СЕКЦІЯ 1

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.04

О. КУЗАН, Н. КУШНІРЕНКО

Національний університет "Одеська політехніка"

КІБЕРСТАЛКІНГ: ПРОБЛЕМИ ТА МЕТОДИ АВТОМАТИЧНОГО ВИЯВЛЕННЯ

Вступ. Швидкий розвиток інформаційних технологій зробив можливим зручне спілкування та обмін особистою інформацією в Інтернеті. Проте такі їх особливості як: низька вартість, простота використання, анонімність, відсутність нагляду та і в цілому безпрецедентний доступ до людей, який виходить за межі часових і географічних обмежень, сприяли поширенню різних форм кіберзлочинності та створили нові можливості для здійснення девіантної поведінки, як кіберсталкінг.

Ця кіберзлочинність має серйозний вплив на психологічний та фізичний стан мільйонів невинних жертв і становить вагому соціальну та правову проблему як в нашій країні, так і в цілому світі. Суспільство все ще шукає шляхи ефективної боротьби з кіберсталкінгом.

Через недостатньо швидкий розвиток нашого законодавства щодо сфери комп'ютерних технологій ми отримуємо ситуацію, коли злочинці діють безкарно. Складність збирання доказів кіберсталкінга заважає отриманню допомоги від кіберполіції; відсутність законодавчого визначення навіть самого поняття "кіберсталкінг", не кажучи навіть про визначення механізмів протидії, позбавляє жертв можливості отримати належну допомогу.

Тож актуальною є потреба в розробці та вдосконаленні правової бази, а також в розробці технічних засобів виявлення кіберсталкінга для ефективної боротьби з цією злочинністю.

Мета: дослідити явище кіберсталкінгу та технічні методи його виявлення.

1. Поняття кіберсталкінгу

Кіберсталкінг - це вид правопорушення в кіберпросторі, безперервний процес кібератак, який передбачає переслідування людини в мережі з агресивним та/або сексуальним підтекстом, і включає в себе досить широкий спектр небажаної поведінки:

- поширення неправдивих обвинувачень в Інтернеті;
- плітки й наклеп;
- прямі й непрямі погрози;
- образливі повідомлення;
- тролінг і доксинг;
- сексистські висловлювання, тощо.

Такі дії спрямовані на те, щоб завдати шкоди, поставити під загрозу або втрутитися в особисте життя жертви.

Переслідування включає саме повторювані інциденти, які окремо можуть бути навіть і нешкідливими діями, але в сукупності підривають відчуття безпеки особи і викликають дистрес, страх і тривогу [1].

Мотивація кіберсталкерів ділиться на:

- задоволення своєї психологічної потреби, бажання або тяги до іншої людини (наприклад, нав'язлива зацікавленість до когось, бажання висміювати, дражнити задарма);
- вселити страх жертві або встановити над нею контроль;
- бажання помститися або покарати жертву; встановлення стосунків з жертвою (включаючи сексуальні відносини).

Кіберсталкерами можуть бути будь-хто, навіть просто угруповання тих, хто робить це задля розваги. Так і жертвою, на жаль, може стати кожна людина. Злочинці практично не мають обмежень щодо віку, статі, сімейного стану, сексуальної орієнтації чи етнічної приналежності. Хоча все ж таки, за статистикою, жертвами переслідувань стають переважно жінки. Саме тому, кіберсталкінг вважається основною складовою для іншого поняття - кібернасильства над жінками.

Згідно з типологією Лерой МакФерлейн і Пола Босіча, існує чотири основні типи кіберсталкерів [1]:

- Мстивий кіберсталкер - це один із найбільш агресивних типів переслідувачів. Вони часто погрожують жертвам і здійснюють напади частіше, ніж інші типи. Метою їхніх дій є постійне завдання шкоди жертвам через спам, крадіжку особистих даних тощо. Зазвичай вони мають середні або високі навички роботи з комп'ютером, а також можливі психічні відхилення, що виявляються у тривожному контенті, який вони надсилають.
- Стриманий кіберсталкер діє спокійно і не демонструє агресії відкрито. Його мета - викликати у жертви постійний стрес через загрозливі дії, такі як погрози насильства. Ці переслідувачі, як правило, не виходять з тіні, залишаючись невидимими. Серед них також можуть бути люди з психічними розладами.
- Інтимний кіберсталкер намагається встановити емоційний зв'язок із жертвою через одержимість або захоплення. Вони можуть використовувати електронну пошту, чати чи сайти знайомств, щоб добитися взаємної уваги. Якщо жертва відмовляє, ці сталкери часто стають агресивними.
- Колективний кіберсталкер - це група з кількох осіб, які переслідують одну жертву. У них, зазвичай, високий рівень комп'ютерних навичок порівняно з іншими типами кіберсталкерів.

