з DarkNet залишаються безкарними лише до тих пір, поки правоохоронні органи не починають приймати контрзаходи, які найчастіше бувають засновані не на новітніх технологіях машинного навчання, а на класичних методах розслідування.

Список використаних джерел:

1. Что такое Даркнет [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82.

2. Как ловят преступников в DarkNet [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/wirex/blog/400723/

Ключові слова: Даркнет, протидія, злочинці
Ключевые слова: Даркнет, противодействие, преступники
Keywords: Darknet, anti-action, criminals
***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Трєгубов Нікіта Олександрович
Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

МЕТОДЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ ПОЛЬЗОВАТЕЛЯ

Все мы сталкивались с небольшим оповещением на сайте о том, что надо принять «cookie» файлы, принять условия соглашения конфиденциальности, о сборе данных и так далее, и просто дальше пользовались сетью Интернет. Но задумывались ли вы на что именно соглашаетесь? Были ли у вас мысли что именно за данные вы отдаёте компаниям, чьими услугами вы пользуетесь?

Возьмем, например, компанию Google. Данная компания собирает данные обо всём что вы делаете, когда вы пользуетесь любым из предлагаемых продуктов или асоциированных

с нею. Почти каждый интернет-магазин асоциирован с маркетинговым продуктом Google – AdSense. Когда вы интересуетесь определенным товаром, то он обязательно когда-нибудь появится в рекламных блоках, интеграциях в видеороликах. Но почему так? Потому что вам уже был присвоен определенный рекламный идентефикатор [1]. Действует он ровно как личное дело или как история браузера. В нём накапливается список сайтов или товаров, которыми вы интересуетесь в данный момент либо интересовались. После чего на базе этого идентификатора алгоритм пытается предоставить в рекламе товары, имеющие наибольший шанс вас заинтересовать на определённый интернет-магазин, который выкупил рекламу. Такой технологией пользуется не только Google, но и другие гиганты IT-индустрии, но именно Google начала собирать данные о вашей геолокации и использовать её в маркетинговых целях. Никто вас не заставляет дальше давать информацию о ваших посещениях – вы можете без проблем выключить данную функцию сбора данных в вашем аккаунте Google.

Перейдем к социальным сетям, взяв за основной пример компанию Facebook. Представленная компания тщательно следит за своими пользователями используя огромное количество различных алгоритмов, а также устройства самих пользователей. Так, в 2017 году один из пользователей социальной сети уличил компанию в слежке на повседневной основе, воспользовавшись микрофоном смартфона для подслушивания бытовых разговоров вдали от телефона, обрабатывая полученные данные и выдавая соответствующую контекстную рекламу. Но недавно Facebook была замечена за продажей данных, использования в своих целях, а также в политической рекламе. Также в 2019 году данные сотен миллионов пользователей были опубликованы в открытом доступе, за что Facebook получил штраф в размере 5 миллиардов долларов США [2].

Допустим, мы можем отказаться от социальных сетей и найти альтернативу. Но что если даже ваша операционная система начинает следить за вашими действиями? Недолго

после выхода операционной системы Windows 10, стало известно, что компания Microsoft начала собирать данные о посещённых сайтах, местоположении, голосовой речи, используемых приложениях и даже получает данные о том, что вы печатаете на клавиатуре [3]. С недавними обновлениями данного продукта стало возможно отключить скрытую функцию, но раньше многие не просто не могли это отключить – они даже не знали, что данная функция слежки присутствует в Windows 10.

