УДК 004.77

Літвіненко А. А., Воротнікова З. Є.

ПРОЕКТУВАННЯ СИСТЕМИ ФОРМУВАННЯ МУЛЬТІ-ІМІДЖУ КОРИСТУВАЧА В МЕРЕЖІ ІНТЕРНЕТ

У статті розглянуто ряд основних ідентифікаторів потрібних для ідентифікації, формування та аналізу користувача в мережі Інтернет, їх властивості і взаємозв'язки між собою всередині Анті-фрод систем. Досліджено типи ідентифікаторів браузерного та мережевого рівня, їх аналіз та взаємодія один з одним всередині інформаційних систем безпеки. Розглянуто основні рівні та етапи ідентифікації користувача в мережі Інтернет. Дано визначення інформативності апаратного та операційного рівня. Проаналізовано загальні статистичні дані користувачів Інтернет ресурсів, розглянуто базові процедури перевірки: ідентифікація, аутентифікація. Розглянуто принципи формування та обчислення рейтингу користувача веб-ресурсу. Розроблено власну систему безпеки на сайті, яка дозволяє ідентифікувати користувача в мережі Інтернет за допомогою аналізу інформації, отриманої в процесі взаємодії користувача з веб-сервером. У роботі було створено елементарного макету системи формування рейтингу легітимності користувача веб-ресурсу, згідно отриманих даних від нього для подальшого аналізу. Ідентифікування користувача веб-ресурсу проводилося за допомогою звичайних методів мови програмування Javascript. При створенні власної системи безпеки ідентифікації анонімних користувачів було відібрано 15 найбільш інформаційних ідентифікаторів, які запитуються у користувача при спробі авторизації на веб-ресурсі. Застосування наведених методів дозволяє збільшити ступінь достовірності ідентифікації користувача в мережі Інтернет, що дає можливість використовувати результати для автоматизованої оптимізації систем виявлення вторгнень або аномальних дій при виставленні адаптивного порога перевірки, а також для виявлення потенційного зловмисника в мережі Інтернет.

Ключові слова: *Інтернет, інформаційні системи, ідентифікація користувача, формування рейтингу користувача, аналіз даних, інформаційна безпека.*

Постановка проблеми. Інтернет є всесвітньо інформаційно-комп'ютерною системою, що поєднує між собою безпосередньо як користувачів цих комп'ютерних мереж, так і користувачів комп'ютерів для обміну інформацією. В даний час інтернет вже досить розвинувся новими технологіями і можливостями, дозволяючи проводити аналіз користувача, його інтересів і переваг, його дій і активності в мережі. Згідно зі статистичними даними на жовтень 2020 року, інтернет веб ресурсами користуються вже більше ніж 4.66 млрд осіб з 7.81 млрд населення нашої планети і цей відсоток нових користувачів в мережі збільшується з кожним днем. Зі зростання нових користувачів інтернет ресурсів, так само збільшуються обороти електронних платежів в мережі і з кожним роком ця цифра зростає. Купівельна спроможність людей (їх придбання в мережі інтернет) збільшується з кожним роком на 500 млрд. доларів, а на час всесвітньої пандемії ця цифра може збільшитися в декілька разів на 2020 рік [1].

Так само слід розуміти, що в цих сферах де циркулюють величезні гроші, кожного дня відбуваються тисячі злочинів шахраїв, які наносять величезну шкоду сумірну з десятками мільярдів доларів на рік [1].

Для запобігання шахрайських операцій і збереження грошей як звичайних користувачів так і великих корпорацій, використовують Антіфрод системи. Такі системи захищають платіжні шлюзи, особисті кабінети веб-ресурсів, форми авторизації і будь-який інший елемент, підвищена експлуатація якого може привести до збитку інтересам веб-ресурсу. Іншими словами, такі системи виконують функцію визначення і розпізнавання користувача як «доброго» або «поганого», приймаючи рішення, що користувачеві дозволити, а що заборонити.

Практично кожен веб ресурс має можливість отримати інформацію про користувача, і ідентифікувати його як особистість, зібравши всі потрібні дані про нього, згідно загального регламенту захисту персональних даних GDRP, CCPA, LGPD.

При реєстрації користувача на якомусь ресурсі або ж при покупці товару в інтернет магазині, при будь-якому цілеспрямованому активному дії, починається етап отримання поверхневої інформації про цього користувача (отримання його ідентифікаторів).

Дослідження ідентифікації користувача в мережі Інтернет дозволяє покращити захист інформації і запобігти неправомірному отриманню її злочинцями. У зв'язку з цим, розробка таких систем є актуальним завданням особливо при використанні не захищених каналів передачі даних.

Аналіз останніх досліджень і публікацій. Управління та розмежування доступу до комп'ютерних систем і до їх ресурсів є одним з важливих аспектів інформаційної безпеки, що може бути реалізовано за рахунок ідентифікації користувачів.

Аналіз відомих методів та рішень показав, які напрямки вже достатньо розроблено:

- методи та засоби комп'ютерно-лінгвістичного аналізу достовірності соціально-демографічних характеристик учасників віртуальних спільнот [2];
- методи реєстрації, верифікації та валідації персональних даних користувачів веб-спільнот [3];
- моделі віртуальної спільноти та інформаційного середовища віртуальної спільноти [4];
- етапи пошуку у WWW різноманітної інформації [5].

