НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Технології дистанційного моніторингу веб-активності користувача із застосуванням інструментів JavaScript

Виконав (-ла): студент (-ка) 2 курсу, групи ФБ-71мп
(шифр групи)

Лопухович Володимир Сергійович
(прізвище, ім’я, по батькові)

Науковий керівник к.т.н., доц. Стьопочкіна Ірина Валеріївна _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н., ст. викл. ОНАЗ Височіненко М.С. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи і технології кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Лопуховичу Володимиру Сергійовичу

1. Тема дисертації: Технології дистанційного моніторингу веб-активності користувача із застосуванням інструментів JavaScript

науковий керівник дисертації к.т.н., доц. Стьопочкіна Ірина Валеріївна,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2018 р. № 4171-с

2. Термін подання студентом дисертації 12.12.2018 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____

_____

_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ (підпис) _____ (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) _____ (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Робота обсягом 90 сторінок містить 18 ілюстрацій, 15 таблиць та 23 джерела посилань.

Метою магістерської дисертації є – визначення засобів JavaScript, які можуть бути використані при аналізі веб-активності користувача для задач безпеки, вибір показників при створенні його портрету веб-активності (веб-портрету).

Об'єктом дослідження у даній роботі є: процес моніторингу користувача (зокрема, процес моніторингу його веб-активності).

Предметом дослідження є - можливості мови програмування JavaScript для задач моніторингу веб-активності, моделі веб-поведінки користувача (веб-портрети) та їх використання при вирішенні завдань інформаційної безпеки.

За час виконання магістерської дисертації запропоновано нову методику обробки даних, зібраних мовою програмування JavaScript та браузером, створення веб-портрету користувача як засобу виявлення порушень політики безпеки.

МОНІТОРИНГ КОРИСТУВАЧА, МОНІТОРИНГ З JAVASCRIPT, ВЕБ-ПРОГРАМУВАННЯ, ВЕБ-ЗАСТОСУНКИ, ПОРТРЕТ ВЕБ-АКТИВНОСТІ КОРИСТУВАЧА.

ABSTRACT

The work includes 90 pages, 18 figures, 15 tables and 23 references.

The purpose of the work is - the definition of indicators that can be used in analyzing user's web activity, the choice of optimal performance when creating his virtual portrait.

The object of research in this work is - monitoring users processes and creating a portrait of their web activity.

The subject of the study is - JavaScript abilities, their using in creating users' virtual portrait and their using in the implementation of information security in the browser.

During the implementation of the master's thesis proposed methods that can be used in the development of user monitoring systems, systems for monitoring their web activity, creating security policies when working in the browser.

USER MONITORING, JAVASCRIPT MONITORING, WEB DEVELOPMENT, WEB APPLICATIONS, USER'S WEB-ACTIVITY PORTRAIT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ВПК – веб-портрет користувача
ПЗ – програмне забезпечення
DLP – data loss prevention
SIEM – security information and event management
GA – google analytics
ОС – операційна система
JS – мова програмування JavaScript
URL - Uniform Resource Locator

ВСТУП

Розповсюдження мережі інтернет та її впровадження до майже всіх сфер нашого життя призводить до того, що підприємства переносять виконання певних бізнес процесів у веб, тим самим збільшуючи свої можливості та прибутки. Але з великими можливостями приходить і велика відповідальність, тому компаніям варто забезпечити динамічний захист своїх систем, інформації та інших цінних ресурсів.

Однією з найважливіших складових успішної роботи підприємства є продуктивність його роботи, яка в свою чергу безпосередньо залежить від результатів роботи його співробітників. Крім виховання таких якостей як сумлінність та ініціативність у робочих, необхідно контролювати комфортне і безпечне інформаційне середовище всередині підприємства. Існують два способи контролю роботи компанії: контроль процесу роботи і контроль результату. Але як показує досвід великих компаній - контролю підлягають усі етапи роботи, що впливають на рішення завдань компанії.

Актуальність роботи. Одним з джерел витоку конфіденційної інформації підприємства є його працівники, які, свідомо чи ні, можуть порушувати політики безпеки та видавати дані чи інші цінні ресурси зловмисникам. Тому необхідне рішення, яке дозволить моніторити діяльність працівника та уживати заходи в реальному часі, які зможуть мінімізувати порушення інформаційної безпеки таким способом. Впровадження системи, яка буде працювати на рівні браузера, дозволить динамічно впроваджувати різні правила політики безпеки, контролювати активність співробітника, а також виявляти аномальну поведінку, що може бути результатом зловмисної діяльності.

Задачі дослідження:

1. Проаналізувати існуючі тенденції моніторингу користувача для вирішення завдань безпеки.
2. Проаналізувати існуючі рішення для реалізації моніторингу, провести порівняльний аналіз можливостей.

3. Виділити основні підходи до реалізації механізмів моніторингу та його напрямки при використанні контролю інтернет-активності співробітника підприємства.
4. Запропонувати засоби JavaScript, які можуть бути використані для вирішення задач моніторингу. Виділити ті показники, які можуть бути включені до веб-портрету користувача для виявлення його типової поведінки, оточення та вподобань – для подальшого виявлення відхилень від його типової поведінки.
5. Запропонувати рішення, які дозволяють контролювати активність працівника із використанням браузера.
6. Виконати аналіз практичних переваг запропонованих рішень.

Мета дослідження. Визначення засобів JavaScript, які можуть бути використані при аналізі веб-активності користувача для задач безпеки, вибір складових для створення його портрету веб-активності (веб-портрету).

Об'єкт дослідження. Об'єктом дослідження є процес моніторингу користувача (зокрема, процес моніторингу його веб-активності).

Предмет дослідження. Можливості мови програмування JavaScript для задач моніторингу веб-активності, моделі веб-поведінки користувача (веб-портрети) та їх використання при вирішенні завдань інформаційної безпеки.

Наукова новизна. Запропоновано нову методику обробки даних, зібраних мовою програмування JavaScript та браузером, створення веб-портрету користувача як засобу виявлення порушень політики безпеки.

Практична значущість результатів. Результати роботи можуть бути використані при розробці систем моніторингу користувачів, систем контролю їх веб-активності, створенні політик безпеки при роботі в браузері. Частина результатів була застосована у open source застосунку Anafora, що також може бути використано при розробці подібних застосунків.

1 АНАЛІЗ ІСНУЮЧИХ ТЕНДЕНЦІЙ МОНІТОРИНГУ КОРИСТУВАЧА ДЛЯ ВИРІШЕНЬ ЗАВДАНЬ БЕЗПЕКИ

Продуктивність роботи підприємства безпосередньо залежить від результатів роботи його співробітників. Виховання таких якостей як сумлінність та ініціативність у робочих, необхідно контролювати їх комфортне і безпечне інформаційне середовище. Тому особливу увагу приділяють аналізу та моніторингу роботи співробітника.

Методи за допомогою яких проводиться контроль роботи співробітників [1]:

1. Проведення meet up'ів - підвищення мотивації, необхідності контролювати потік інформаційних потів і дотримання політик безпеки, перегляд динаміки виконання завдань, при чому не тільки вирішених, а й тих, що знаходяться на стадії виконання;
2. Метод таємний клієнт - заздалегідь підготовлений клієнт з правдоподібною легендою і проблемою, яка є слабкою ланкою в забезпеченні безпеки, виконанням якої займуться працівники персоналу підприємства;
3. Встановлення нормативів (KPI, key performance indicators) - автоматичний контроль якості виконання співробітником своїх обов'язків. За значеннями KPI судять про ступінь досягнення цілей діяльності. Це захід, що дозволяє прямо або побічно оцінити, наскільки ми досягли ту чи іншу мету.
4. Дошка мотивацій;
5. Система розвитку та контролю роботи співробітників - система, що включає комплекс заходів, що сприяють фіксації дій персоналу, який працює за ПК: захищає конфіденційну інформацію компанії від її поширення «третім особам» і встановлює ефективність роботи конкретного співробітника.
6. Також впроваджується Scrum – гнучка методика для розробки продуктів чи виконання певних коротко- чи довгострокових проектів.

Ці методи прямо чи опосередковано використовуються і для підвищення рівня виконання вимог політики безпеки підприємства.

Розглянемо систему контролю роботи співробітників за допомогою яких здійснюється моніторинг. Найпопулярнішими є 3 методи контролю, що відображають дії співробітника протягом робочого дня, та не втручаються в його особистий простір :

1. Відеоспостереження[1];
2. Програми-шпигуни на робочий комп'ютер;
3. Програми обліку робочого часу.

Установка відеоспостереження - підходить для фірм, співробітники якої не сидять на одному місці. Зроблені протягом робочого дня записи дадуть повну картину зайнятості персоналу: хто що робив, відлучався чи ні, як довго був відсутній і т. д.

Установка програм-шпигунів або програм обліку робочого часу - метод, найбільш підходящий для фірм, співробітники яких працюють в офісі за ПК. Такі програми збирають майже всю активність користувача за комп'ютером. Їх використання приносить користь бізнесу. Хоча розробники настійно рекомендують повідомляти співробітників про встановлення на їх ПК дане програмне забезпечення. Мінусом цих програм є те, що їх поведінка схожа з вірусним, різниця лише в тому, що дані йдуть визначеній людині - адміністратору системи безпеки. Також, якщо на комп'ютер працівника ставиться антивірус, то з великою ймовірністю ці програми будуть конфліктувати, а налаштування займе багато часу.

Роботодавці віддають перевагу програмі обліку робочого часу [2], так як вона видає інформацію, відсортовану за категоріями. При її установці співробітники не відчувають абсолютно ніякого дискомфорту, вони можуть вільно використовувати свій ПК як на робочому місці, так і віддалено, якщо співробітник працює поза офісом, для цього система фіксує час його роботи і відвідувані протягом дня ресурси, при цьому контролюючи інформаційні потоки всередині мережі. Правильно підібрана система надає керівнику можливість знати про всі дії підлеглих. Іноді, для підвищення ефективності контролю використовують 2 методи, додаючи відеоспостереження або комбінуючи їх.

1.1 Виділення основних підходів до реалізації механізмів моніторингу та його напрямки при використанні контролю інтернет активності користувача для забезпечення інформаційної безпеки

При дослідженні робочого процесу кожного працівника підприємства, який використовує засоби веб на робочому місці, можна використовувати як засоби для моніторингу, так і безпосередньо системи керування інформаційною безпекою.

Виділимо основні підходи:

1. Використання десктопних застосунків, здатних відслідковувати інтернет трафік, та забороняти доступ до веб ресурсів при необхідності;
2. Використання JavaScript бібліотек, розширень браузера чи веб застосунків для моніторингу активності працівника в інтернеті чи на певному порталі;
3. Використання DLP та SIEM систем для контроля інформаційних потоків.

1.2 Десктопні застосунки з можливістю відслідковувати інтернет трафік

Були обрані кращі як комерційні, так і безкоштовні інструменти для контролю робочого столу співробітників за критеріями [3]:

1. Збір інформації про запущені програми і час їх роботи;
2. Інформація про відвідані сайти - збір інформації про відвідані сайтах і час перебування на них;
3. Активність співробітника - розподіл активності співробітника на продуктивну і непродуктивну;
4. Графік роботи - налаштування робочих графіків для окремих користувачів і груп;
5. Перегляд робочих столів[5] - перегляд робочих столів (екранів) співробітників в реальному часі для всієї організації або ж зняття snapshot в певні моменти часу;
6. Контроль порушень - контроль порушень і підозрілих подій онлайн;
7. Звіти щодо порушень - звіти порушень і підозрілих подій (початок, тривалість, інтенсивність);

8. Перехоплення повідомлень - перехоплення відправлених і прийнятих повідомлень (пошта, месенджери);
9. Перехоплення документів - перехоплення документів та їх копіювання для аналізу.

