Література

1. Днепр и коронавирус: одиноким пенсионерам привозят бесплатные пищевые наборы. URL: https://opentv.media/dnepr-i-koronavirus-odinokim-pensioneram-privozyat-besplatnye-pishhevye-nabory

2. «Мне ребенку надо молоко купить, а они мне — карантин»: в Днепре закрыли «Озерку». URL: https://dp.informator.ua/2020/03/20/mne-rebenku-nado-moloko-kupit-a-oni-mne-karantin-v-dnepre-zakryli-ozerku/; Куда вы все несетесь в 6 утра: зам мера Днепра обратился к людям пожилого возраста. URL: https:// nashemisto.dp.ua; В Днепре пенсионеры отказались выполнять меры карантина в трамвае: водителю пришлось вызвать полицию

3. URL: https://dp.informator.ua/2020/03/19/v-dnepre-pensionery-otkazalis-vypolnyat-mery-karantina-v-tramvae-voditelyu-p

4. Во Львове льготы на проезд для пенсионеров отменили до конца карантина URL:https://lb.ua/society/2020/03/19/453075_lvove_lgoti_proezd.html

5. Процких О. Ю. Інформаційна взаємодія Національної поліції України з органами публічної влади та громадськістю / О. Ю. Процких // Право і Безпека. - 2015. - № 4. - С. 50-55

Світличний Віталій Анатолійович
к.т.н., доцент, доцент кафедри
інформаційних технологій та кібербезпеки
Харківського національного університету
внутрішніх справ

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧА ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Однією з проблем з якою стикається працівник поліції при розслідувані злочинів, які були здійсненні через мережу Internet є визначення комп'ютера користувача з якого були здійснені кримінальні дії (кіберзлочини). Погрішність ідентифікації, заснованої на IP-адресі, складається з погрішностей передачі і погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через ргоху-сервер уся мережа, яка за ним ховається, у більшості випадків матиме єдиний IP-адрес. Завдання ідентифікації користувача не втрачає своєї актуальності в зв'язку постійною гонкою технологій захисту інформації і технологій неправомірного отримання доступу до інформації. Актуальність цього завдання для мережі Інтернет підвищується використанням незахищених каналів передачі даних.

Завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів таких як MAC або IP-адрес в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь на питання те ж цей пристрій або ні, але не повідомляє точний тип пристрою і спосіб його використання конкретним користувачем. Окрім ідентифікаторів, можливе використання додаткової інформації, яка затребувана у разі обробки непрямих

ознак, на підставі інформації отримуваної з датчиків пристрою і в результаті роботи програмного забезпечення на пристрої. В даному випадку мається на увазі визначення типу діяльності користувача за даними глобальних систем позиціонування і гіроскопа, а також застосування методів динамічної і статичної біометрії, таких як, рисунок вен на долоні, відбиток пальця, веселкова оболонка ока, геометрія кисті руки або особи, 3D-проекція черепа, клавіатурній почерк, форма вуха, голос і будь-яка інша відмітна ознака може служити для ідентифікації людини біометричною системою.

Використовуємо поняття відбиток пристрою, стосовно інформації що залишається на серверах і інших пристроїв реєстрації, а поняття відбиток особи в пристрої до інформації що побічно характеризує людину за інформацією що залишилася у використаному їм пристрої. Прикладом відбитку пристрою служить запис в log-файлі сервера, а відбитком особи інформація про використані програми, час і тривалість використання програм, набір використаних файлів і інших ресурсів.

Особливе місце серед програмного забезпечення з точки зору завдання ідентифікації пристрою займає браузер, як програма, за допомогою якої користувач дістає доступ до більшості Internet-ресурсів. Для ідентифікації використовується інформація cookies-файлів та інформація про встановлені шрифти і плагіни. Вирішуючи задачу ідентифікації з використанням непрямих ознак, слід враховувати швидкість зміни конфігурацій апаратного і версій програмного забезпечення вживаного користувачем, а так само біологічні ритми до яких схильна людина. Динамічні біометричні ознаки людини змінюються впродовж півроку. Статичні біометричні ознаки зберігаються упродовж усього життя.

Рішення задачі ідентифікації людини і пристрою використовуватиметься при реалізації концепції «програмний агент», для визначення психофізіологічного стану людини і в завданнях з області безпеки, для створення механізмів відстежування шляху. Ідентифікація пристрою і людини є проміжними цілями. Завдяки ідентифікації пристрою можливе калібрування методів знімання інформації. Кінцевою метою ідентифікації пристрою є ідентифікація людини, отримання прямої або непрямої інформації про нього.

Початковими даними для ідентифікації пристрою і людини пропонується вважати: інформацію про пристрій, інформацію про навколишній світ, інформацію про людину. Складність формалізації початкових даних полягає в неможливості побудови вичерпної безлічі значень деяких ознак. Інформація про використання клавіатури складається з коду клавіші, часу події, типу події. Проте формалізувати ознаку, пов’язану з граматичними і орфографічними помилками, що допускаються користувачем при наборі тексту, як мінімум, складно. Інформація про пристрій складається з: списку і конфігурації використовуваного апаратного забезпечення; списку і конфігурації встановлених програм, і, якщо це можливо, часу установки програм; інформації збереженої на облаштуванні користувача у вигляді

соокіев-файлів, інших тимчасових файлів; відбитку файлової системи пристрою.

Під відбитком файлової системи розуміється інформація про структуру файлової системи, а не отримання математичної свертки даних у файловій системі. Особлива увага приділяється файлам старше за місяць, в яких не відбувалося змін за цей час. Вони мають достатню стабільність, щоб на деякий час стати ідентифікуючою ознакою. Для створення відбитку файлової системи пропонується використовувати інформацію про їх ім'я, місце розташування, розмір, дату створення і дату редагування.

Інформація про користувача складається з: днів тижня, часу доби використання, тривалості активності програмного забезпечення; друкарських помилках, що повторюються, словах паразитах, помилках при наборі тексту; подіях миші або клавіатури.

Кінцевою метою дослідження завдання пошуку користувача мережі Internet і пристрої доступу є побудова системи розпізнавання, здатної з необхідною точністю здійснити процес ідентифікації. Перспективами подальших розробок у даному напрямку є дослідження способів ідентифікації злочинця, які використовують засоби анонімізації даних в мережі Інтернет, вивчення мережевих ідентифікаторів, які сприяють встановленню криміналістично значимої інформації, аналіз останніх наукових та технічних досягнень, спрямованих на ідентифікацію винних осіб, а також подальший аналіз способів дослідження особистості злочинця на підставі віртуальних слідів, залишених в глобальній мережі.

Бабенко Олександр Сергійович
babenko_as@ukr.net
курсант 3 курсу факультету №1
ДЮІ МВС України
Науковий керівник:
кандидат юридичних .наук,
завідувач кафедри спеціальної техніки та інформаційних технологій
ДЮІ МВС України
Тулінов Валентин Сергійович

ЗАГРОЗИ ІНТЕРНЕТ МЕРЕЖ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ ПОЛІЦІЇ

З кожним роком, користувачів інтернет мереж становиться все більше, разом с цим, також з'являються хакери, які користуються, вразливостями в програмах, сайтах, створюють шкідливі програми та інше, метою отримання доступу до баз даних, де зберігається особиста інформація, зі злочинною метою використання цих даних.