Концепція фінгерпринтингу ґрунтується на припущенні, що кожен електронний пристрій має унікальний набір фізичних чи логічних функцій, які можуть використовуватись для його ідентифікації на основі інформації, переданої браузерами. Залежно від використовуваних методів, користувача можна відстежувати за допомогою функцій браузера (фінгерпринтинг браузера) або на основі системних налаштувань (крос-браузерний фінгепринтинг), який дає змогу ідентифікувати пристрій та користувача, навіть коли використовується декілька браузерів [6].

Найпростіший спосіб відслідкувати користувача в мережі інтернет – це побудова ідентифікаторів об'єднанням набору параметрів, доступних у середовищі браузера, кожен з яких сам по собі не становить жодного інтересу, але разом вони утворюють унікальне для кожного комп'ютера значення: User Agent (версія браузера, версія операційної системи, деякі аддони), годинник (відхилення між реальним та системним часом), інформація про CPU та GPU, роздільна здатність екрана та розмір вікна браузера, список встановлених у системі шрифтів, список усіх встановлених плагінів, ActiveX-контролів, Browser Helper Object'ів та їх версій, інформація про встановлені розширення та інше програмне забезпечення [6, 7]. Автори [8] запропонували незалежний від браузера метод ідентифікації користувача – показали, що частини IP-адреси, певного набору шрифтів, часового поясу та роздільної

здатності екрана достатньо, щоб однозначно ідентифікувати більшість користувачів п'яти найпопулярніших браузерів. Ці параметри користувацького агента доволі ефективні, що підтвердила перевірка такого методу на наборі даних з майже тисячі записів, зібраних через загальнодоступний тестовий веб-сайт [8].

Низка ознак для ідентифікації користувача міститься в архітектурі локальної мережі та налаштуванні мережевих протоколів. Такі ознаки характерні для всіх браузерів, встановлених на клієнтському комп'ютері, їх не можна приховати за допомогою налаштувань приватності або якихось утиліт. Це: зовнішня IP-адреса, номери портів для вихідних TCP/IP-з'єднань, локальна IP-адреса для користувачів за NAT'ом або HTTP-проксі, інформація про проксі-сервери (отримана з HTTP-заголовка), які використовує клієнт [6, 7].

Ще одним варіантом ідентифікації користувача є аналіз характеристик кінцевого користувача: вибрана мова, кодування за замовчуванням, часовий пояс; дані в кеші клієнта та історія його переглядів; рухи мишею, частота та тривалість натискання клавіш, дані з акселерометра; будь-які зміни стандартних шрифтів сайта та їх розмірів, масштаб, використання спеціальних можливостей перегляду; стан певних функцій браузера, таких як блокування сторонніх cookies, DNS prefetching, блокування спливання вікон, налаштування безпеки [6, 7].

У роботі [9] подано спосіб відстеження користувача на основі профілю його системи з метою збирання даних за очищених або відключених користувачем cookies.

У роботі [10] проаналізовано властивості браузерів, які відправляють на сервер, дозволяючи створювати унікальний "відбиток" цих браузерів. Браузери, які підтримують Flash або Java, в середньому містять принаймні 18,8 біта ідентифікаційної інформації [11]. Але зазначені методи і засоби не розв'язують задачу формування інформаційного портрета користувача мережі інтернет.

Останнім часом суттєво збільшилася кількість досліджень та публікацій, присвячених цій проблемі. Значна більшість наукових статей розглядає лише один з можливих способів ідентифікації користувачів. Наприклад, парольна ідентифікація [2], біометрична ідентифікація [3, 4, 5, 12], але найчастіше розглядаються лише окремі біометричні ознаки, що використовуються для визначення особи користувача. Апаратна ідентифікація представлена лише низкою практичних рішень без докладного аналізу та порівняльної характеристики [13]. Що ж стосується комплексного підходу до ідентифікації користувачів, то в сучасній науковій літературі майже не представлено досліджень та практичних рішень систем, в яких використовується декілька ознак для ідентифікації одночасно [14, 15, 16].

Мета статті. Розробка методу підвищенні ступеня достовірності ідентифікації користувача в мережі Інтернет за рахунок використання допоміжної інформації про комп'ютер користувача.

Викладання основного матеріалу. Завдання дослідження полягає в розробці методу ідентифікації користувача в мережі інтернет та формування його інформаційного іміджу за рахунок використання допоміжної інформації про комп'ютер користувача

Практично кожен веб ресурс має можливість отримати інформацію про користувача, і ідентифікувати його як особистість, зібравши всі потрібні дані про нього, згідно загального регламенту захисту персональних даних GDRP, CCPA, LGPD.

При реєстрації користувача на якомусь ресурсі або ж при покупці товару в інтернет магазині, при будь-якому цілеспрямованому активному дії, починається етап отримання поверхневої інформації про цього користувача (отримання його ідентифікаторів).

На цьому ж етапі зборі інформації, відбувається отримання cookie-файлів - фрагментів даних, відправлених веб-сервісом і збережених на пристрої користувача, з метою отримання інформації про клієнта, який можливо вже існував на цьому сайті, або ж «познайомитися» з користувачем і запам'ятати його, як клієнта цього веб-ресурсу.

Після етапу збору інформації, настає етап аналізу отриманої інформації і в першу чергу, відбувається порівняння ідентифікаторів згідно фрод листам. Проще кажучи, якщо системою буде виявлено відбиток користувача який передає будь-якої унікальний ідентифікатор (швидше за все є фальшивим, прихованим або заміненим цим користувачем), то цей ідентифікатор буде знаходиться в так званому фрод листі і відповідно наявності цього ідентифікатора в цьому листі категорично негативно зіграє на всіх подальших діях цього користувача.