Варто відмітити, що пункти 1, 2, 4-9 мають пряме відношення до контролю дотримання організаційних вимог з боку безпеки, в той час як пункт 3 має посереднє до цього відношення. Незважаючи на це, по активності співробітника ми можемо встановлювати, чи є його активність аномальною або в зоні допустимої поведінки. Аномальна поведінка може свідчити про порушення безпеки (від імені діє інший користувач або процес, даний користувач діє під впливом певних обставин - наприклад, психологічного тиску, соціальної інженерії і т.д.). Саме цю проблему вирішує веб-портрет користувача.

1.3 JavaScript бібліотеки, розширення для браузера чи веб застосунки для моніторингу активності працівника

В той час як десктопні застосункі мають повний контроль над інформаційними потоками даних, їх використання потребує встановлення, налаштування, та залучення фахівців на стороні, що не завжди є вигідним та безпечним для керівника чи адміністратора підприємства та комфортним для працівників, за якими спостерігають сторонні люди. Вирішенням цієї проблеми - є використання JavaScript модулів, які допомагають непомітно моніторити роботу працівника завдяки впровадженню необхідного функціоналу в портал. Якщо ж необхідній крос доменний моніторинг, то використовують розширення для браузера чи веб застосунок, встановлення якого набагато простіше, а використання не спричиняє дискомфорт для користувача такого застосунку. При цьому можна використовувати як готові рішення, які обробляють дані анонімно, пов'язуючи зібрану статистику тільки з локальною адресою комп'ютера. А ось інформація про закріплений ПК за певним користувачем міститься тільки у системного адміністратора або засновника підприємства. Якщо робоче середовище працівника має розроблений веб-інтерфейс, то можна дописати певні

JavaScript модулі до цього застосунку, для моніторингу та додання захищеності цьому ресурсу.

1.4 Опис наявних платформ та сервісів із використанням JavaScript та їх можливостей для моніторингу користувачів

Найширшою сферою використання даних моніторингу користувачів в браузері є маркетинг та machine learning, метою яких є підвищення рівня продажу своїх товарів, персоналізація кожного користувача, та підбір підходів для продажу певної продукції. Тому найуспішніші модулі використовуються саме в цій галузі.

1.4.1 Google analytics

Google analytics - сервіс, що надається Google для створення детальної статистики відвідувачів веб-сайтів[6]. Статистика збирається на сервері Google, користувач тільки розміщує JS-код на сторінках свого сайту. Код відстеження спрацьовує, коли користувач відкриває сторінку в своєму веб-браузері (за умови дозволеного виконання Javascript у браузері).

Опишемо налаштування для запровадження засобів Google Analytics.

Код, що потрібно помістити на початок кожної сторінки виглядає приблизно так:

```
<script>
 (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||
   function(){
    ( i[r].q=i[r].q||[]).push(arguments)}, i[r].l=1*new Date();
      a=s.createElement(o)m=s.getElementsByTagName(o)[0];
      a.async=1; a.src=g; m.parentNode.insertBefore(a,m)}
     )( window,document, 'script','//www.google-nalytics.com/analytics.js',   'ga');
 ga('create', 'UA-51939022-1', 'slaviali.ru'); ga('send', 'pageview');
</script>
```

Крім цього, додання коду відстеження в саму верхню частину вихідного коду сторінок гарантує, що браузер при розборі цього коду (починаючи зверху і йдучи вниз) активує виконання скрипту Analytics[7].

Тому, навіть якщо користувач піде до закінчення завантаження сторінки, його взаємодія з вашим сайтом буде враховано. Код Analytics виконується асинхронно, тобто запускається на задньому фоні, поки браузер виконує інші завдання по завантаженню елементів веб-сторінки. Це знову ж таки дозволяє почати збирати дані ще до повного завантаження сторінки.

Після того, як код відстеження на даній сторінці виконався, система створює анонімні унікальні ідентифікатори, призначені для відмінності користувачів. Існує кілька способів створення таких ідентифікаторів. За замовчуванням, Google Analytics використовує власний файл cookie, але є можливість створити і використовувати свій власний ідентифікатор.

При завантаженні сторінки JavaScript код лічильника збирає інформацію про сам веб-сайт, наприклад, URL адресу поточної сторінки. Також лічильник збирає інформацію про браузер, в якому ця сторінка відкрита, наприклад, його назва, налаштування мови і операційну систему, під керуванням якої працює цей браузер. Вся ця інформація пакетується і відправляється на сервер Google у вигляді хіта перегляду сторінок. І цей процес повторюється щоразу, коли в браузері завантажується сторінка.

Варто зазначити, все цей код буде працювати і без будь-яких попередніх налаштувань. Достатньо реєстрації в Google Analytics, отримати код і все буде працювати. Також є додаткова можливість налаштування коду, що дозволяє збирати більше інформації про користувачів, їх сеанси (сесії) і взаємодії з вашим сайтом.

Засоби Google Analytics дозволяють робити: рекламні звіти, проводити імпорт даних витрат, робити вимірювання мобільних оголошень, ремаркетингу, проводити пошукову оптимізація, пошук розширених сегментів, робити анотації, експерименти з вмістом, настроювані звіти, звіти в режимі реального часу, робити аналіз аудиторії та звітність, збирати дані про Браузер / ОС, візуалізувати потоки, накладати карти,

відслідковувати мобільний трафік, робити соціальні звіти, сканувати джерела трафіку, застосовувати фільтри, налаштовувати дозволи для користувача, робити звіти про збої і винятки, збирати дані про цільовий потік, багатоканальні послідовності, сповіщення, інтелектуальні події, відстеження подій, аналітика на сторінці, пошук по сайту, робити аналіз швидкості сайту;

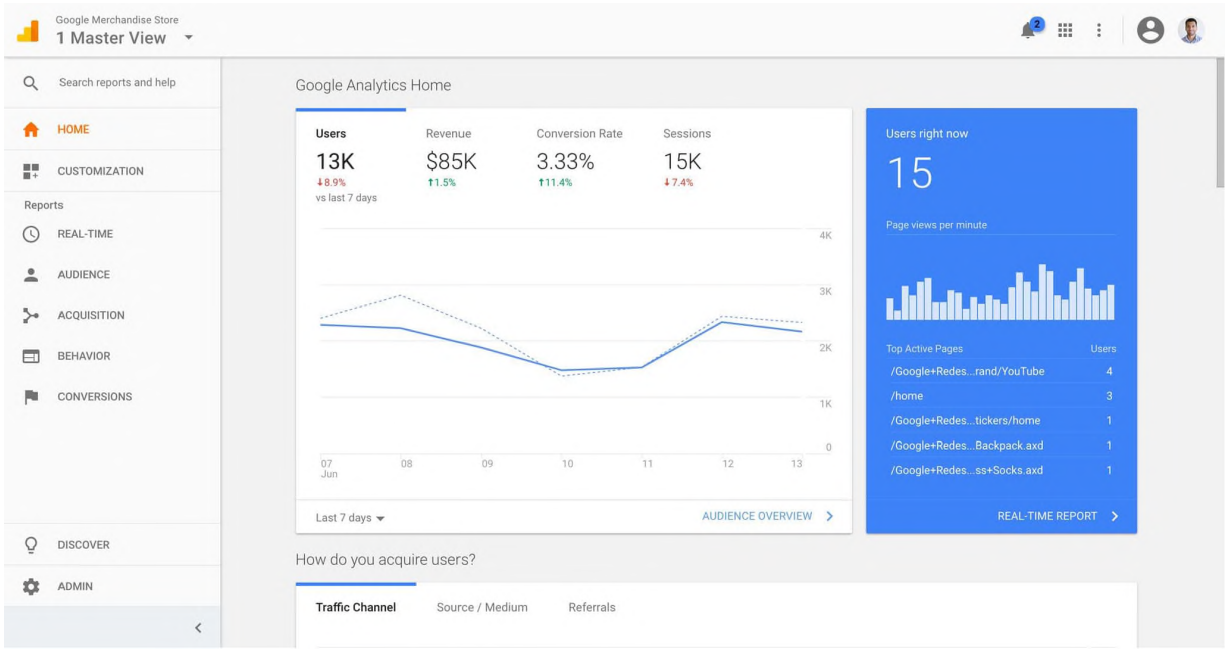

Рисунок 1.1 - Базовий інтерфейс веб-застосунку Google analytics

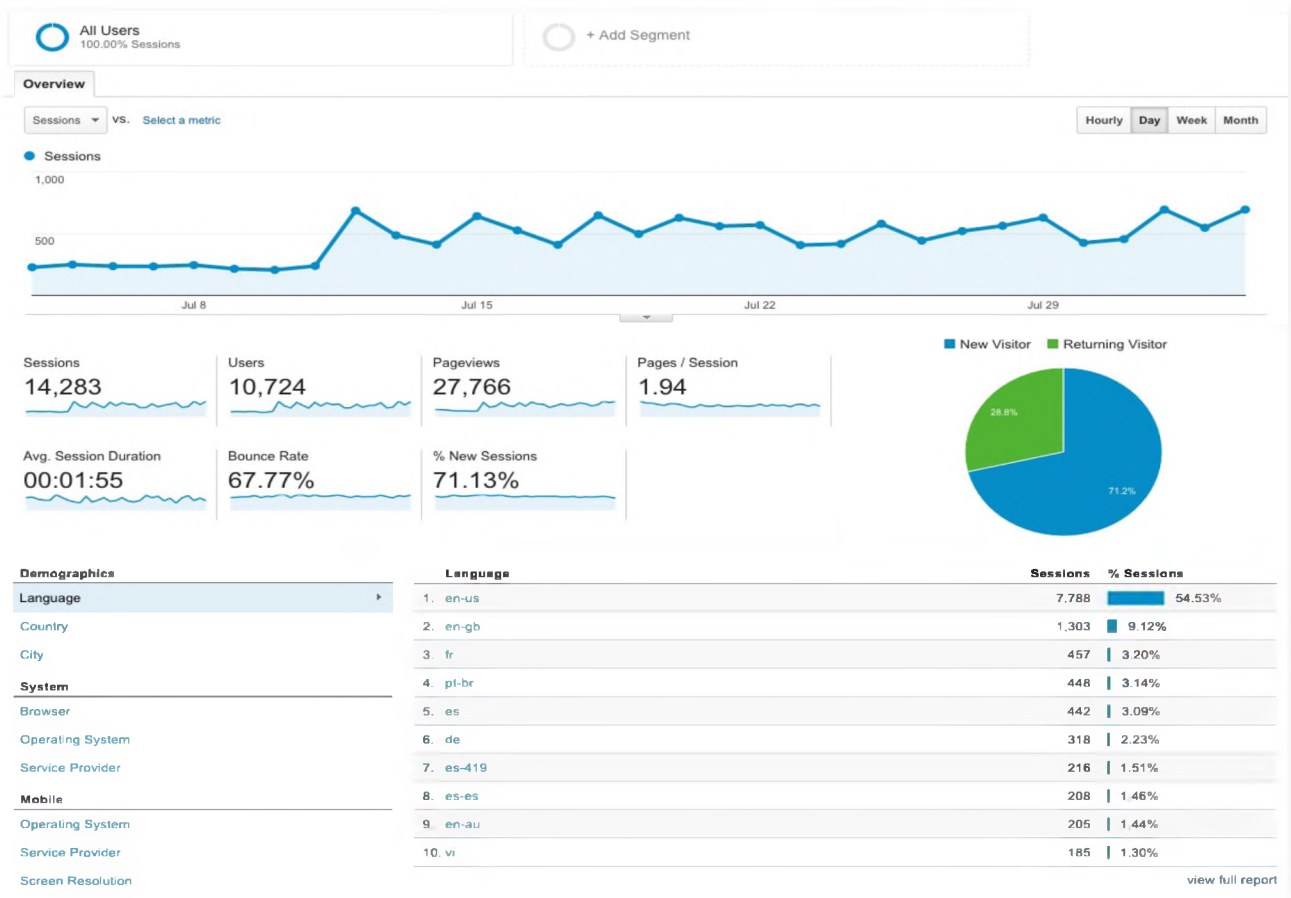

Рисунок 1.2 - Сторінка перегляду статистики користувачів та мов

1.4.2 Clicktale

ClickTale - система веб-аналітики, застосування якої дозволить зібрати масу корисних для аналізу даних про відвідувачів сайту.

