набирати, розробляти стратегії та розповсюджувати пропаганду анонімно.

На підставі проведеного дослідження, можна зробити наступні висновки, що Darknet є інстрементом криміналізації політичного процесу та його все частіше використовують як інформаційне поле бою для різноманітних ключових розвідувальних та кібер-військових кампаній.

Отже, завдання виконані у повному обсязі, мета досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. History of the dark web. *Standard Office Systems:* веб-сайт. URL: https://www.soscanhelp.com/blog/history-of-the-dark-web (дата звернення 20.09.2020)
2. Darknet. *SearchNetworking:* веб-сайт. URL: https://searchnetworking.techtarget.com/definition/darknet (дата звернення 20.09.2020)
3. Історія Інтернету. *Internet Society*: веб-сайт. URL: https://www.internetsociety.org/internet/history internet (дата звернення 20.09.2020)
4. Інтернет. *OpenMinds Authors*: веб-сайт. URL: https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/ (дата звернення 20.09.2020)
5. Tor браузер. *TechTarget:* веб-сайт. URL: https://whatis.techtarget.com/definition/TOR-third-generation-onion-routing (дата звернення 20.09.2020)
6. Tor. *Investopedia:*веб сайт. URL: https://www.investopedia.com/terms/t/tor.asp (дата звернення 20.09.2020)
7. BitMassage. *Bitmessage Wiki:* веб-сайт. URL: https://bitmessage.org/ (дата звернення 20.09.2020)
8. Keepassx. *Офіційна веб-сторінка Keepassx:* веб-сайт. URL: https://www.keepassx.org/ (дата звернення 20.09.2020)
9. Bitcoin. *Технічний словник для студентів, викладачів та IT-спеціалістів:* веб-сайт.URL: https://www.webopedia.com/TERM/B/bitcoin.html (дата звернення 20.09.2020)
10. Bitcoin mixers. *Bitcoin magazine*: веб-сайт. URL: https://bitcoinmagazine.com/what-is-bitcoin/what-are-bitcoin-mixers (дата звернення 20.09.2020)

11. Інтернет та політичні організації. *Parliament of Australia:* веб-сайт. URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/RP9798/98RP11#INTRO (дата звернення 10.10. 2020)

12. Еволюція Інтернету. *Журнал кіберполітика*: веб-сайт. URL: https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1157619?src=recsys (дата звернення 10.10.2020)

13. Кіберзлочиність. *Офіційна веб-сторінка Kaspersky*: веб-сайт. URL: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (дата звернення 10.10.2020)

14. Fake news. *Цифровий путівник IONOS:* веб-сайт. URL: https://www.ionos.com/digitalguide/online-marketing/social-media/what-is-fake-news/ (дата звернення 10.10.2020)

15. Віртуальна приватна мережа. *Norton:* веб-сайт. URL: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html (дата звернення 10.10.2020)

16. Суспільно-політична сфера життя. *Файловий архів студентів:* веб-сайт. URL: https://studfile.net/preview/5650512/page:51/ (дата звернення 10.10.2020)

17. Вплив Інтернету на суспільство. *OpenMinds Authors*: веб-сайт. URL: https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective/ (дата звернення 10.10.2020)

18. Блокчейн. *Techterms*: веб-сайт. URL: https://techterms.com/definition/blockchain (дата звернення 10.10.2020)

19. Hidden Wiki. *Інформаціний портал:* веб-сайт. URL: https://www.eyerys.com/articles/timeline/hidden-wiki -a (дата звернення 10.10.2020)

20. Ботнет. *Інформаціний портал Akamai*: веб-сайт. URL:https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp (дата звернення 10.10.2020)

21. I2P. *Techopedia:* веб-сайт. URL: https://www.techopedia.com/definition/24966/i2p (дата звернення 10.10.2020)

22. Darknet та Darkweb. *Techslang technology awareness platform:* веб-сайт. URL: https://www.techslang.com/definition/what-is-the-darknet/ (дата звернення 10.10.2020)

23. Telegram. *JustAskThales digital world site:* веб-сайт. URL: https://justaskthales.com/en/telegram-different-messaging-apps/ (дата звернення 10.10.2020)

24. Telegram замінить TOR і даркнет. *Популярна Механіка:* веб-сайт. URL: https://www.popmech.ru/technologies/news-546834-telegram-zamenit-tor-i-darknet-novyy-funkcional-ton-sites/ (дата звернення 12.10.2020)

25. Принцип роботи TON. *Bitcoin wikipedia:* веб-сайт. URL: https://ru.bitcoinwiki.org/wiki/TON (дата звернення 12.10.2020)

26. Криптовалюта. *Federal Trade Commission:* веб-сайт. URL: https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency (дата звернення 12.10.2020)