Крім цього, є можливість перевірити легітимність такого ідентифікатора, іншими словами перевіривши чи є цей ідентифікатор реальним.

Найважливішим етапом ідентифікації - є етап формування рейтингу надійності користувача який безпосередньо розраховується щодо зібраних і проаналізованих даних користувача. Залежно від цього рейтингу, приймається рішення або подальша дія буде дозволена, або дію заборонять, або попросять надати будь-яку додаткову інформацію про себе.

Наші гаджети містять в собі величезну кількість ідентифікаторів за допомогою яких можна оцінити нас як користувача і їх набагато більше аніж ми можем уявити. Систематизуємо їх в окремі рівні:

- апаратний - «залізо» (всі електронні та механічні частини обчислювального пристрою);
- операційний - безпосередньо сама операційна система і її програмний підрівень - програмне забезпечення встановлене на пристрої;
- браузерний - браузер, його налаштування (плагіни, розширення);
- мережевий - визначення шляхів передачі даних по мережі.

Ідентифікаторами апаратного рівня виступають: монітор, процесор, відеокарта, батарея, оперативна пам'ять, мікрофон, веб камера, колонки, usb пристрої, мишка чи клавіатура.

Ідентифікатори операційного рівня: версія операційної системи, відбитки canvas, ім'я комп'ютера, геолокація ip адреса, встановлені шрифти, розкладка клавіатури, часовий пояс і час, відкриті порти.

Ідентифікатори операційної системи (апаратного та операційного рівня) в більшості випадків використовуються не для ідентифікації користувача, а для виявлення аномальних активностей і використання будь-якого анонімізуючого програмного забезпечення.

Ідентифікатори браузерного рівня: цифрові відбитки, властивості і функції нашого веб-браузера. Розглянемо їх детальніше.

Функції:

- User-Agent - буквено-цифровий рядок, що ідентифікує програму, яка відправляє запит на сервер і одночасно запитує доступ до веб-сайту.
- Browser engine - являє собою програму, що перетворює вміст веб-сторінок (файли HTML, XML, цифрові зображення і т.д.) і інформацію про форматування (в форматах CSS, XSL і т.д.) в інтерактивне зображення на екрані.

- WebGL - програмна бібліотека для мови JavaScript призначена для візуалізації інтерактивної тривимірної графіки і двомірної графіки в межах сумісності веб-браузера без використання плагінів.
- WebGL Extensions - розширення WebGL які дозволяють звертатися до відеокарти за допомогою OpenGL ES і виробляти отрисовку 3D-графіки через HTML5-елемент Canvas.
- Підтримка USB API - Інтерфейс управління передається usb пристроєм браузеру для ідентифікації.
- Підтримка CSS (каскадних таблиць стилів) - мови опису зовнішнього вигляду веб сторінки написаного з використанням мови розмітки (HTML або XHTML). Будь-який сайт запросивши CSS Reflections відображення, може визначає який Browser engine використовується.
- WebRTC - технологія призначена для передачі потокових даних між браузерами або додатками з використанням технології двоточкової передачі (point-to-point transmission). Суттю впровадження даної технології розробниками була можливість надання користувачам мультимедійної комунікації між браузерами.

Властивості браузера:

- Апаратне прискорення графіки - використовується для швидкого рендеринга графіки на комп'ютері або ноутбуці шляхом переміщення цієї дії з центрального процесора в графічний процесор. Її наявність вказує на реального користувача, її відсутність вказує на користувача або віртуальної машини або віддаленого сервера.
- Загальна продуктивність - будь-який веб-ресус може перевірити продуктивність процесора. Суть перевірки полягає в тому, що браузеру надається високо-ресурсний об'ємний JavaScript код час обробки якого, виражено в шкалі. Завдяки визначенню продуктивності браузера, можна визначити сімейство браузера, його версію.

За допомогою обчислення загальної продуктивності нашого процесора, є можливість розмежувати відразу 3 групи користувачів: користувачів реальних обчислювальних машин; користувачів віртуальних машин; користувачів серверів.

У користувачів реальних машин - значення будуть усереднені, у користувачів віртуальних машин - низькими, у користувачів серверів - значення будуть завищеними.

Відбитки:

- Самостійні відбитки - отримані в результаті використання однієї технології.
- Залежні відбитки - отримані при поєднанні технологій.

Приклади самостійних відбитків:

- Canvas - технологія Canvas використовується для малювання графіки засобами мов програмування (зазвичай JavaScript). Простими словами це елементарні інструкції з побудови графіки в браузері користувача, тим самим картинка буде будуватися на комп'ютері кожного користувача і зображення на виході, буде відрізнятися. Відмальованє зображення, перекладається в бінарний код. Найменша зміна пікселя зображення, призведе до зміни масиву бінарних чисел і подальше перетворення за допомогою хеш функції призведе до кордінальної зміни хешу зображення на двох різних комп'ютерах.
- WebGL - на відміну від технології кинувся WebGL малює 3D фігуру.
- AudioContext - аудіо відбиток, використається для виявлення віртуальних машин і віддалених серверів, в залежності від відмінності відтворення аудіо або неможливістю відтворення взагалі, як при використанні віддалених серверів.