Ця програма дозволяє робити:

1. Відео-записи відвідувань сайту

Всі відео записи збираються в спеціальному звіті Recordings[9]. У списку для кожного запису визначається тривалість відвідування, джерело відвідувача. Будь-який запис можна скачати на локальну машину для перегляду, або переглянути прямо в веб-браузері. В системі передбачені спеціальні фільтри, які дозволяють відфільтрувати необхідні записи відвідувань за певними параметрами. Фільтри легко можуть комбінуватися між собою, тому можна швидко відсіяти записи відвідувань відвідувачів.

Рисунок 1.3 - Відеозаписи відвідувань порталу

2. Відстеження цільових дій

Крім стандартних параметрів фільтрації відео-записів відвідувань ClickTale пропонує гнучкий інструмент Events, який дозволяє фіксувати певні ключові дії на сайті: скачування файлів, оформлення замовлення, відправка заявки і так далі. З технічної точки зору використання подібних подій на увазі невелику модифікацію вихідного коду сайту шляхом додавання спеціальної JavaScript функції до відповідних об'єктів (деякий аналог TrackPageview () з віртуальними сторінками в Google Analytics).

3. Теплові карти

Теплові карти накладаються на сторінки сайту і являють собою агреговані дані, які описують поведінку відвідувачів в рамках окремо взятих сторінок. Clicktale пропонує 4 види теплових карт[8]: карти, засновані на русі миші; карти, засновані на кліки миші; карти, засновані на увазі відвідувачів; карти, засновані на глибині скролінгу.

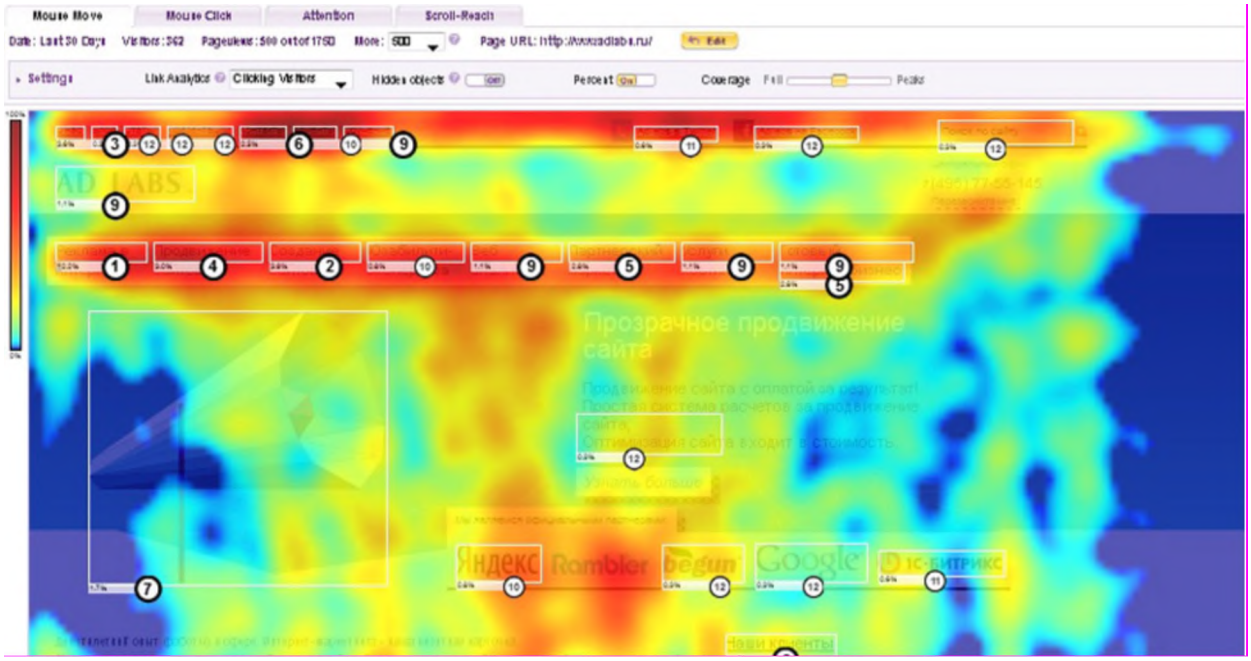

Рисунок 1.4 - Теплова карта заснована на русі миші

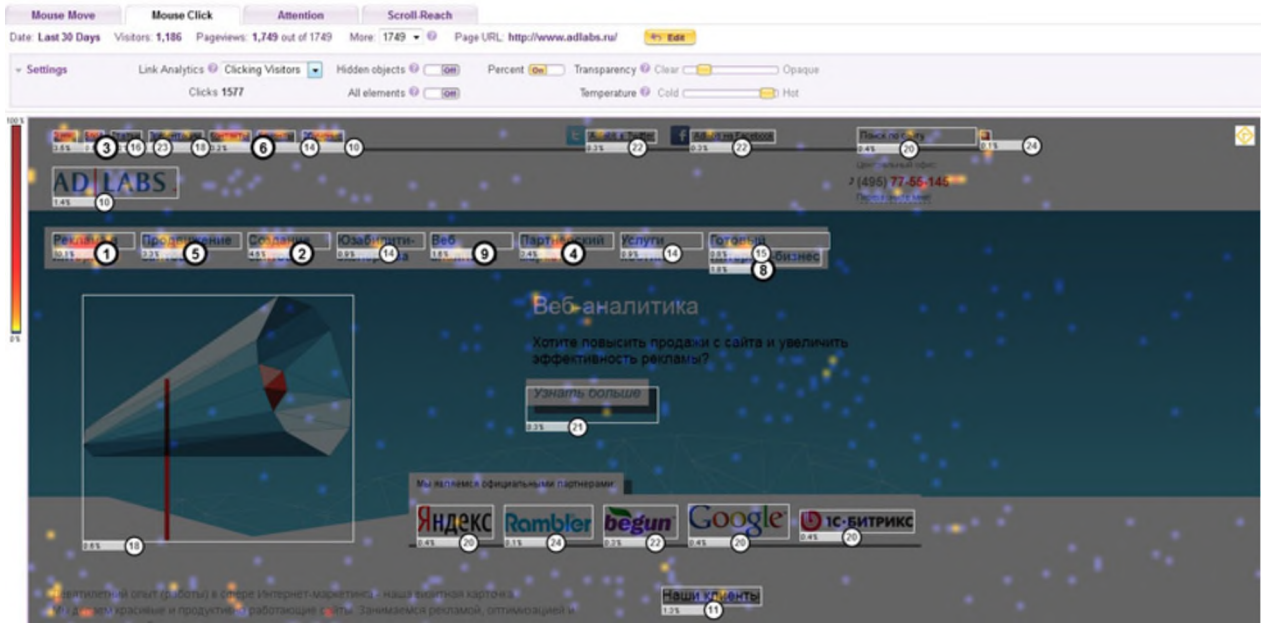

Рисунок 1.5 - Теплова карта заснована на кліках миші

Аналізуючи всі чотири теплові карти, можна зрозуміти, як відвідувачі сприймають ту чи іншу сторінку, наскільки очевидні для них ключові об'єкти і т.д.

На теплових картах також наводиться статистика для посилань, які перебувають на сторінці. Вона включає в себе такі показники як: кількість кліків по посиланню, середній час, який курсор провів над посиланням перед кліком, відсоток наведень на

посилання, які закінчилися кліком, і т.д. У відповідність з обраним показником ClickTale визначає рейтинг для кожної з посилань сторінки.

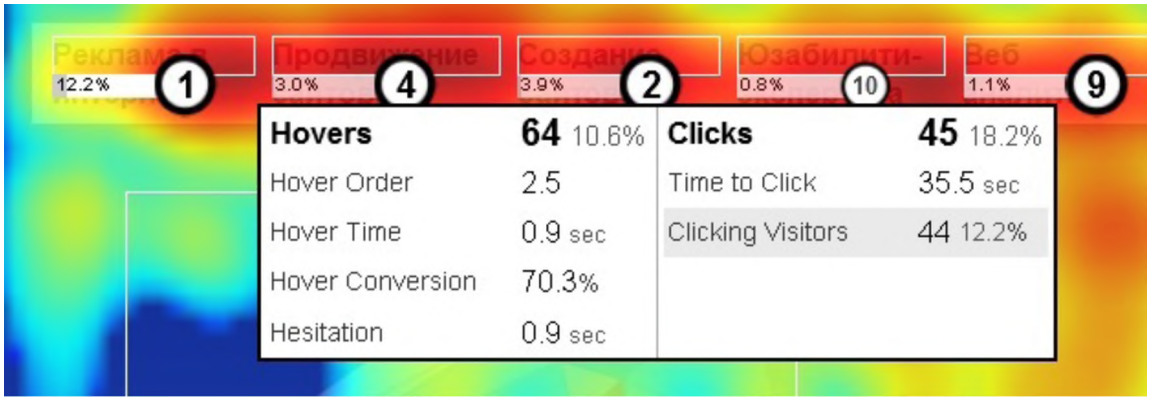

Рисунок 1.6 - Статистика посилань на сторінці

4. Тунелі конверсій.

Тунелі конверсій ClickTale дозволяють проаналізувати поведінку користувачів на кожному з кроків проходження форм і зрозуміти, який з них може відштовхувати відвідувачів. Усунення виявлених проблем дозволить знизити відмови відвідувачів і підвищити кінцеві показники конверсії [8].