27. Інтернет-безпека. *Mcafee:* веб-сайт. URL: https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-internet-security.html (дата звернення 12.10.2020)

28. Спам. *Eset internet security*: веб-сайт. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/spam/ (дата звернення 12.10.2020)

29. Комп'ютерний хробак. *Indevlab:* веб-сайт. URL: https://indevlab.com/uk/blog-ua/virusi-troyani-ta-hrobaki-shho-tse-take-i-yak-vberegti-svoyu-tehniku/ / (дата звернення 12.10.2020)

30. Фішинг веб-сайт. *Інформаційний портал:* URL: https://ua.godaddy.com/help/sho-take-fishing-346 (дата звернення 15.10.2020)

31. Шкідливе програмне забезпечення. *Online система дистанційної підтримки навчання:* веб-сайт.URL: https://disted.edu.vn.ua/courses/learn/12421 (дата звернення 15.10.2020)

32. Інформаційа безпека. *Інформаційний портал Exabeam:* веб-сайт. URL: https://www.exabeam.com/information security/information security/ (дата звернення 15.10.2020)

33. Кібербезпека. веб-сайт. *Офіційна веб-сторінка Kaspersky*: URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (дата звернення 15.10.2020)

34. Кібербезпека визначення. *Довідник студентський*: веб-сайт. URL: https://spravochnick.ru/informacionnaya_bezopasnost/kiberbezopasnost_i_informacionnaya_bezopasnost/ (дата звернення 15.10.2020)

35. Кібербезпека. Як захистити себе. *Norton:* веб-сайт. URL: https://us.norton.com/internetsecurity malware what is cybersecuriy-what-you-need-to-know.html (дата звернення 15.10.2020)

36. Важливість мережевої безпеки. *Ecpi University:* веб-сайт. URL: https://www.ecpi.edu/blog/importance-of-network-security-safety-in-the-digital-world (дата звернення 15.10.2020)

37. Історія інтернету: ARPANET. *IT-новини*. 17.06.2019: веб-сайт. URL: https://habr.com/ru/post/456200/ (дата звернення 16.10.2020)

38. Freenet. *Онлайн енциклопедія*: веб-сайт. URL: https://www.pcmag.com/encyclopedia/term/freenet (дата звернення 16.10.2020)

39. Freepto. веб-сайт. *Онлайн блог.* 12.03.2017: URL: https://www.loudtechie.com/7-best-alternatives-to-tor-browser-for-anonymous-browsing/ (дата звернення 16.10.2020)

40. Темна мережа. *Hackware news:* веб-сайт. URL: https://hackwarenews.com/the-dark-web-a-history-lesson/ (дата звернення 16.10.2020)

41. Сатоші Накомото. *Bitcoin wiki:* веб-сайт. URL: https://ru.bitcoinwiki.org/wiki (дата звернення 16.10.2020)

42. Визначення кіберзлочинність. *Наукова електронна бібліотека «КіберЛенінка»:* веб-сайт. URL: https://cyberleninka.ru/article/n/opredelenie pon

yatiya kiberprestuplenie-otdelnye-vidy-kiberprestupleniy/viewer (дата звернення 16.10.2020)

43. Про основні засади забезпечення кібербезпеки України. *Верховна Рада України. Законодавство України*: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 16.10.2020)

44. Кримінальний кодекс України. Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – Відомості Верховної Ради (ВВР) – 2001. – №25-26, ст. 131. *Верховна Рада України. Законодавство України*: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 16.10.2020)

45. Соціальна бажаність. *Україномовна енциклопедія*: веб-сайт. URL: http://enc.com.ua/velika-psixologichna-enciklopediya/e-vo-zaik/101409-socialnabazhanist.html (дата звернення 16.10.2020)

46. Фреймінг новин. *Файловий архів студентів:* веб-сайт. URL: https://studfile.net/preview/8098842/page:2/ (дата звернення 16.10.2020)

47. Лідери громодської думки. *Інтернет видання про маркетинг і технології:* веб-сайт. URL: https://marketer.ua/ua/who-are-the-opinion-leaders/ (дата звернення 16.10.2020)

48. Як формується громадська думка. *Lumen Learning:* веб-сайт. URL: https://courses.lumenlearning.com/boundlesspoliticalscience/chapter/forming-public-opinion/ (дата звернення 18.10.2020)

49. Соціальні мережі. *Business Data Platform*: веб-сайт. URL: https://www.statista.com/topics/1164/socialnetworks/#dossierSummary__chapter1 (дата звернення 16.10.2020)

50. Злочини у сфері інформаційних технологій. *Інформаційно-аналітична газета:* вебсайт. URL: http://www.rupor.gr/2016/11/26/prestupleniya-v-sfere-informacionnyx-texnologij/ (дата звернення 16.10.2020)