- Font Fingerprint - розробник веб-ресурсу може вимагати наявність певних шрифтів і певних гарнітур до цих шрифтів і в залежності від того, чи знаходяться ці шрифти у користувача на його пристрої є можливість ідентифікувати його систему з дуже великою часткою ймовірності, є можливість ідентифікувати що система «свіжа», є можливість ідентифікувати систему якщо вона в собі має додаткове програмне забезпечення.
- ClientRect - масштабність тексту зображеного на веб сторінці.

Ідентифікатори мережевого рівня: прямі ідентифікатори - конкретні значення; непрямі ідентифікатори - підлягають додатковій перевірці, засновані на прямих ідентифікаторах; ідентифікатори отримані в результаті технічного аналізу прямих і з них похідних непрямих ідентифікаторів.

Прямі ідентифікатори:

IP адреса:

- IPv4 (Internet Protocol version 4) четверта версія протоколу IP. Перша широко використовувана версія. IPv4 використовує 32-бітові (чотирибайтових) адреси, що обмежують адресний простір 4 294 967 296 можливими унікальними адресами.
- IPv6 (Internet Protocol version 6) нова версія протоколу IP, покликана вирішити проблеми з якими зіткнулася попередня версія (IPv4) при її використанні в Інтернеті, за рахунок використання довжини адреси 128 біт замість 32 біт. IPv6 використовує 128-бітові адреси, що обмежують адресний простір теоретично доступними 340 282 366 920 938 463 463 374 607 431 768 211 456 унікальними адресами.

DNS - (Англ. Domain Name System «система доменних імен») - комп'ютерна розподілена система для отримання інформації про домени. Найчастіше використовується для отримання IP-адреси по імені хоста (комп'ютера або пристрою), отримання інформації про маршрутизації пошти або обслуговуючих вузлах для протоколів в домені (SRV-запис).

WebRTC (англ. Real-time communications - комунікації в реальному часі) - проект з відкритим вихідним кодом, призначений для організації передачі потокових даних між браузерами. Антіфрод взяли цю технологію собі на увагу, з якості того, що WebRTC дозволяє показати реальний IP-адресу користувача. Перевірка відбувається запитом від декількох stun серверів і в залежності від того, як ці запити будуть оброблені, такий і WebRTC-адреса буде закріплений за користувачем.

Відкриті порти. На будь-якому комп'ютері користувача існує 65535 портів. Практично всі служби і додатки використовують під себе окремий виділений порт. Завдяки скануванню портів користувача (запиту до певних портів) є можливість ідентифікувати користувача.

TLS відбиток. Абревіатура TLS (Transport Layer Security / Протокол захисту транспортного рівня) з'явилася в якості заміни позначення SSL (Secure Sockets Layer) після того, як протокол остаточно став інтернет-стандартом. TLS ставить собі за мету створення між двома вузлами мережі захищений від прослуховування і підміни інформації канал зв'язку, придатний для передачі довільних даних в обох напрямках, а також виконання перевірки того, що обмін даними відбувся між саме тими вузлами, для яких канал і планувався. TLS відбиток складається на основі даних аналізу параметрів шифрування і використовується, як додатковий сигнал при ідентифікації користувача.

Непрямі ідентифікатори:

Hops - кількість проміжних вузлів, від користувача до шуканого веб-ресурсу, чим більше ця відстань, тим більша ймовірність того, що користувач використовує будь-які засоби анонімності.

Двосторонній пінг - завдяки використання двостороннього пинга, є можливість і з одного боку, сторони клієнта і з боку веб-ресурсу, зрозуміти яка кількість пакетів буде витрачено на обробку сигналу.

Пасивний відбиток операційної системи - Passive Operation System Fingerprinting - це відбиток операційної системи встановленої на пристрої. Основне завдання POSF - визначити тип і версію ОС комп'ютера.

Аналізовані ідентифікатори:

ASN - автономна система (AS) являє собою групу з кількох IP-мереж, що мають окрему політику маршрутизації. Щоб ці автономні системи могли взаємодіяти один з одним, їм потрібен унікальний номер або ідентифікатор. Номер автономної системи (ASN) - це унікальний номер, доступний глобально, що дозволяє відповідним автономних систем обмінюватися даними маршрутизації з іншими підключеними системами. ASN може бути приватним або загальнодоступним.

Підмережа - це розділена мережа на менші частини за допомогою запозичення бітів з частини IP-адреси, в якій визначається хост, це дозволяє більш ефективно використовувати мережеву адресу. Підмережа і кількість IP адрес за якими відбуваються будь-якого роду інциденти, зафіксовані анти-фрод системами безпосередньо впливає на легітимність самого користувача.

Fraud List / Black List - при здійсненні фрод дій (шахрайських операцій в мережі Інтернет) користувачем, його IP-адреси заносять в Fraud List. І при подальших перевірках і аналізах IP-адреси вже буде можливість провести перевірку, яким користувачем, він є «добрим» або «поганим». Fraud List - листи знаходяться всередині анти-фрод системи.

IP-Type - визначення типу з'єднання

Region Data - зіставлення часу користувача за IP-адресою до часу отриманого на системі цього користувача.

Is bot? - рейтинг того чи є користувач живою людиною або він бот, на підставі IP-адреси і активності користувача в мережі інтернет.

Формування рейтингу користувача базується відносно всіх зібраних і проаналізованих даних, але окрім перевірки певних ідентифікаторів всіх рівнів та їх окремих взаємодій одного між одним, також проводиться цифрова розвідка, звана як OSINT. Open Source INTelligence - пошук, збір і аналіз інформації, отриманої із загальнодоступних джерел. Перевірка соціальних мереж користувача.