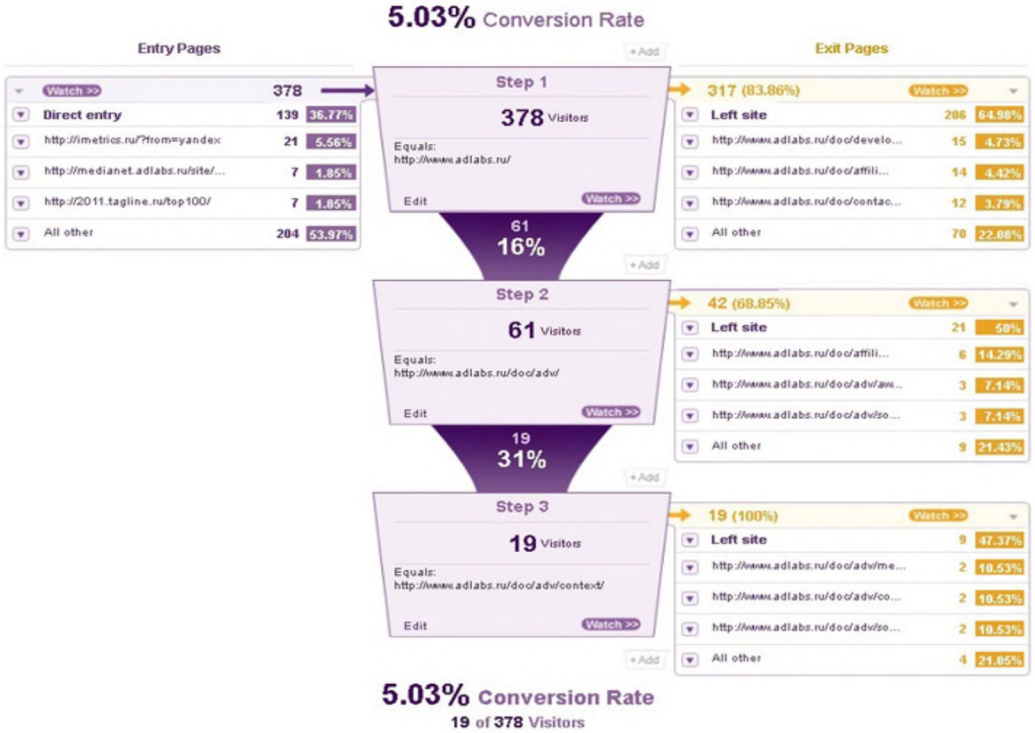

Рисунок 1.7 - Тунелі конверсій

5. Аналіз взаємодії з формами.

Форми один з найбільш популярний способів взаємодії відвідувачів з сайтом. Вводячи необхідні дані в поля форми, відвідувачі оформляють замовлення, підписуються на новинні розсилки, відставляють заявки на зворотний дзвінок і так далі. Заповнення форми є одним з кроків на шляху відвідувача від залучення на сайт до кінцевої конверсії, тому, як і інші кроки, він потребує аналізу і подальшої оптимізації. Цей інструмент дозволяє: робити звіт по конверсії, звіт по відмовах, звіт за часом взаємодії, звіт по порожніх полях, звіт по повторне заповнення.

6. Консоль сторінки.

Звіт, який збирає всі основні дані по певним сторінках сайту: час на сторінці, кількість переглядів, найбільш популярні попередні і подальші переглянуті сторінки, швидкий доступ до теплових карт тощо.

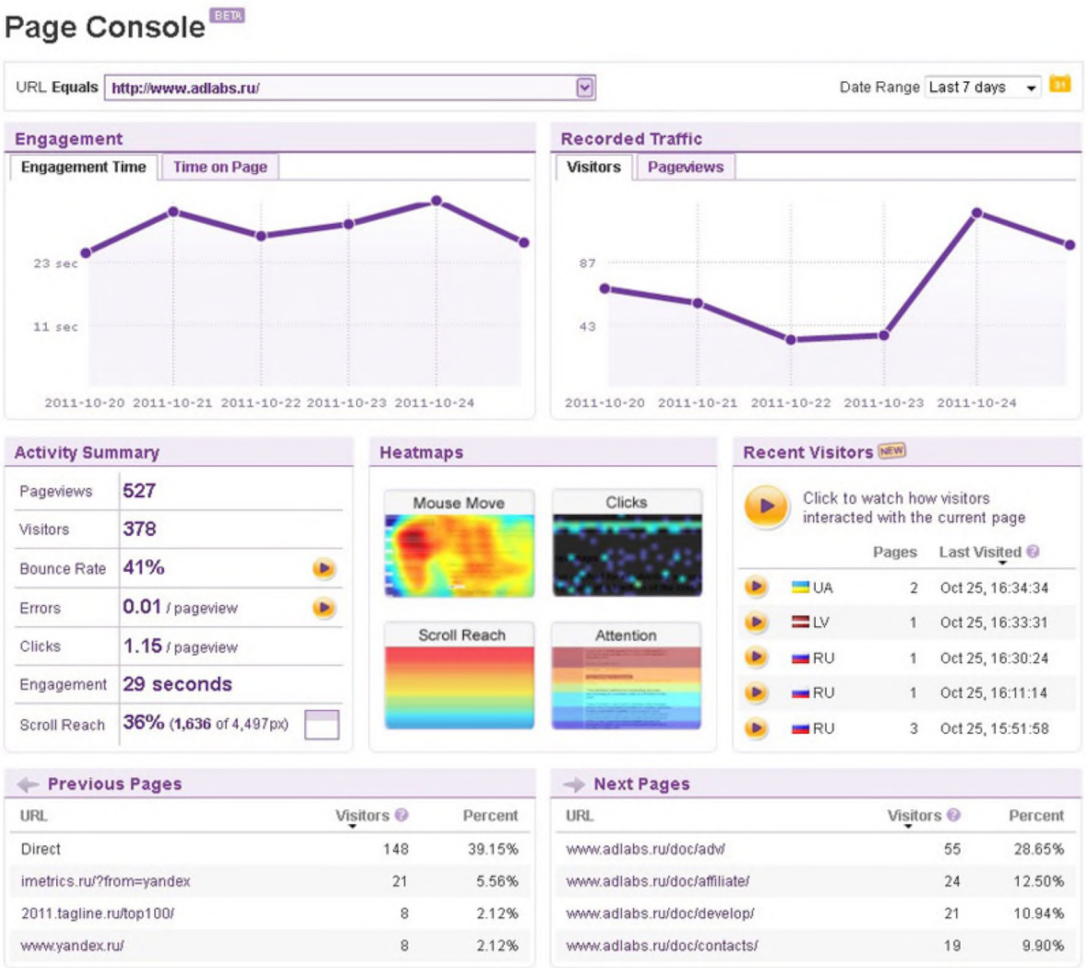

Рисунок 1.8 – Консоль сторінки

1.4.3 Segment.io

Segment.io - це платформа, яка збирає, зберігає і направляє дані на сотні інструментів для аналітики. При чому інструментами можуть бути власні модулі.

При запуску бібліотек Segment.io для iOS і Android, буде підтримуватися відправка даних в ряд послуг мобільної аналітики, включаючи Countly, Mixpanel, Localytics, Flurry, Google Analytics та інші. Нові бібліотеки забезпечать гнучкість мобільних розробок, так як тепер вони зможуть розгорнути бібліотеку аналітики Segment.io тільки один раз, а потім включити або відключити служби всередині Segment.io, з якими вони хочуть працювати [10].

Крім того, шляхом proxying даних через сервери Segment.io бібліотеки вперше надають мобільним розробникам доступ до Marketo, HubSpot, Customer.io, Vero, Klaviyo, Pardot, Woopra, Help Scout, Librato, Outbound.io і Salesforce [10].

Рисунок 1.9 - Принцип роботи Segment.io

1.4.4 Extrawatch

ExtraWatch - це платформа вимірювання продуктивності веб-сайту, яка аналізує активність відвідувачів, контролює завантажені файли, відстежує кліки та створює теплову карту, виявляє і звітує за ключовими словами і т. д.

Характеристики:

7. Аналізує взаємодію відвідувачів в режимі реального часу.
8. Здійнює моніторинг активних точок кліка через HeatMaps. Працює на платформах Joomla, Magento, Prestashop і Wordpress, через плагін або код відстеження, якщо використовується інша система управління контентом.
9. Проводить трекінг ключових слів і фраз, які привели користувачів на сайт для поліпшення SEO. Трекінг елементів які найбільш активні [10].
10. ExtraWatch використовується для збільшення проведеного часу на сайті і знижує показник відмов і доглядів шляхом відстеження кліків на різних кнопках і посиланнях, а також оптимізує цільові сторінки для поліпшення конверсій.

1.4.5 Mouseflow

Mouseflow - сервіс, що відслідковує поведінку користувачів на сайті, ґрунтуючись на русі миші і прокручуванні веб-сторінок. Містить відразу кілька інструментів, які допомагають аналізувати аудиторію ресурсу для подальшого підвищення конверсії та поліпшенні юзабіліті [11].

Платформа, в першу чергу, розрахована на маркетологів для вивчення ефективності контенту і аналізу воронок продажу. Завдяки відеозапису дій користувачів, можна зробити висновки, чому потенційний покупець не придбав товар. Пропонується широка лінійка тарифів, розраховану як на невеликі сайти, так і на великі інтернет-магазини.

Після встановлення JS-коду на сайт, сервіс відстежує дії кожного користувача і записує відео, подивитися яке можна в зведеній таблиці - поряд з інформацією про те,

з якого джерела прийшов відвідувач, скільки часу провів на сторінці і які дії виконав. Mouseflow генерує теплові карти по заданих сторінок: з них можна дізнатися, які посилання і товари привернули аудиторію, на що і скільки разів кликали, який відсоток сторінки прокручений. Можна подивитися, скільки часу у відвідувачів займає заповнення реєстраційної форми та яка частка аудиторії погоджується пройти опитування.

Можливості сервісу:

1. Відеозапис активності миші і прокручування сторінок. Mouseflow відстежує кліки, рух миші, форми і багато іншого. Показує анонімну запис активності від кожного відвідувача на вашому сайті - точно так само, як і CCTV. Краще за все, ви можете фільтрувати сеанси, щоб знайти ті, у кого є розчаровані користувачі, помилки, проблеми сумісності і багато іншого [12].

   Це усуває здогади, тому ви можете вирішувати проблеми оперативніше. І це швидко, безпечно, зручно для мобільних пристроїв і підтримує сторінки перевірки, динамічного контенту або учасників.
2. Теплова карта. Mouseflow надає карти для анонімного узагальнення, де люди клацають / торкаються, переміщують курсор миші, прокручують, звертають увагу і знаходяться. Застосунок показує ключові етапи поведінки в простому, зручному для читання форматі.

   Це дозволяє легко виявити те, що працює, а що ні. Також підтримує налаштування діапазони дат, мобільні і адаптивні макети, а також тести A / B або split [11].
3. Відстеження воронок. Mouseflow відстежує активність зі сторінки на сторінку на певному сайті. Це допомагає проаналізувати виходу с сайту і пов'язані процеси (наприклад, вхід або реєстрація). Надає можливість створювати звіти для вивчення поведінки відвідувачів.
4. Робота з формами. Mouseflow контролює взаємодію відвідувачів з формами. Він вимірює скидання, порожні відправки, помилки і т. д. - для кожного поля відповідної форми - і такий звіт може бути відфільтрований в реальному часі.

Це допоможе вам виявити проблеми, поліпшити зручність використання і збільшити кількість конверсій між різними сегментами відвідувачів [12].

Збір інформації про поведінку кожного користувача окремо. Mouseflow дозволяє легко аналізувати відвідувачів. Ви можете створювати користувацькі інтерактивні опитування для цільової аудиторії в лічені секунди. Це дає цінний зворотний зв'язок, коли це має найбільше значення: оскільки, якщо відвідувачі розчаровані, вони переживають проблеми та потребують допомоги.