51. DDos визначення. *Imperva cybersecurity:* веб-сайт. URL: https://www.imperva.com/learn/ddos/denial-of-service/ (дата звернення 16.10.2020)

52. Cybercriminals are turning to Telegram due to its security capabilities. *Internet security*: веб-сайт. URL: https://www.helpnetsecurity.com/2018/05/08/telegram-cybercriminals/ (дата звернення 18.10.2020)

53. Криптовалюта Gram. *Группа однодумців TON:* веб-сайт. URL: https://www.gramston.com/ (дата звернення 18.10.2020)

54. Багатофакторна автентифікація. *Захист вашого бізнесу в інтернет*і*:* веб-сайт. URL: https://datami.ua/uk/shho-take-mfa-bagatofaktorna-autentifikatsiya/ (дата звернення 18.10.2020)

55. Мережева безпека. *Sibis:* веб-сайт. URL: https://www.sibis.com.ua/ua/services/sybersecurity/network-security/ (дата звернення 18.10.2020)

56. Кібертерроризм. *Файловий архів студентів:* веб-сайт. URL: https://studfile.net/preview/15921398/page:23/

57. Хактивізм. *Securitylab:* веб-сайт. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/348956.php (дата звернення 20.10.2020)

58. Інформаційні технології. *Apes Departament of Igor Sikorsky KPI*: веб-сайт. URL: http://apeps.kpi.ua/shcho-take-informatsiini-technologii/en (дата звернення 20.10.2020)

59. Darknet. *Techopedia*: веб-сайт. URL: https://www.techopedia.com/definition/2395/darknet (дата звернення 20.10.2020)

60. Безпека електроной пошти. *Zillya антивірус:* веб-сайт. URL: https://zillya.ua/bezpeka-elektronno-poshti (дата звернення 20.10.2020)

61. ATMDtrack. *Хакерські новини:* веб-сайт. URL: https://xakep.ru/2019/09/24/dtrack/

62. Вірус. WannaCry. *Інформаційний портал:* веб-сайт. URL: https://www.ferra.ru/review/apps/all-about-wannacry.htm (дата звернення 20.10.2020)

63. ІДІЛ. *Інформаційний портал:* веб-сайт. URL: https://www.lustrum.com.ua/islamic-state/ (дата звернення 20.10.2020)

64. Актори національної держави. *Darknet experts:* веб-сайт. URL: https://www.darkowl.com/blog-content/nation-state-actors-on-the-darknet (дата звернення 20.10.2020)

65. Human intelligence HUMINT. *Wikipedia:* веб-сайт. URL: https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering) (дата звернення 20.10.2020)

66. Британська спецслужба GCHQ. *3dnews.* 29.09.2015: веб-сайт. URL: https://3dnews.ru/920875 (дата звернення 20.10.2020)

67. Шпигунська програма Pegasus. *Онлайн бізнес-газета.* 01.09.20: веб-сайт. URL: https://www.business-gazeta.ru/article/479436 (дата звернення 20.10.2020)

68. Хакерське угруповання Fancy Bear. *Wikipedia:* веб-сайт. URL: https://uk.wikipedia.org/wiki/Fancy_Bear (дата звернення 25.10.2020)

69. Discord. *Офіційна веб-сторінка:* веб-сайт. URL: https://discord.com/

70. Агенство Національної Безпеки США. *Securitylab:* веб-сайт. URL: https://www.securitylab.ru/news/tags/%D0%90% (дата звернення 25.10.2020)

71. Військовий підрозділ НОАК 61398. *Хакерські новини:* веб-сайт. URL: https://xakep.ru/2018/08/09/china-apt/ (дата звернення 25.10.2020)

72. Протокол №1 до Конвенції про кіберзлочинність. *Верховна Рада України. Законодавство України*: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/994_687 (дата звернення 25.10.2020)

73. TON DNS. *Telegram info*: веб-сайт. URL: https://tginfo.me/ton-dns/ (дата звернення 25.10.2020)

74. TCP. IT forum: веб-сайт. URL: https://www.opennet.ru/docs/RUS/linux_base/node350.html (дата звернення 25.10.2020)

75. Лідер думок. *Підручники для студентів онлайн:* веб-сайт. URL: https://stud.com.ua/64483/zhurnalistika/lideri_dumok (дата звернення 25.10.2020)

76. Блокчейн. *Інформаційний портал «Blockchaininfo»:* веб-сайт. URL: https://blockchain.info/ru/charts/market-price (дата звернення 25.10.2020)

77. Визначення Darknet. *Techopedia*: веб-сайт. URL: https://www.techopedia.com/definition/2395/darknet (дата звернення 30.10.2020)

78. США: Закони та положення про кібербезпеку 2021. *Провідна глобальна платформа для правових довідок, аналізу та новин:* веб-сайт. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (дата звернення 30.10.2020)