Проект передачі даних - це ініціатива з відкритим вихідним кодом, яка забезпечує переносимість даних між декількома онлайн-платформами. Проект був запущений і представлений Google 20 липня 2018 року, і в даний час він дозволяє обмінюватися інформацією між собою такими великими компаніями як Google, Facebook, Microsoft, Twitter і Apple.

Завдяки збору цієї інформації можна визначити користувача як нового і позначити його умовним рейтингом ще до перевірки його ідентифікаторів. Згідно аналізу даних, розрахунку легітимних і підозрілих дій сторони користувача, система дає свою оцінку цієї особи та вирішує подальші дії з ним. Наприклад якщо рейтинг користувача розрахований системою умовно більше певного значення - користувачу надається можливість подальших дій, якщо рейтинг менше певного значення - система може запросити додаткову інформацію про користувача і нам сам кінець якщо система визначить безліч підозрілих даних, вона може заблокувати такого юзера або обмежити його права.

Окрім збору інформації про користувачів з метою убезпечити себе і свої веб-ресури, сайти також використовують дані користувача і в маркетингових цілях. Наприклад ціна товару може відрізнятися в інтернет-магазині в залежності від вашої операційної система на телефоні (iOS, Android). В залежності від вашого місця знаходження, на веб-ресурсах може відрізнятися список готелів в які ви би хотіли або хочете заселитися, і таких прикладів дуже багато.

Веб-ресурс сам проектує ці системи оцінок користувачів, згідно зі своїх інтересів, переваг, ідей, виконуючи свої функції та поставленні завдання.

Для сучасних інформаційних систем застосовуються засоби ідентифікації, засновані на зберіганні IP-адрес комп'ютерів відвідувачів і записах на комп'ютер користувача даних Cookie. До недоліків першого способу відноситься широка поширеність динамічних IP-адрес, що виділяються з пулу провайдера в момент підключення користувача, а також можливість використання в мережі проксі-серверів, анонімайзерів і механізму NAT (NetworkAddressTranslation), що знижує ступінь достовірності ідентифікації користувача . Недоліком другого способу є прив'язка Cookie до конкретного браузеру, що знижує вірогідність ідентифікації при використанні декількох браузерів. Іншим недоліком використання даної технології є можливість підміни і знищення даних Cookie, а також відключення самого механізму користувачем.

Таким чином, обидва способи не дозволяють в ряді випадків досягти необхідного ступеня достовірності ідентифікації. В той же час існують способи отримання даних, що характеризують робоче середовище користувача. Під робочим середовищем користувача розуміються дані про операційній системі користувача, шрифтах, параметрах екрана, плагинах, відвіданих посиланнях і т.п.

В даний час майже кожен веб ресурс має свої системи оцінки та методи оцінки користувача. Перевірки їх аномальних та підозрілих дій на сайті, їх використання декількох акаунтів для подальшого зловживання.

У роботі було створено елементарного макету системи формування рейтингу легітимності користувача веб ресурсу, згідно отриманих даних від нього для подальшого аналізу.Ідентифікувати користувача веб ресурсу ми будемо за допомогою звичайних методів мови програмування Javascript.

JavaScript - прототипно-орієнтована сценарна мова програмування, зазвичай використовується як вбудований мова для програмного доступу до об'єктів додатків. Найбільш широке застосування знаходить в браузерах як мова сценаріїв для додання інтерактивності веб-сторінках.

Технологія Javascript дозволяє отримати дані про операційну систему, плагінах, часовому поясі користувача та вирішенні екрану. Безсумнівним плюсом технології є її поширеність, кроссбраузерність і непомітність для користувача. Javascript включений у 99,9 % користувачів.

Одним з найпростіших методів отримання ідентифікаторів від браузера є властивості і методи об’єкту navigatorJavascript.

Об'єкт navigator - інформаційний об'єкт, який використовується для отримання різної інформації браузеру, мережевого з’єднання, операційній системі і т.ін.

Ця інформаця доступна через такі властивості цього об'єкту:

- appCodeName - повертає внутрішнє "кодове" ім'я браузера;
- appName - повертає ім'я браузера;

- appVersion - повертає інформацію про версії браузера;
- cookieEnabled - визначає чи включені cookies в браузері;
- geolocation - повертає об'єкт Geolocation, який використовується для визначення місця розташування користувача;
- language - повертає яка мова використовується в браузері;
- online - визначає чи перебуває браузер в режимі онлайн;
- platform - повертає назву платформи, в якій браузер працює;
- product - повертає ім'я движка, на якому працює браузер;
- userAgent - повертає рядок useragent, яка містить інформацію про браузері.

Вона використовується в якості заголовка, який браузер посилає на сервер.