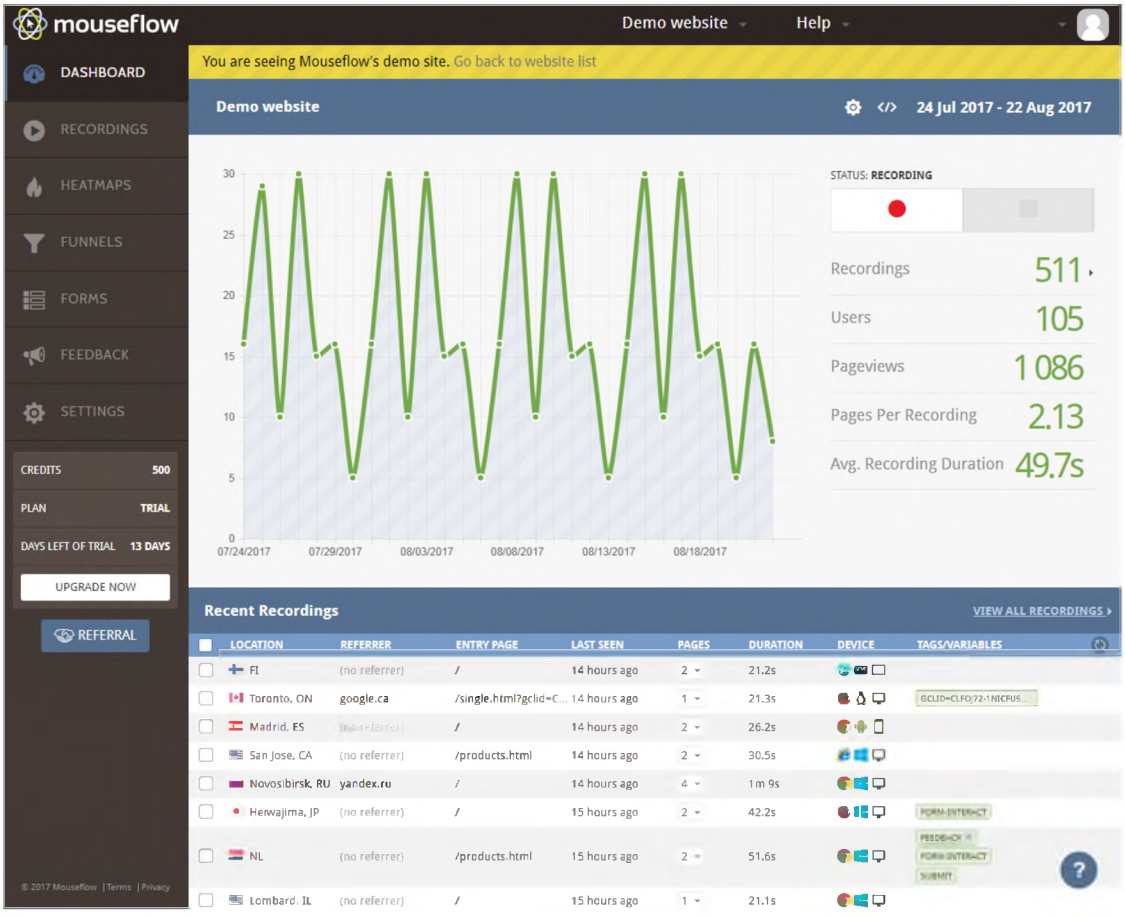

Рисунок 1.10 – Загальна характеристика відвідуваності веб-сайту

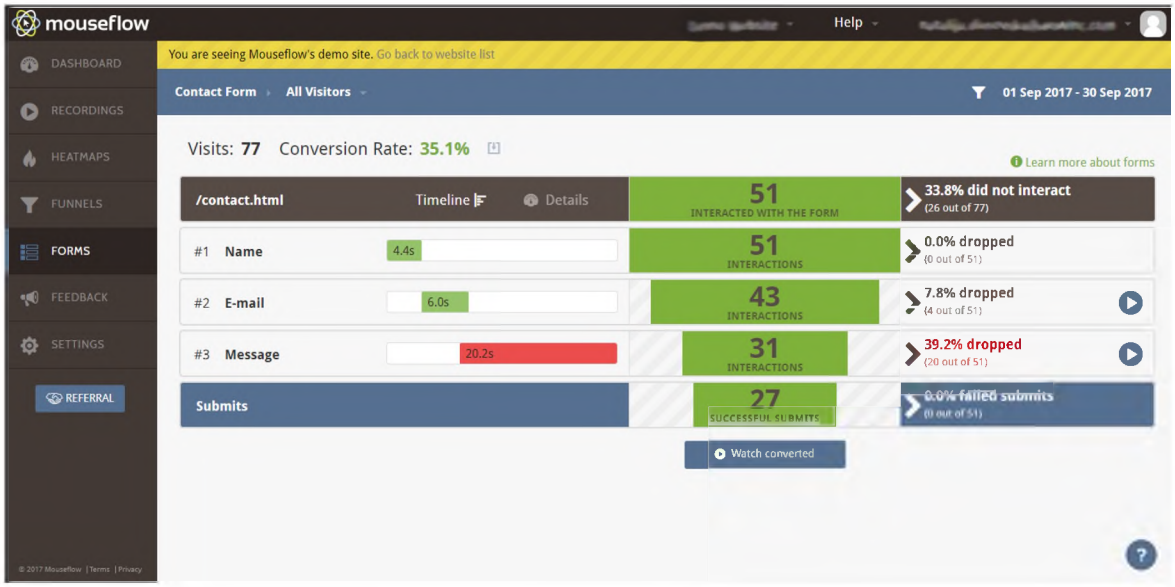

Рисунок 1.11 – Взаємодія користувачів з формами

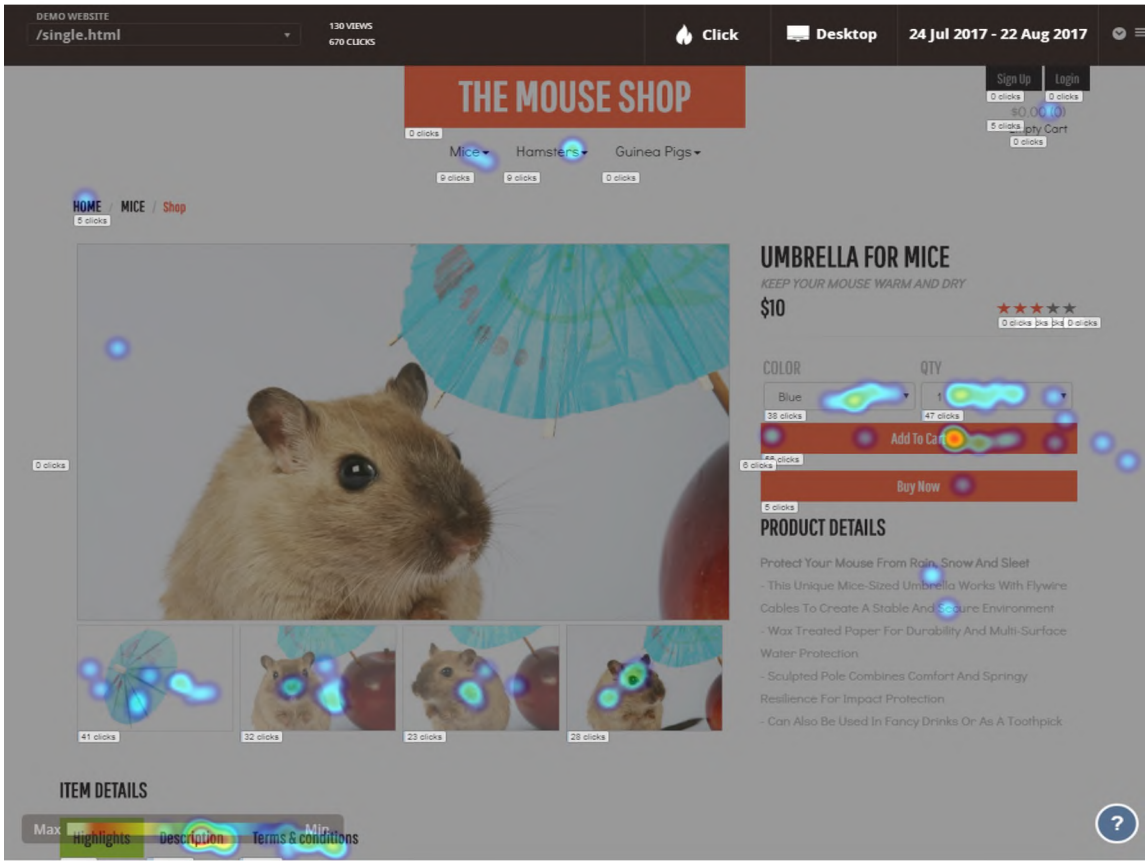

Рисунок 1.12 – Теплова карта заснована на кліках миші

1.4.6 SeeVolution

SeeVolution - це інструмент аналізу веб-аналітики, який дозволяє вам зрозуміти поведінку відвідувачів на вашому веб-сайті.

Цей застосунок включає надання таких почлуг:

1. Site and Page Analytics: інструмент аналітики, відстежує загальні кліки [13];
2. Модуль для відстеження гарячих / холодних точок, на кожній сторінці вашого порталу;
3. Eye Tracking: перегляд рухів миші на сторінці відвідувача;
4. Карту прокрутки уваги - як далеко прокручується кожна сторінка;
5. Розширені фільтри: результати фільтрації за типом пристрою, джерелами або географічним розташуванням;
6. Живі кліки [13]. Зворотній зв'язок про зміни і кампанії. Кожен клік з'явиться на мапі LIVE. Функція масштабування дозволяє отримати краще уявлення про геолокації аудиторії. Можливість фільтрації своїх цілей для взаємодії відвідувачів з конкретними ресурсами.
7. Записані сеанси: забезпечує близьке і особисте уявлення про досвід користувача. Немає буферів. Можливість ефективного налаштування конкретних сценаріїв, використовуючи відфільтровані записані сеанси по країнам, кількість переглянутих сторінок і тривалість сеансу [14].
8. Уявлення за лаштунками. Є опція збільшення кількості гарячих точок на сайті, щоб дізнатися, хто з користувачів відвідає "гарячу" точку: звідки вони з'явилися, як вони потрапили на сайт, яку платформу і браузери вони використовують.
9. Аналіз активів. Функція аналізу активів покаже, як залучати кожне зображення, посилання і форму, і в режимі реального часу.
10. Аналіз форми: Оптимізація форми, щоб відвідувачі частіше натискали в «Відправити». Можливість дізнатися скільки користувачів заповнило кожне поле і скільки часу пройшло.

11. Задання цілей. Задання цілей, можливість аналізувати кампанії і отримувати результати встановлених цілей [14].