З точки зору поведінкових стратегій існує три основні моделі кіберсталкінгу [2]:

- Таємний кіберсталкінг - переслідувач приховано спостерігає за жертвою, відстежуючи її оновлення без прямої взаємодії. Його дії, як правило, не завдають прямої шкоди і часто залишаються непомітними для жертви.
- Непрямий кіберсталкінг - включає такі дії, як пошкодження особистих даних чи обладнання жертви, крадіжку особистої інформації, створення фальшивих профілів або документів від імені жертви. Тут відсутній прямий контакт із жертвою, але дії можуть мати довгострокові наслідки, зокрема психологічну травму.

- Прямий кіберсталкінг - включає прямий зв'язок із жертвою, наприклад, через повідомлення чи коментарі. Може включати погрози, домагання, кібербуллінг, образи чи залякування. Цей тип переслідування завдає значної шкоди у різних сферах життя жертви: емоційній, психологічній, фінансовій або професійній.

Хоча, як можна побачити, кіберсталкери навмисно створюють умови морального, емоційного та психологічного страждання для жертви. На жаль, до цього часу національним законодавством України не розглядається сталкінг та кіберсталкінг як окремий вид правопорушень. Не створені механізми фіксації, підтвердження та збору доказів, а також захисту жертви.

Існують державні документи, як наприклад Стаття 32 Конституції України, що гарантує непорушність приватного життя [3], проте всі ці закони не дають правоохоронцям повноцінно покарати злочинців. Однак, з останніх подій, 2 жовтня 2024, група народних депутатів зареєструвала Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України Про запобігання та протидію домашньому насильству щодо встановлення відповідальності за злочинне переслідування (сталкінг), номер реєстрації 12088 [4]. Згідно з ним, було визначено термін сталкінг. Також пропонується ввести в законодавство новий термін - кіберпереслідування.

Отже, можна сказати, що не так швидко як би хотілося, але все ж таки, в правовому плані відбуваються позитивні зміни.

2. Методи виявлення та протидії

Незважаючи на визнання кіберсталкінга дуже серйозною і швидкозростаючою проблемою, це явище все ще є недостатньо вивченим, особливо з боку технічного виявлення та запобігання. Максимально вживаною і в той же час найменш ефективною тактикою жертв для запобігання переслідуванням є ігнорування або уникнення. І виникає ця стратегія через банальну необізнаність, що робити в даній ситуації. А необхідно перш за все заспокоїтися і почати збирати докази.

Саме для виявлення фактів кіберсталкінга і збору доказів можна використовувати технічні засоби як наприклад методи машинного навчання, дата майнінгу, статистичні методи та інші технології, такі як криптографія, біометрія, комп'ютерний зір і цифрова криміналістика.

Машинне навчання часто використовується для виявлення кіберсталкінгу, оскільки дозволяє автоматизувати процес аналізу даних та знаходити закономірності серед великого обсягу інформації. Основні техніки тут включають:

- нейронні мережі;
- глибинне навчання;
- нечітку логіку.

ML-системи можуть працювати безперервно, оперативно виявляючи загрози. Вони ефективно обробляють великі обсяги даних, що дозволяє використовувати їх у соціальних мережах з мільйонами користувачів та електронній пошті [5].

І звичайно, головним плюсом є здатність навчатися на нових даних і вдосконалювати точність виявлення загроз. В свою чергу, дата майнінг - це більш ручний цикл, який залежить від людського посередництва та керівництва. Так як основна мета тут - це виявлення прихованих сигнатур або закономірностей у великих масивах даних, це процес, який залежить від попередньо встановлених критеріїв і правил. В цьому випадку експерти задають параметри, аналізують отримані дані та на основі цього створюють інструкції для подальшого аналізу. Тож дата майнінг більше підходить для початкового аналізу великих обсягів даних.