При створенні власної системи безпеки ідентифікації анонімних користувачів було відібрано 15 найбільш інформаційних ідентифікаторів, які запитуються у користувача при спробі авторизації на веб-ресурсі. Серед них:

1. IP – адрес, при наявності дублікату IP в базі даних веб-ресурса, помічає користувача як порушника, відстеження мультиакаутінгу.
2. Ім’я браузера.
3. Версія браузера.
4. Заголовок UserAgent, при невідповідності до отриманих даних (Ім’я та Версія браузера отриманих методами Javascript) помічає користувача як ненадійного, ймовірне використання засобів анонімності.
5. Мова системи.
6. Розширення екрану, при аномальних значеннях, помічає користувача як ненадійного.
7. Активне розширення екрану, відстеження мультиакаутінгу.
8. Місто, відстеження використання засобів анонімності VPN, PROXY та ін.
9. Країна, відстеження використання засобів анонімності VPN, PROXY та ін.
10. Перевірка Cookie, їх наявність. При вимкнених Cookie, ймовірність анонімізації користувача, помічає користувача як ненадійного.
11. Часовий пояс, порівняння з IP адресою та місцезнаходженням користувача, при невідповідності даних, помічає користувача як ненадійного.
12. Перевірка методу maxTouchPointsJavascript на наявність TouchScreen користувача, при невідповідності даних (Розширення екрану, UserAgent зокрема відмінності в операційній системі) помічає користувача як порушника.
13. Отримання унікального ідентифікатору WebGLhash, розрахованого побудовою 3d фігури, при наявності дублікату в базі даних, помічає користувача як порушника.
14. Отримання унікального ідентифікатору Canvashash, створення 2d малюнку зображення з накладанням ефекту на встановлений шрифт, при наявності дублікату в базі даних, помічає користувача як порушника.
15. Власний ідентифікатор унікального користувача, присвоєний одноразово, до унікальної IP адреси, WebGL та Canvas відбитка.

Приклад таблиці MySql зі збору ідентифікаторів показано на рис. 1.

	#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐	1	id	int(5)			Нет	*Нет*		AUTO_INCREMENT	Изменить Удалить Ещё
☐	2	Name	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	3	SName	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	4	Date	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	5	IP	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	6	Browser	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	7	Version	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	8	Lang	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	9	UserAgent	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	10	Screen	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	11	AScreen	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	12	City	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	13	Country	varchar(128)	utf8_general_ci		Да	*NULL*			Изменить Удалить Ещё
☐	14	WebGL	text	utf8_general_ci		Нет				Изменить Удалить Ещё
☐	15	Canvas	text	utf8_general_ci		Нет				Изменить Удалить Ещё

Рисунок 1 – База даних MySql веб-ресурсу

Приклад ідентифікації нового легітимного користувача веб-ресурсу через форму авторизації на сайті показано на рис. 2.

id	Name	SName	Date	IP	Browser	Version	Lang	UserAgent	Screen	AScreen	City
99	Andrey	Litvinenko	12.10.2008:51:35	178.209.67.216	Google Chrome	87.0.4280.88	ru-RU	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	1920x1080	1920x969	Mariupol

City	Country	WebGL	Canvas	Uniq	COOKIE	UTC
Mariupol	Ukraine	7a1c5eb9985acfb615c0d57d4c44ebfb97f2f014e3d7534e6d50e409526ef001	1316880612	true	true	2

Рисунок 2 – Новий легітимний користувач веб-сайту

Наявність усіх типів ідентифікаторів, та їх унікальність, характеризує користувача як легітимного і позначає зеленим кольором в базі даних MySql, такий користувач є унікальним.

Приклад ідентифікації нового ненадійного користувача веб-ресурсу показано на рис. 3.

id	Name	SName	Date	IP	Browser	Version	Lang	UserAgent	Screen	AScreen	City
96	Andrey	Litvinenko	12.10.20 08:43:40	178.209.67.216	Google Chrome	87.0.4280.88	ru-RU	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	1920x1080	1920x969	Mariupol

City	Country	WebGL	Canvas	Uniq	COOKIE	UTC
Mariupol	Ukraine	7a1c5eb9985acfb615c0d57d4c44ebfb97f2f014e3d7534e6d50e409526ef001		true	true	2

Рисунок 3 – Новий ненадійний користувач веб-сайту

Спроба сховати дані ідентифікатору, вже можуть свідчити, про «погані» діяння такого користувача, система буде вважати його ненадійним і позначає жовтим кольором в базі даних, такий користувач, скоріш за все використає засоби анонімності.

Приклад ідентифікації нового користувача веб-ресурсу у вигляді порушника показано на рис. 4.

id	Name	SName	Date	IP	Browser	Version	Lang	UserAgent	Screen	AScreen	City
99	Andrey	Litvinenko	12.10.20 08:51:35	178.209.67.216	Google Chrome	87.0.4280.88	ru-RU	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	1920x1080	1920x969	Mariupol
100	Nikita	Ivanov	12.10.20 09:02:39	92.60.190.249	Mozilla Firefox	80.0	ru-RU	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0	1920x1080	1920x969	Mariupol

Рисунок 4 – Користувач порушник веб-сайту

Здавалося б, новий користувач сайту, з іншою IP адресою, та іншим браузером, але система ідентифікує такого шахрая за його іншими однотипними ідентифікаторами.

City	Country	WebGL	Canvas	Uniq	COOKIE	UTC
Mariupol	Ukraine	7a1c5eb9985acfb615c0d57d4c44ebfb97f2f014e3d7534e6d50e409526ef001	1316880612	true	true	2
Mariupol	Ukraine	7a1c5eb9985acfb615c0d57d4c44ebfb97f2f014e3d7534e6d50e409526ef001	1316880612	false	true	2

Рисунок 5 – Користувач порушник веб-сайту

Отже такий користувач, не є унікальним на сайті, система визначила збіг даних ідентифікаторів (WebGL та Canvas) з іншим користувачем, це свідчить що реєстрація нового користувача проводилася з одного пристрою, тому такий аккаунт помічається червоним кольором, як порушник.