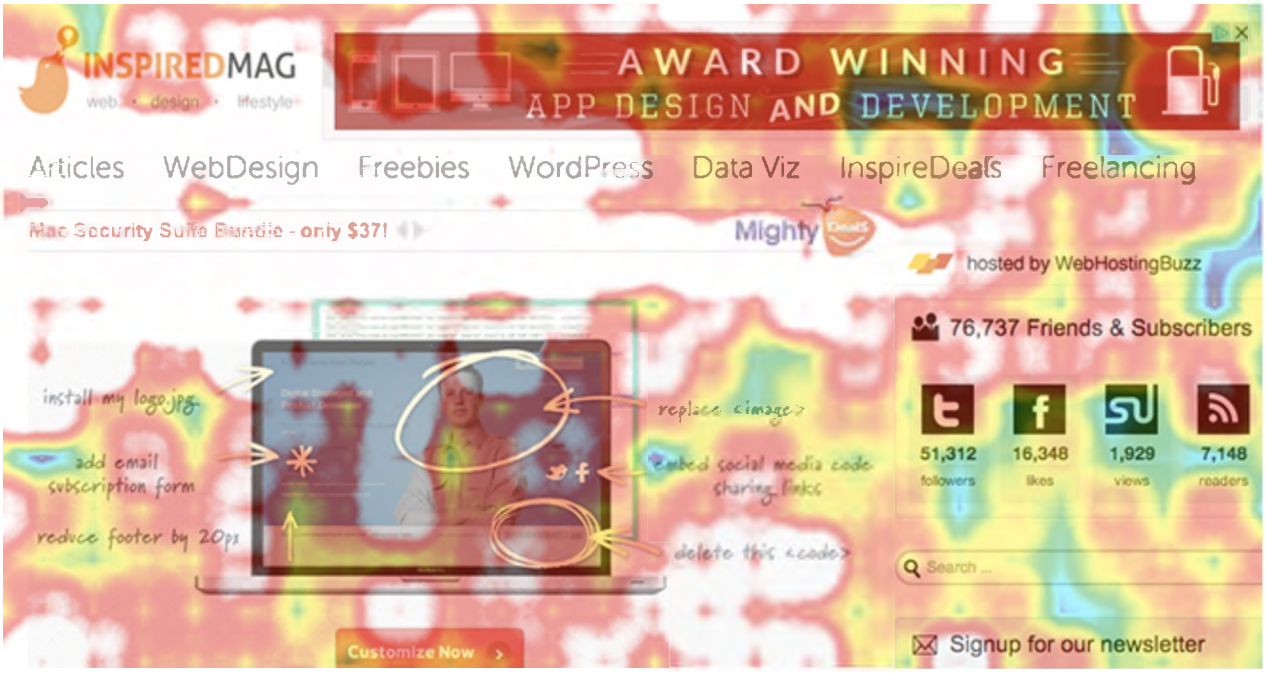

Рисунок 1.13 – Теплова карта заснована на русі миші

1.4.7 Розширення для Google Chrome чи Mozilla Firefox

При необхідності моніторингу активності працівника в усьому браузері, можна використовувати розширення для браузерів, які дозволяють збирати обмежену статистику у всіх вікнах. Виділимо два загальнодоступних инстумента - Webtime Tracker і Browsing ActivityTracker [15]. Вони не вимагають авторизації, а також дозволяють скачати вихідний код цих розширень і налаштувати їх під себе. Дозволяють робити резервне копіювання і відновлення, експорт логів в файли CSV формату, скріншоти, працюють в автономному режимі і мають алгоритми вимірювання часу, вважають час на сайті, тільки коли вікно Chrome активно. Також такі застосунки можуть відправляти логи чи іншу інформацію на сервер.

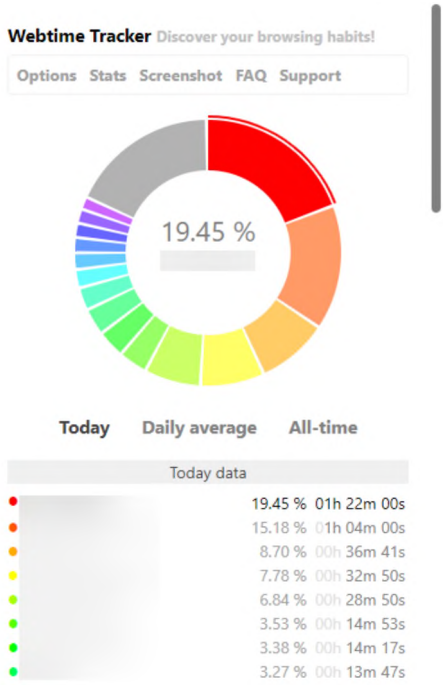

Рисунок 1.14 – Рисунок інтерфейсу розширення для браузера

1.4.8 Написання власних модулів

Написання власних модулів і їх впровадження до робочого середовища працівників надає можливість власноруч налаштовувати лише ті засоби та заходи, які необхідні на вашому ресурсі для моніторингу активності да діяльності робітників. Такі модулі є досить гнучкими, та динамічними, дозволяють швидко змінювати та додавати новий функціонал, при необхідності. Їх можливості залежать лише від засобів мови програмування, в даному випадку JavaScript, та браузера, на якому працюють співробітники.

1.5 Використання DLP та SIEM систем

В той час як десктопні застосунки мають повний доступ до даних працівника, існують певні системи, які відстежують тільки інформаційні потоки в корпоративних мережах. Такі системи називаються DLP(Data Loss Prevention) и SIEM(Security information and event management).

DLP - система, створена для запобігання витоку конфіденційної інформації за межі корпоративної мережі. Будується ця система на аналізі потоків даних, що проходять в мережі підприємства. У разі спрацювання певної сигнатури і виявлення передачі конфіденційної інформації, система або блокує таку передачу, або посилає повідомлення уповноваженому працівнику сигнал тривоги. Таким працівником зазвичай є або системний адміністратор, або офіцер безпеки.

Основними вимогами до таких систем є:

- вартість комплексу;
- зручність використання;
- модульність системи [16];
- чи може продукт все контролювати або необхідно закуповувати різні модулі для контролю певних каналів витоку інформації і кількість контрольованих каналів.

SIEM - забезпечує аналіз в реальному часі подій (загроз) безпеки, що виходять від мережевих пристроїв і додатків. SIEM представлено застосунками, приладами або послугами, і використовується також для логування даних і генерації звітів з метою безпеки. SIEM сама по собі не здатна нічого запобігати [17]. Якщо інцидент в ній зареєстрований, то він вже стався. Інша розмова - що могло не бути продовження інциденту.

SIEM відноситься до систем, які не забезпечують весь заявлений функціонал «з коробки» і без попередньо зробленого ретельного обстеження і подальшого ретельного налаштування під конкретного замовника перетворюються на сміття, головний біль IT-відділу і відповідальних за безпеку.

При правильному налаштуванні дана система забезпечує:

- управління журналами даних, зібраних з різних джерел - мережеві пристрої і сервіси, датчики систем безпеки, сервери, бази даних, застосунки;
- автоматизований аналіз корелюючих подій і генерація оповіщень (загроз) про поточні проблеми.
- відображення діаграм, які допомагають ідентифікувати патерни відмінні від стандартної поведінки.

- застосування довготривалого сховища даних в історичному порядку, можливість пошуку по безлічі журналів на різних вузлах; може виконуватися в рамках програмно-технічної експертизи [18].

Оскільки системи DLP і SIEM пропонують можливість відстежувати лише частково поведінку конкретного користувача, ми не будемо розглядати ці засоби як основні при дослідженні контролю веб-активності користувача і будемо враховувати тільки можливість використовувати їх в комбінації з іншими як допоміжні, для профілактики і контролю інформаційних потоків.

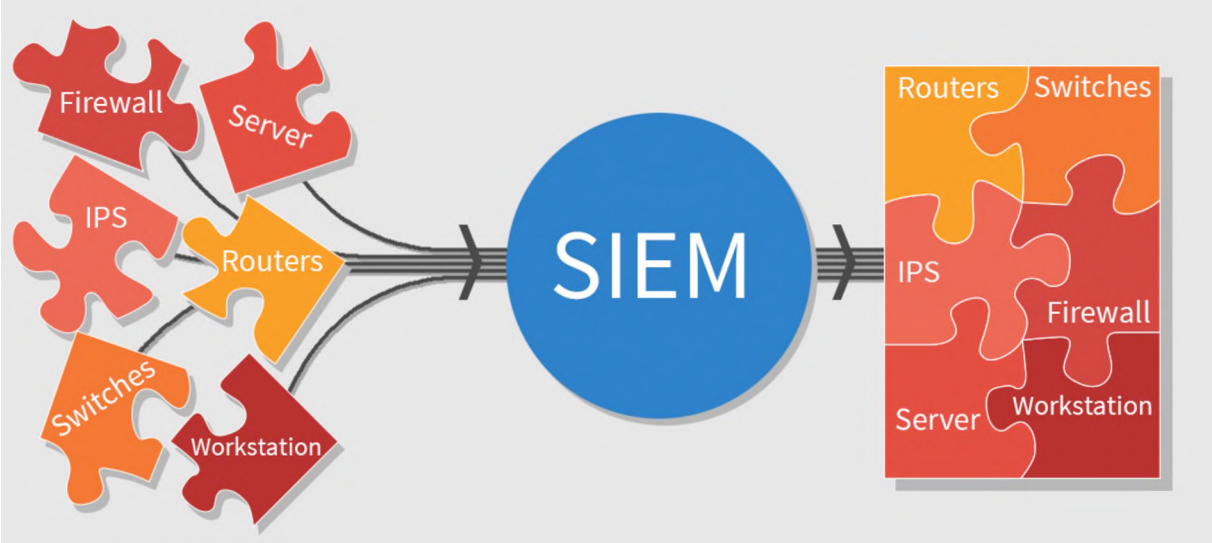

Рисунок 1.15 – Принцип роботи SIEM системи

Висновки до розділу 1

Проаналізовано основні тенденції по існуючим рішенням в сфері моніторингу користувацької поведінки в цілому. Це десктопні застосунки, засоби JavaScript, та DLP та SIEM системи.

Визначено, що для моніторингу саме веб-активності найбільш гнучко можна використовувати JavaScript бібліотеки, платформи і сервіси, з їх допомогою запроваджувати розширення для браузерів, чи розробити власні веб-застосунки, які окрім необхідного функціоналу будуть забезпечувати моніторинг користувача та спостереження дотримання правил політики безпеки.

2 АНАЛІЗ ТА ВИБІР РІШЕНЬ ДЛЯ РЕАЛІЗАЦІЇ МОНІТОРИНГУ, ПОРІВНЯЛЬНИЙ АНАЛІЗ МОЖЛИВОСТЕЙ

2.1 Засоби JavaScript, які можуть бути використані для вирішення задач моніторингу

При популяризації використання веб в бізнес процесах, з'явилася необхідність впровадження політик безпеки і програмних засобів для підтримки безпеки даних і бізнес процесів підприємства в даний сектор. Оскільки дуже багато часу співробітники проводять використовуючи браузер, є сенс використовувати можливості мови програмування JavaScript для застосування можливих заходів безпеки. Підходами до моніторингу працівника підприємства з використання засобів JavaScript можуть бути як власні модулі, так и готові бібліотеки та платформи. Використання цих підходів є двостороннім, тобто вони використовуються як власниками веб-ресурсів, з якими взаємодіють співробітники підприємства (для захисту від ботів та профілактики від загроз), так і власниками підприємств, які мають намір моніторити співробітників при їх взаємодії з зовнішніми ресурсами. Також використання таких методів залежить від того, чи не шкодить збір третіми особами інформації про діяльність підприємства.

JavaScript дозволяє відстежувати працівників і їх дії в браузері, а саме:

1. Число переглядів певної сторінки;
   a. Збираємо дані про вхід на певну сторінку. При вході на сторінку відправляємо дані на сервер з інформацією агента і з якої сторінки був виконаний перехід:

```
<script type="text/javascript" src="https://*****?var=userip"></script>
```

```
// отримуємо змінну userip у глобальній області видимості, яка співпадає з ip адресою користувача
window.onload = function() {
    var xhr = new XMLHttpRequest();
```

```
    var agent = navigator.userAgent;
    var history= document.referrer;
    var timer = new XMLHttpRequest();
    timer.open("POST", "/register-view-adress", true);
    timer.setRequestHeader("Content-Type", "application/json");
    timer.send(JSON.stringify({url: api, agent:agent, userIp: userip}));
}
```

Такі дії потрібні для захисту ресурсу від ботів, запобігання ddos атак, а також від збору статистики. Вирішує завдання спостережності, цілісності і доступності даних.