Может показаться, что от всего можно скрыться задействовав технологию VPN и ни о чем больше не беспокоится. Так можно было действовать 10 лет назад, но не сейчас. На данный момент в скрытом режиме сайт может собирать не просто данные о браузере, но и системе вцелом: какая версия операционной системы используется, какие технологии поддерживает браузер, какие спецификации вашего устройства, какие установлены шрифты, какой ваш публичный и локальный IP адрес и так далее. Это называется «отпечатком» и у каждого он уникальный. Если мы хотим всё это прикрыть и больше никому не выдавать информацию о вашем устройстве, то какие технологии и программы использовать? На данный момент есть несколько систем, позволяющие скрыть ваше присутствие в сети:

– Операционная система Tails. Это действующая в режиме реального времени операционная система Linux, которую можно запускать практически на любом компьютере с DVD, USB-накопителя или SD-карты и не оставлять следов на компьютере, который вы используете. Важной особенностью Tails является то, что все исходящие соединения вынуждены проходить через Tor, а не анонимные соединения блокируются.

– Операционная система Whonix. Операционная система состоит из двух виртуальных машин: один исключительно управляет Tor и действует как шлюз, который называется Whonix-Gateway. Другой, который называется Whonix-Workstation, находится в полностью изолированной

сети. Отличие между ними в том, что Tails это независимая операционная система, которую можно запустить с любого компьютера, и она не оставляет после себя следов, а также не хранит данные. Каждый раз при запуске системы она будет как новая. В свою очередь Whonix устанавливается на уже готовую ОС посредством виртуальной машины, и она сохраняет все данные, одна Whonix невозможно деанонимизировать.

– Програмное обеспечение AntiOS является небольшой программой с открытым исходным кодом на Python и является самым простым способом изменить данные о вашем компьютере. Большую эффективность показывает в работе с другими приложениями.

– Браузер Linken Sphere. Браузер работает в OTR-режиме, что делает его самым безопасным. На компьютере не сохраняется абсолютно никаких следов действий, что не позволит даже случайно попавшим на машину вредоносным программам получить доступ к информации, шифрует всю сохраняемую информацию по стандарту шифрования AES-256, позволяет одновременно работать с различными типами подключений в мультипоточном режиме HTTP, SOCKS, SSH, TOR, TOR + SSH и многие другие функции возможны в данном продукте.

Многие компании хотят знать как можно больше о потенциальных клиентах, собирая как можно больше данных об их действиях и только те люди, которые ценят себя и свою личную жизнь, знают как себя обезопасить от скрытого сбора данных о себе.

Список использованной литературы

1. Политика конфиденциальности и Условия использования Google [Електронний ресурс] – Режим доступу до ресурсу: https://policies.google.com/technologies/partner-sites?hl=ru

2. Как Facebook собирает и продает данные пользователей [Електронний ресурс] – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/Статья:Как_Facebook_собирает_и_продает_данные_пользователей

3. Windows 10 поставляется с кейлоггером [Електронний ресурс] – Режим доступу до ресурсу: https://xakep.ru/2014/10/10/windows-10-keylogger/

Ключові слова: дані, система, Facebook, Google.
Ключевые слова: данные, система, Facebook, Google.
Keywords: data, system, Facebook, Google.
***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Лопаєв Дмитро Валерійович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультет кібербезпеки
та інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ В СУЧАСНИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ ТЕХНОЛОГІЇ LTE

Необхідність захищати технології LTE приманює багато уваги операторів мобільного зв'язку, так і рядових користувачів інтернету.

Бездротові цифрові тенета, яскраво стартувавши, постійно розвиваються і дуже швидко. Це грає на руку в мікроелектроніці, що допускає можливість робити все складніші і також – дешевші – засоби бездротового зв'язку.

Технологія WIMAX (IEEE802.16–2004) не була тепло прийнята, вона уступала по швидкості, конфідеційності і вартості. Але оператори очікують інноваційного прориву від мобільного WIMAX (IEEE802.16e).

Розвиток технології LTE як стандарту офіційно розпочався наприкінці 2004 року. Основною метою початкового дослідження є вибір 84 технологій фізичного рівня, які можуть забезпечити високу швидкість передачі даних. В якості запропонованих запропоновано два основні варіанти: розробка звичайного бездротового інтерфейсу W-CDMA (для HSPA) та створення на основі технології OFDM (ортогональне мультиплексування з частотним поділом) нової добірки.