Тільки за рахунок системної оцінки та аналізу даних користувача отриманих веб-ресурсом досягається такий високий рівень ефективності ідентифікації особи в мережі інтернет.

Застосування наведених методів дозволяє збільшити ступінь достовірності ідентифікації користувача в мережі Інтернет, що дає можливість використовувати результати для автоматизованої оптимізації систем виявлення вторгнень або аномальних дій при виставленні адаптивного порога перевірки, а також для виявлення потенційного зловмисника в мережі Інтернет.

ВИСНОВКИ

У статті розглянуто ряд основних ідентифікаторів потрібних для ідентифікації, формування та аналізу користувача в мережі інтернет, їх властивості і взаємозв’язки між собою всередині Анті-фрод систем.

Розглянуто основні рівні та етапи ідентифікації користувача в мережі Інтернет. Визначення інформативності апаратного та операційного рівня.

Проаналізовано загальні статистичні дані користувачів Інтернет ресурсів, розглянуто базові процедури перевірки: ідентифікація, аутентифікація. Розглянуто принципи формування та обчислення рейтингу користувача веб-ресурсу.

Розроблено власну систему безпеки на сайті, яка дозволяє ідентифікувати користувача в мережі Інтернет за допомогою аналізу інформації, отриманої в процесі взаємодії користувача з веб-сервером.

Наукова новизна роботи визначається ґрунтовним дослідженням всіх типів ідентифікаторів браузерного та мережевого рівня, їх аналіз та взаємодія один з одним всередині інформаційних систем безпеки. Практична значущість роботи полягає у детальній розробці власної інформаційної системи безпеки ідентифікації користувача Інтернет.

Список використаних джерел:

1. DataReportal [Electronic resource]. – Mode of access: https://datareportal.com/reports
2. *Федушко, С. С.* Методи та засоби комп'ютерно-лінгвістичного аналізу достовірності соціально-демографічних характеристик учасників віртуальних спільнот : дис. ... канд. техн. наук : 10.02.21 / *Федушко Соломія Степанівна*. – Львів, 2015. – 205 с.
3. *Пелещишин, А. М.* Методи верифікації персональних даних на основі гендерного аналізу мови користувачів Веб-спільнот / *А. М. Пелещишин, С. С. Федушко* // Східно-Європейський журнал передових технологій. – 2010. – № 3/4. – С. 37–39.
4. *Пелещишин, А. М.* Аналіз існуючих типів віртуальних спільнот у мережі інтернет та побудова моделі віртуальної спільноти на основі веб-форуму / *А. М. Пелещишин, Р. Б. Кравець, О. Ю. Сєров* // Вісник Нац. ун-ту "Львівська політехніка". Серія : Інформаційні системи та мережі. – 2011. – № 699. – С. 212–221.
5. *Канюк, Н. В.* Етапи пошуку в WWW інформації, призначеної для аналізу політичних явищ / *Н. В. Канюк, А. М. Пелещишин* // Східно-Європейський журнал передових технологій. – 2013. – № 4. – С. 57–60.
6. *Flood, E.* Browser Fingerprinting / *E. Flood, J. Karlsson*. – Göteborg : Chalmers University of TechnologyUniversity of Gothenburg, 2012. – 99 p.
7. *Галатенко, В. А.* Основы информационной безопасности : учебное пособие / *В. А. Галатенко; под ред. акадмика РАН В. Б. Бетелина*. – 4-е изд. – М. : Интернет Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.
8. *Шарипов, Р. Р.* Идентификация и аутентификация пользователей по клавиатурному почерку / *Р. Р. Шарипов* // Электронное приборостроение : научно-практ. сб. – Казань, 2005. – Вып. 3 (44). – С. 50–54.
9. *Джхунян, В. Л.* Электронная идентификация / *В. Л. Джхунян, В. Ф. Шаньгин*. – М. : NT Press, 2004. – 695 с.
10. *Завгородний, В. И.* Комплексная защита информации в компьютерных системах: учебное пособие / *В. И. Завгородний*. – М. : Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.
11. *Шрамко, В. Н.* Комбинированные системы идентификации и аутентификации / *В. Н. Шрамко* // PCWeek/RE. – 2004. – № 45. – Режим доступа: https://www.itweek.ru/infrastructure/article/detail.php?ID=69114
12. *Flood, E.* Browser Fingerprinting / *E. Flood, J. Karlsson*. – Göteborg : Chalmers University of TechnologyUniversity of Gothenburg, 2012. – 99 p.
13. User Tracking on the Web via Cross-Browser Fingerprinting / *K. Boda, A. M. Foldes, G. G. Gulyas, S. Imre* // 16th Nordic Conference on Secure IT-Systems (Tallinn, October 26–28 2011 y.) : Proceedings. – Tallinn, 2011. – P. 31–46.
14. User Profiling Through Browser Finger Printing / *M. Ali, Z. A. Shaikh, M. K. Khan, T. Tariq* // International Conference on Recent Advances in Computer Systems (Hail, November 30 – December 01, 2015 y.) : Proceedings. – Hail, 2015. – P. 135–140.
15. Browser Fingerprinting as User Tracking Technology / *N. Kaur, S. Azam, K. Kannoorpatti, K. C. Yeo, B. Shanmugam* // 11th International Conference on Intelligent Systems and Control (Coimbatore, January 05–06 2017 y.) : Proceedings. – Coimbatore, 2017. – P. 103–111.
16. *Eckersley, P.* How Unique Is Your Web Browser? / P. Eckersley // 10th International Symposium on Privacy Enhancing Technologies (Berlin, July 21–23 2010 y.) : Proceedings. – Berlin, 2010. – P. 1–18.