2. Відстеження подій - взаємодія користувача з контентом, який можна відстежувати незалежно від переглядів сторінок або екранів. Це поняття включає в себе завантаження, кліки по мобільним оголошенням, використання гаджетів, елементів Flash і AJAX, відтворення відео і т. Д .;

   Додати подію на кожен клік, при якому буде виконуватися функція, яка реєструє куди натиснув користувач, в який момент часу.

```
<button onclick="registerClick(event)" typeBtn="shoes" id='buy-
id'>Buy</button>
function registerClick(event) {
    var id = event.target.id;
    var date = new Date();
    var btnType = event.target.attributes.btnType.value;
    var click = new XMLHttpRequest();
    click.open("POST", "/click/", true);
    click.setRequestHeader("Content-Type", "application/json");
    click.send(JSON.stringify({id: id, date: date, type: btnType}));
}
```

Відстеження таких подій допомагає визначити чи реальна людина зараз на сайті чи бот/скрипт; відстежує які дані йдуть на сервер, чи впроваджуються рекламні боти на сайт і який їх вплив і тп. Вирішує завдання спостережності , цілісності і доступності даних.

3. Відстежити скільки разів користувачі натискали кнопки соціальних мереж і надати інформацію як вони взаємодіють з різними соціальними мережами. Також додаємо обробник натискання на кнопки соціальних мереж і

при відправленні даних додаємо сервіс, який вони частіше використовують, наприклад, при авторизації. Вирішує завдання спостережності за користувачем.

4. Вимірювати призначене для користувача час знаходження на певному сайті. При вході на сайт створюємо мітку часу, при цьому сервер разом з відкриттям ресурсу відправляє нам id, і через певний інтервал часу відправляємо серверу цей id і поточний час. Потім на сервері рахуємо час між першим і останнім значенням цього id. Вирішує задачу спостережливості за користувачем.
5. Відстежувати кількість збоїв і де вони відбувалися. Впроваджуємо скрипт, який логує помилки, оптимізує наш сайт. Вирішує проблему доступності та цілісності даних.
6. Відстежувати використання даних з cookie і localStorage та Web кешування сторінки. Додаємо обробник подій і відстежуємо, коли користувачеві «потрібно» взяти дані з cookie або localStorage. Оскільки ці сховища містять інформацію про користувача, які посилають на сервер, то відстеження змін, вирішує проблему спостережливості і цілісності даних користувача.
7. Отримання параметрів екрану. Через об'єкт window.screen. availTop, colorDepth, height, left, orientation.
8. Проводити відстеження спеціальних параметрів, наприклад, зайти на сайт, але не виконати вхід. В основному допоможе вирішити проблему спостережливості, але в окремих випадках вирішує проблему доступності і цілісності даних при відстеженні хто заходить на сайт, в який час доби і тд.
9. Відстежувати використовувані протоколи, список допустимих форматів, визначає версію браузера, версію ОС, деякі з встановлених доповнень браузера, які додаткові проксі-сервери використовуються клієнтом і, скільки разів був виконаний вхід на ресурс. Допомагає розпізнати атаки спрямовані на доступність і цілісність даних.
10. Анонімізація користувача;

11. При взаємодії з ресурсами браузера можна виконати завдання крос доменного відстеження (Google analitycs / analytics.js). Вирішує проблему спостережливості за користувачем.

2.2 Порівняльний аналіз можливостей засобів веб моніторингу

В порівняльному аналізі перерахуємо переваги та недоліки використання розглянутих модулів.

2.2.1 Google analytics

Переваги, які надає Google analytics:

- Рекламні звіти;
- Імпорт даних витрат;
- Вимірювання мобільних оголошень;
- Ремаркетинг;
- Пошукова оптимізація;
- Пошук розширених сегментів;
- Анотації;
- Настроювані звіти;
- Звіти в режимі реального часу;
- Аналіз аудиторії та звітність;
- збір даних про Браузер та ОС;
- накладання карт;
- відслідковування мобільного трафіку;
- сканування джерел трафіку;
- накладання фільтрів;
- налаштування дозволів для користувача;
- звіти про збої і винятки;
- аналіз швидкості сайту.

Недоліки Google Analitycs:

1. Найголовнішим недоліком є те, що компанія може аналізувати дані підприємства для власних цілей, і хоча це не доведено, без вагомих причин краще не використовувати цей модуль.

2.2.2 Clicktale

Переваги, які надає Clicktale:

1. Аналіз поведінки аудиторії, збільшення конверсії;
2. Система зберігає відеозаписи відвідувань;
3. Створює агрегованих теплових карт, що характеризують поведінку відвідувачів в рамках окремо взятих сторінок. Наявність таких карт служить для складання веб-портретів користувачів. Це можна використовувати як для персоналізації користувача в машинному навчанні, так і для забезпечення безпеки на ресурсі при відстеженні аномальної поведінки;
4. Оптимізація форми на сайті з метою мінімізувати відмови відвідувачів при їх заповненні;
5. Застосування конверсійного маркетингу;
6. Використання Data Science технологій;
7. Відстеження повторних сеансів;
8. Застосування засобів психологічної аналітики, загалом для маркетингу;
9. Використання цифрової психології натискань, тому цей інструмент є популярним за заході.

2.2.3 Segment.io

Що дозволяє Segment.io:

1. Збирати дані клієнтів;
2. Робити аналіз даних;
3. Інтегрувати дані;
4. Робити перенесення даних;
5. Проводити контроль якості даних;
6. Забезпечити безпеку даних;

7. Управління інформацією користувача;
8. Управління основними даними;
9. Аналіз збігів на наявність правил поза системою;

Переваги у використанні Segment.io:

1. Реалізація функцій різних застосунків стала простішою. Більшість інструментів отримують приблизно однакові дані, тому немає сенсу писати один і той же код для обробки тих самих події кілька разів.
2. Функціонує як менеджер тегів, дозволяючи завантажувати спеціальний контент на сайт, наприклад, пікселі маркетингу.
3. Segment.io дозволяє створювати історичну копію даних в базі даних, яка контролюється. Це особливо важливо, коли потрібно переключити інструменти і цілі дослідження, не втрачаючи історичних даних.

Недоліки Segment.io:

1. Потрібен фахівець при початковому налаштуванні роботи сервісу;
2. Проблеми з налагодженням при додаванні декількох систем з різним підходом роботи. Це зазвичай пов'язано з технічною підтримкою популярних інструментів, таких як Mixpanel, Kissmetrics і т.д.
3. Деякі функції сайту можуть не працювати через Segment.io. Це пов'язано з відсутністю інтеграції або просто тому, що засоби несумісні.
4. Використання цього сервісу оплачується окремо від основних інструментів аналізу.

2.2.4 Extrawatch

Extrawatch допомагає збирати:

1. Інформацію про відвідувачів:
    a. Країну входу, браузер, ОС;
    b. Який контент послужив посиланням на веб-сайт;
    c. Статистика ключових слів, використовувана для переходу на сайт;
    d. Позиція ключового слова з Google;
2. Статистику:
    a. Збирає щотижневу статистику унікальних відвідувань, статистику завантажень сторінок, середнє число переглядів сторінок за відвідування;
    b. Статистика для цілей, які були визначені, відвідування соціальних мереж, таких як Facebook, Twitter, Google та на вашому сайті;
    c. Щоденні і щотижневі статистичні дані для: мобільних пристроїв, що використовуються для доступу до сайту, зареєстрованих користувачів, внутрішнього потоку сторінок;
3. Блокування і антиспам:
    a. Блокування спамерів;
    b. Імпортування слова в список спаму;
    c. Ручне блокування IP;
    d. Імпорт чорного списку сторонніх IP-адрес в форматі CSV;
4. Забезпечує отримання звітів на електронну пошту - отримання звітів про роботу сайту кожен ранок у вигляді листа на ел.пошту;
5. Створення цілей:
    a. цілі дозволяють відслідковувати дії, які важливі для збільшення продажу або інших перетворень. Такі цілі можуть бути використанні і для підвищення рівня захищеності сайту від різного виду загроз, завдяки приділенню уваги на певні, найменш захищені ланки сайту;

b. ExtraWatch може відправити вам електронного листа, коли буде досягнута така мета, які кроки передували цієї мети;
c. Блокувати користувача на основі цільових умов;
d. Перенаправляти користувача на основі цільових умов;

6. Діаграма - отримання щоденних і щотижневих графіків по розділах:

- Посилання;
- Ключові фрази;
- Ключові слова;
- Сторінки;
- Користувачі;
- Цілі;
- Країни;
- IP;
- Браузери;
- OS;
- Розміри таблиць бази даних.

Недоліком використання цієї технології є те, що вона працює з фреймворками на PHP, які є досить ненадійними засобами з точки зору безпеки.

2.2.5 Mouseflow

Переваги використання Mouseflow:

1. Відеозапис активності миші і прокручування сторінок;
2. Створення теплових карт;
3. Відстеження воронок;
4. Робота з формами;
5. Персоналізація користувача;
6. Підтримка бібліотек Geo Heatmaps, Feedback, Click-Error & Click-Rage;
7. Підтримка по телефону;
8. Наявність API.

2.2.6 SeeVolution

SeeVolution надає такі можливості:

1. Відстеження гарячих / холодних точок – теплові карти;
2. Перегляд рухів миші;
3. Карта прокрутки уваги – скільки контенту продивився відвідувач? Перед им як покинути сайт;
4. Різні види фільтрів;
5. Відстеження кліків;
6. Записані сеанси;
7. Програма збільшення кількості гарячих точок на сайті;
8. Аналіз активів;
9. Аналіз форми;
10. Задання цілей.

2.2.7 Використання розширень для Google Chrome чи Mozilla Firefox

Хоча можливості розширень для браузерів на даний момент не дуже гнучкі, вони мають ряд сильних переваг:

1. Резервне копіювання логів у форматі CSV;
2. Скріншоти;
3. Можливість роботи в автономному режимі;
4. Визначення часу перебування на окремому сайті;
5. Детальна статистика домену;
6. Статистика про відвідувані сайти за певний період;
7. Можливість різних налаштувань;
8. Використання як засобів браузеру, так і засобів JavaScript, в тому числі і для забезпечення безпеки користування браузером;

2.2.8 Використання власних модулів

Переваги використання даних модулів:

1. Можливість написати всі ті рішення, які є в уже готових модулях;
2. Динамічно контролювати весь функціонал, підключаючи лише необхідні методи;
3. Підключати сторонні бібліотеки и налаштовувати їх під себе, наприклад Geo Heatmaps, heatmaps.js;
4. Можливість написання як розширення для браузеру з імплементацією інших сервісів, так і написання модулю до певного веб-застосунку;
5. При виявленні нових загроз – імплементують вирішення проблеми швидше, ніж вже готові продукти.

Недоліки у розробці власних модулів:

1. Потребують спеціалістів з їх розробки;
2. Займають певний час на розробку;

2.3 Десктопні рішення, які дозволяють контролювати активність користувача

У результаті здійсненого аналізу десктопних застосунків по критеріям пункту 4.1 були обрані кращі засоби, а також додані деякі параметри орієнтовані зручність і швидкодія з боку користувачів і адміністраторів компаній.

У список застосунків потрапили: Kikidler, TimeInformer, CrocoTime, Disciplina, Lanagent Enterprice, StaffCop, TeraMind Employee Monitoring, ActivTrak Monitoring for Employee, Qustodio Monitoring for PC, VeriClock Monitoring Software, InterGuard PC Monitoring, Time Doctor for PC.