Статистичні методи також можуть використовуватися для виявлення аномалій у поведінці користувачів, що можуть вказувати на кіберсталкінг. Деякі з цих методів включають:

- алгоритми виявлення відхилень, що допомагають визначити відхилення від норми, наприклад, якщо користувач починає значно частіше переглядати профіль певної людини або надсилати їй повідомлення;
- байєсівські мережі, які використовуються для ймовірнісного аналізу поведінки та дозволяють прогнозувати дії кіберсталкера на основі попередніх даних;
- приховані марковські моделі, які можуть моделювати послідовності поведінки та допомагають передбачити, чи є певна послідовність дій підозрілою.

Криптографія зазвичай допомагає аутентифікувати особу кіберсталкера, захищаючи дані жертв та забезпечуючи конфіденційність їхньої інформації.

Біометричні системи використовуються для розпізнавання осіб за зображеннями чи відео, що також може допомогти ідентифікувати кіберсталкерів. Комп'ютерний зір використовується для аналізу зображень, виявлення підроблених облікових записів або перевірки автентичності URL-адрес. Це може бути особливо корисним для перевірки фальшивих профілів чи підозрілих дій. І нарешті, цифрова криміналістика допомагає збирати цифрові докази, аналізувати електронну тінь, що може бути корисним для відстеження активності кіберсталкерів та збору доказів для подальших дій [5].

Продуктивність алгоритмів машинного навчання наразі перевершує всі інші способи виявлення кіберсталкінгу, але все ще є досить багато питань, які необхідно вирішити в цьому напрямі, тож необхідні дослідження.

Соціальні мережі та онлайн-додатки, такі як Twitter, Facebook, Youtube, Instagram, електронна пошта та інструменти для проведення онлайн-конференцій, часто використовуються кіберсталкерами за допомогою текстового та мультимедійного контенту. Серед них, імейл сталкінг все ще є найпоширенішим інструментом для переслідування, після нього - телефонний та сталкінг в соцмережах.

Більшість технічних підходів зосереджуються лише на фішингу, фільтрації пошти та класифікації спаму, але злочинці також переслідують жертв, використовуючи електронні листи, які не є спамом. Тож більше уваги та досліджень необхідні для виявлення кіберсталкінга через неспам повідомлення.

До того ж, в основному, існуючі проєкти зосереджені на контенті саме англійською мовою, що унеможливлює їх використання в україномовному середовищі. Виникає потреба в розробці системи виявлення кіберсталкінгу для

нашого кіберпростору, яка за допомогою фільтрації спама, неспама електронної пошти та автоматичного збору доказів, полегшить процес первинного розгляду скарг жертв для правоохоронних органів.

Крім того, вона заохочуватиме жертв звертатися зі скаргами для притягнення до відповідальності кіберсталкерів, а також забезпечить надання жертвам послуг та підтримки.

Висновок. Сучасні технології створили нову арену для сталкерів, додавши багато різновидів і способів займатися переслідуваннями. Неминучим наслідком відчуття анонімності в Інтернеті та слабкого реагування на кіберзлочини є те, що потенціал для кіберсталкінгу, із супутньою можливістю погроз, тривоги та страждань, наклепів та фізичної небезпеки, які йдуть пліч-о-пліч зі сталкінгом у реальному світі, збільшуватиметься ще більше.

А отже, щоб ситуація не погіршилася, необхідно приділити увагу цьому питанню на всіх рівнях: соціальному, правовому, академічному і звичайно технічному. Щоб нарешті була можливість у технічному збиранні та обміні доказами з кіберполіцією, а всіх винних було притягнуто до відповідальності.

Перелік використаних джерел.

1. McFarlane L. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers, L. McFarlane, P. Bocij, First Monday, 2003. URL:https://firstmonday.org/ojs/index.php/fm/article/view/1076/996

2. Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning, P.B. Lowry, J. Zhang, C. Wang та ін., International Conference on Systems Sciences. - 2013. [Електронний ресурс].- Режим доступу: https://www.researchgate.net/publication/268597303_Understanding_and_predicting_cyberstalking_in_social_media_Integrating_theoretical_perspectives_on_shame_neutralization_self-control_rational_choice_and_social_learning

3. Конституція України. [Електронний ресурс].- Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

4. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України Про запобігання та протидію домашньому насильству щодо встановлення відповідальності за злочинне переслідування (сталкінг). [Електронний ресурс].- Режим доступу: https://itd.rada.gov.ua/billInfo/Bills/Card/44972

5. Arvind Kumar Gautam, Abhishek Bansal, A Review on Cyberstalking Detection Using Machine Learning Techniques: Current Trends and Future Direction, International Journal of Engineering Trends and Technology, 2022.