79. Як захистити особисту інформацію від Darknet. *веб-сайт.иІнформаційний портал:* URL: https://www.dnaindia.com/technology/report-dark-web-what-is-it-here-s-how-to-keep-personal-information-off-darknet-2855862 (дата звернення 30.10.2020)

80. Закон Гремма-Ліча-Бліл. *Investopedia.* 11.05.2020: веб-сайт. URL: https://www.investopedia.com/terms/g/glba.asp (дата звернення 30.10.2020)

81. Health Insurance Portability and Accountability Act. *Wikipedia:* веб-сайт. URL: https://uk.wikipedia.org/wiki/HIPAA (дата звернення 30.10.2020)

82. NIST. *Cybersecurity Framework*: веб-сайт. URL: https://www.nist.gov/cyberframework (дата звернення 30.10.2020)

83. Кібершпигунство визначення. *Everfi blog:* веб-сайт. URL: https://everfi.com/blog/workplace-training/cyber-espionage-3-important-facts-about-high-tech-spying/ (дата звернення 05.11.2020)

84. Дезінформація у ЗМІ. *Економічні новини24.* 22.01.2020: веб-сайт. URL: https://news.24tv.ua/vidpovidalnist_neugodnih_zhurnalistiv_y_utisk_s

vobodi_slova_shho_zminiti_v_novomu_proyekti_uryadu_n1267560 (дата звернення 05.11.2020)

85. Принцип роботи PayPal. *Офіційна веб сторінка PayPal:* веб-сайт. URL: https://www.paypal.com/ru/webapps/mpp/how-paypal-works (дата звернення 05.11.2020)

86. Віртуальний приватний сервер. *Techterms*: веб-сайт. URL: https://techterms.com/definition/vps (дата звернення 05.11.2020)

87. Інтернет безпека. *Профспілка працівників освіти і науки України:* веб-сайт. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html (дата звернення 05.11.2020)

88. TOR. *Офіційна веб сторінка TOR:* веб-сайт. URL: https://www.torproject.org/ (дата звернення 05.11.2020)

89. Майнери. *Економічні новини24.* 28.02.2018: веб-сайт. URL: https://economy.24tv.ua/ru/kto_takie_majnery_i_kak_zarabotat_na_kriptovaljute_n916426 (дата звернення 05.11.2020)

90. Internet of Things. *Лідер ринку складних IT-рішень:* веб-сайт. URL:https://www.it.ua/ru/knowledge-base/technology-innovation/internetveschej-internet-of-things-iot (дата звернення 11.11.2020)

91. DarkNet: темна сторона мережі. веб-сайт. *Аналітика, обзори, дослідження з світу Інформаційної безпеки*: URL: https://ipiskunov.blogspot.com/2016/08/darknet.html (дата звернення 11.11.2020)

92. Хакерство. Темна сторона інтернету веб-сайт. *Науковий форум:* URL: https://scienceforum.ru/2019/article/2018016083 (дата звернення 11.11.2020)

93. Інтернет та сучасне життя. *Eyerys*: веб-сайт. URL: https://www.eyerys.com/articles/news/internet-and-modern-life (дата звернення 11.11.2020)

94. Злочини у сфері інформаційних технологій. *Інформаційно-аналітична онлайн газета:* веб-сайт. URL:

http://www.rupor.gr/2016/11/26/prestupleniya-v-sfere-informacionnyx-texnologij/ (дата звернення 13.11.2020)

95. Кібербезпека відповідає політиці безпеки: Складні технології, фрагментована політика та мережева наука. *Taylor & Francis authors*: веб-сайт. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855 (дата звернення 13.11.2020)

96. Вплив кіберзлочинності та кібербезпеки на геополітику та націю. веб-сайт. *Інтернет блог:* URL: https://www.crowdstrike.com/blog/cybercrime-cybersecurity-affects-nations-geopolitics/ (дата звернення 13.11.2020)

97. Darknet словник. *VPNOverview:* веб-сайт. URL: https://vpnoverview.com/privacy/anonymous-browsing/dark-web-dictionary/ (дата звернення 13.11.2020)

98. Кібератаки на демократію. *The George W. Bush Presidential Library*: веб-сайт. URL: https://www.bushcenter.org/catalyst/democracy/zarate-cyberattacks-on-democracy.html (дата звернення 13.11.2020)

99. Політика DarkWeb. *Advanced Intelligence*: веб-сайт. URL: https://www.advanced-intel.com/post/darkweb-politics-cybercrime-meddling-threat-landscape (дата звернення 13.11.2020)

100. Вплив темної мережі на управління інтернетом та кібербеку. веб-сайт. *Global commission of interner governace:* URL: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf (дата звернення 13.11.2020)