17. *Глущенко, Н.* Слишком большие данные : сколько информации хранится в Интернете? [Электронный ресурс] / *Н. Глущенко*. – Режим доступа: https://ain.ua/special/skolko-vesit-internet/

Литвиненко А. А., Воротникова З. Е.

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ФОРМИРОВАНИЯ МУЛЬТИ-ИМИДЖА ПОЛЬЗОВАТЕЛЯ В СЕТИ ИНТЕРНЕТ

В статье рассмотрен ряд основных идентификаторов необходимых для идентификации, формирования и анализа пользователя в сети Интернет, их свойства и взаимосвязи между собой внутри Анти-фрод систем. Исследованы типы идентификаторов браузерного и сетевого уровня, их анализ и взаимодействие друг с другом внутри информационных систем безопасности. Рассмотрены основные уровни и этапы идентификации пользователя в сети Интернет. Дано определение информативности аппаратного и операционного уровня. Проанализированы общие статистические данные пользователей Интернет ресурсов, рассмотрены базовые процедуры проверки: идентификация, аутентификация. Рассмотрены принципы формирования и вычисления рейтинга пользователя веб-ресурса. Разработана собственная система безопасности на сайте, которая позволяет идентифицировать пользователя в сети Интернет с помощью анализа информации, полученной в процессе взаимодействия пользователя с веб-сервером. В работе был создан элементарный макет системы формирования рейтинга легитимности пользователя веб-ресурса, согласно полученным данным от него для дальнейшего анализа. Идентификации пользователя веб-ресурса проводилось с помощью обычных методов языка программирования Javascript. При создании собственной системы безопасности идентификации анонимных пользователей было отобрано 15 наиболее информативных идентификаторов, которые запрашиваются у пользователя при попытке регистрации на веб-ресурсе. Применение указанных методов позволяет увеличить степень достоверности идентификации пользователя в сети Интернет, дает возможность использовать результаты для автоматизированной оптимизации систем обнаружения вторжений или аномальных действий при выставлении адаптивного порога безопасности, а также для выявления потенциального злоумышленника в сети Интернет.

Ключевые слова: *Интернет, информационные системы, идентификация пользователя, формирование рейтинга пользователя, анализ данных, информационная безопасность.*

Litvinenko A. A., Vorotnikova Z. J.

DESIGNING A SYSTEM FOR FORMING A MULTIFACETED USER IMAGE ON THE INTERNET

The article discusses a number of basic identifiers required for identification, formation and analysis of a user on the Internet, their properties and interconnections within Anti-Fraud systems. The types of identifiers of the browser and network level, their analysis and interaction with each other within information security systems have been investigated. The main levels and stages of user identification on the Internet are considered. The definition of the information content of the

hardware and operational level is given. General statistical data of users of Internet resources are analyzed, basic verification procedures are considered: identification, authentication. The principles of forming and calculating the rating of a web resource user are considered. We have developed our own security system on the site, which allows you to identify a user on the Internet by analyzing information obtained in the process of user interaction with a web server. In the work, an elementary model of the system for forming the legitimacy rating of a web resource user was created, according to the data received from him for further analysis. The user of the web resource was identified using the usual methods of the Javascript programming language. When creating our own security system for identifying anonymous users, 15 of the most informative identifiers were selected that are requested from the user when trying to register on a web resource. The use of these methods makes it possible to increase the degree of reliability of user identification on the Internet, makes it possible to use the results for automated optimization of intrusion detection systems or anomalous actions when setting an adaptive security threshold, as well as for identifying a potential attacker on the Internet.

Key words: *Internet, information systems, user identification, user rating formation, data analysis, information security.*

Рецензент: канд. техн. наук, ДВНЗ «ПДТУ» КривенкоО. В.
Стаття надійшла 15.12.2020 р.

УДК 669.162.22

Щербаков С. В., Черевко О. О.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ КРИСТАЛІЗАЦІЇ ЗЛИТКУ

В умовах сучасного виробництва велика увага приділяється питанням підвищення якості злитків, виготовлених за технологією безперервного лиття, а також питанням надійності та безпеки роботи обладнання. На якість відлитої заготовки впливає комплекс різних факторів, основними з яких є конструктивні особливості основних вузлів МБЛЗ і наявність систем автоматичного управління.

Ключову роль у забезпеченні високої якості поверхні та внутрішньої структури злитка відіграє робота системи автоматичного управління зоною вторинного охолодження. На сучасних МБЛЗ застосовуються динамічні системи вторинного охолодження (ДСВО). Сутність даних систем полягає в можливості корекції параметрів зони вторинного охолодження на основі інформації про поточний тепловий стан злитка, яку ДСВО отримує в режимі реального часу. Необхідність отримання достовірної інформації про поточний стан злитка представляє головну складність при проектуванні ДСВО. На даний час не існує методу, який дозволяє безперервно контролювати температуру внутрішніх точок злитка, і розробка такого методу в найближчому майбутньому не представляється можливою. Тому, для контролю температурного стану злитка в ДСВО використовуються математичні моделі, які ґрунтуються на чисельному рішенні задачі нестаціонарної теплопровідності.

В роботі проведений аналіз існуючої системи управління вторинним охолодженням злитка на МБЛЗ № 6 ПАТ «МК «Азовсталь». Розроблено модель кристалізації злитка, яка