Таблиця 2.1 - Опис функціоналу десктопних застосунків моніторингу робочого столу

Критерії порівняння / назва інструменту	Kikidler	TimeInformer	CrocoTime	Disciplina	Lanagent Enterprice	StaffCop
Збір інформації про програми	+	+	+	+	+	+
Збір інформації про відвідані сайтах	+	+	+	+	+	+
Статистика активності співробітника	+	+	+	+	+	+
Аналіз графіку роботи співробітника	+	+	+	+	+	+
Перегляд робочого столу	+	screenshot	screenshot	screenshot	screenshot	+
Контроль порушень	+	+	+	-	+	+
Звіти щодо порушень	+	+	-	-	-	only flag
Перехоплення повідомлень	-	+	-	-	+	+
Перехоплення документів	-	+	-	-	+	-
Тип клієнта	desktop	device	browser	browser	device	browser
Зручність використання адміністратором	8/10	6/10	7/10	7/10	6/10	6/10
підтримка платформ	windows/ linux/ma cOS	windows	windows/ma cOS	windows	windows	windows/linu x

Кінець таблиці 2.1

Критерії порівняння / назва інструменту	TeraMind Employee Monitoring	ActivTrak Monitoring for Employee	Qustodio Monitoring	VeriClock Monitoring Software	InterGuard	Time Doctor for PC
Збір інформації про програми	+	+	+	-	+	+
Збір інформації про відвідані сайтах	+	+	+	-	+	+
Статистика активності співробітника	+	+	+	+	+	+
Аналіз графіку роботи співробітника	+	+	+	+	+	+
Перегляд робочого столу	+	+	screenshot	-	screenshot	screenshot
Контроль порушень	+	+	+	+	+	-
Звіти щодо порушень	+	+	-	+	+	-
Перехоплення повідомлень	+	+	-	-	+	-
Перехоплення документів	+	-	-	-	+	-
Тип клієнта	device	device	device	device/browser	device	device/browser
Зручність використання адміністратором	7/10	9/10	7/10	8/10	7/10	7/10
підтримка платформ	windows/macOS	windows/ubuntu/mac	windows/macOS/IOS, android	windows/macOS/android/IOS/	windows/ macOS/IOS/adnroid	windows/macOS/linux/IOS/android

2.4 Огляд існуючих DLP и SIEM систем

При огляді Data Loss Prevention і Security information and event management систем, основна увага приділялася широті покриття застосунку, ефективності роботи, швидкісті налаштування і можливостям зі словником.

Серед існуючих DLP систем можемо виділити такі:

1. Zecurion Zgate;
2. InfoWatch Traffic Monitor;
3. Symantec Data Loss Prevention;
4. Searchinform Контур безопасности;
5. FalconGaze SecureTower7

Таблиця 2.2 - Порівняння DLP систем

Назва системи	Zecurion Zgate	InfoWatch Traffic Monitor	Symantec Data Loss Prevention	Search Inform Контур безопасности	FalconGaze SecureTower
Модульність системи	Так	Ні	Ні	Так	Ні
Пристрій встановлення	Сервер ZLock, та клієнтські машини	Сервер, клієнт	Сервер, клієнт	Сервер, клієнт	Сервер, клієнт
Наявні ролі	Будь-яка кількість	Декілька	Будь-яка кількість	Будь-яка кількість	Адміністратор системи, офіцер безпеки
Контроль IM(Instant messaging)	Так	Так	Так	Так	Так
Контроль HTTP/HTTPS, FTP	Так	Так	Так	Так	Так
Контроль Skype	Лише текст	Лише текст	Ні	Так	Так

Продовження таблиці 2.2

Контроль E-mail	Так	Так	Так	Так	Такй
Соціальні мережі та блоги	Так	Так	Так	Так	Так
Контроль портів	USB, COM, LPT, Wi-Fi, Bluetooth	USB, COM, LPT, Wi-Fi, Bluetooth	USB, COM, LPT, Wi-Fi, Bluetooth	USB, LPT	USB, LPT
Протоколи блокування	HTTP, HTTPS, SMTP, OSCAR	HTTP, HTTPS, FTP, FTPS, SMTP, SMTP/S, POP3, POP3S, IMAP4, IMAP4S	SMTP, HTTP, HTTPS, FTP, MSN, AIM, AIM Pro	SMTP, POP3, MAPI, IMAP, HTTP, FTP, ICQ, Jabber	HTTP, HTTPS, FTP, FTTPS.
Аналіз за словником	Так	Так	Так	Так	Так
Лінгвістичний аналіз	Так	Так	Так	Так	Так
Аналіз трансліта	Так	Так	Ні	n/a	n/a
Аналіз архівів	Так	Так	Так	Так	Так
Аналіз рисунків	Так	Так	Так	Так	Ні
Попередньо встановлені шаблони фільтрації	Так	Так	Так	Так	Так
Затримка відправлення підозрілих повідомлень	Так, ОБ приймає рішення	Так, ОБ приймає рішення	Так, користувач пояснює причину відправки, інцидент фіксується	n/a	Ні, лише інформування офіцера ІБ
Логування дій адміністраторів системи	Так	Так	Так	n/a	У разі встановлення агенту на РМ адміністратора

Кінець таблиці 2.2

Запис звітів до локального сховище в разі недоступності сервера	Так	Так	Так	Так	Так
Перегляд історії інцидентів	Так	Так	Так	Так	Так
Режими сповіщень	Консоль, пошта, графіки	Консоль, пошта	Консоль, пошта, графіки	Консоль, пошта, графіки	Консоль, пошта, графіки

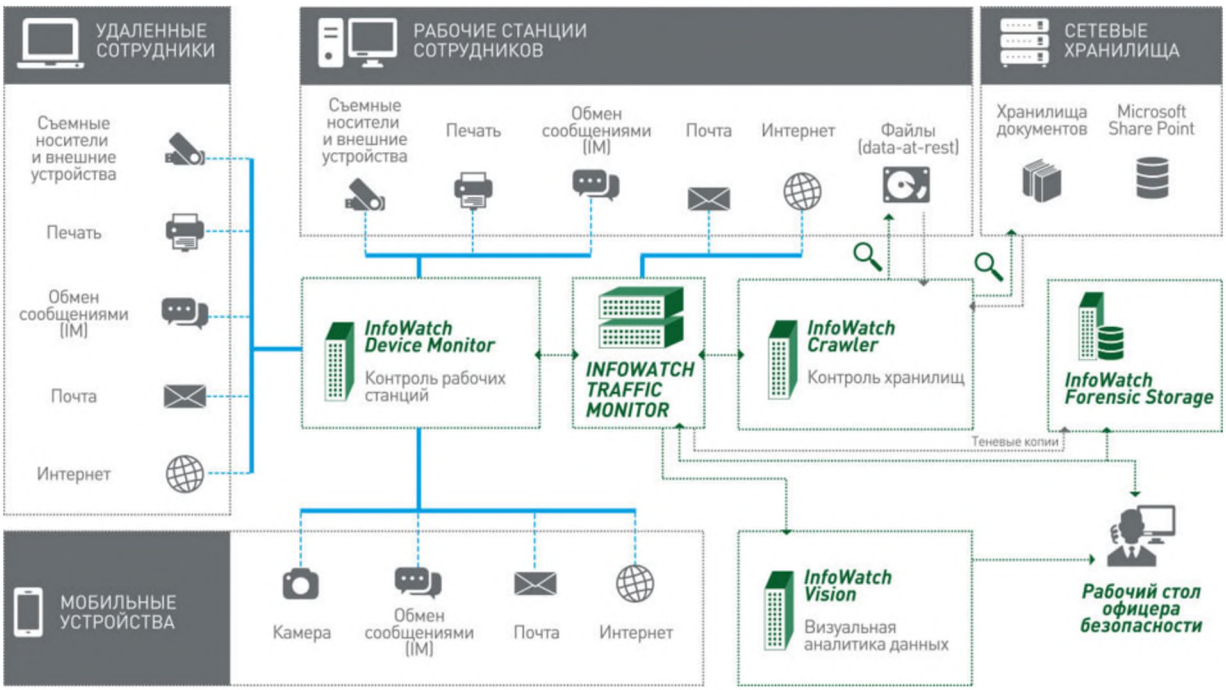

Рисунок 2.1 – Приклад роботи InfoWatch системи

Серед лідерів світового ринку SIEM можна виділити наступних:

- HP ArcSight
- IBM QRadar SIEM
- Tibco Loglogic
- McAfee
- NitroSecurity
- RSA Envision

- Splunk
- LogRhythm

2.5 Визначення вимог до розроблюваної технології веб моніторингу

Використання вже готових модулів і рішень дозволяє нам швидко почати відстежувати і збирати дані по кожному співробітнику. Проблема в тому, що оскільки готові рішення працюють з даними компанії і мають доступ до її бізнес процесів, це збільшує ймовірність витоку конфіденційної інформації та особливостей внутрішніх процесів роботи підприємства. Рано чи пізно підприємство приходить до рішення використовувати модулі внутрішньої розробки, який буде забезпечувати збір даних її працівників і збільшить захищеність компанії, якщо це звичайно можливо реалізувати.

При дослідженні цього питання і спираючись на попередні пункти отримуємо кілька варіантів вирішення:

Таблиця 2.3 - Порівняння рішень моніторингу користувачів

Рішення	Плюси	Мінуси
Десктопний застосунок	Можливість моніторити всю активність користувачів і контролювати інформаційні потоки на їх машинах.	Налагодження та розробка вимагає великої кількості фахівців, займе досить багато часу.

Продовження таблиці 2.3

JavaScript модуль чи розширення	Самі модулі збирають багато даних і мають великі можливості, які можна використовувати не тільки як контроль і моніторинг, але і як засіб для оптимізації роботи співробітника.	Працюють тільки в браузері. Досвідчений користувач може «обманювати» модулі. Вже готові модулі збирають дані з машин і можуть використовувати їх в корисливих цілях, що може небажаний вплив, наприклад збиток і загрозу даними підприємства.
DLP и SIEM системи	Відстежують весь трафік в мережі, при правильному налаштуванні можна контролювати інформаційні потоки.	Не орієнтовані на моніторинг саме веб-активності користувача

Дослідивши користь кожного з програмних продуктів і доцільність вкладення ресурсів, не складно зробити висновок, що найоптимальнішим варіантом є розробка власного модуля для відстеження веб-активності співробітника в браузері, а також впровадження DLP системи для контроля інформаційних потоків всередині корпоративної мережі.

Використання такої комбінації дозволить вирішити такі загрози безпеки як:

1. Витік даних;
2. Виявлення аномальних явищ, які можуть бути проявом шкідливої активності;

3. Виявлення порушень політики безпеки підприємства;
4. Відстеження в листуваннях в браузері конфіденційної інформації компанії.

Для відстеження веб-активності на різних сторінках браузера найкраще буде розробити розширення або плагін для браузера, який буде працювати у фоновому режимі і в який можна буде впровадити всі функції з уже відомих модулів, розглянутих в розділі 2. Також варто розробити модель користувача цього розширення.

Кожен середньостатистичний працівник проводить певний час в соціальних мережах або на інших ресурсах, і завдання застосунку полягає не в тому, щоб заблокувати йому доступ до цих порталів, а в тому, щоб проаналізувати робочий день і активність співробітника, зібрати інформацію і використовуючи ці дані, збільшити зацікавленість до роботи, тим самим збільшити його продуктивність. А також зробити весь цей процес захищеним, з дотриманням політик безпеки і без впливу на звичайний будній день працівника.

Тобто схема організації моніторингу може включати:

1. Збір інформації про ресурси, на які переходить працівник підприємства;
2. Створення теплової карти на кожен часто відвідуваний ресурс, для визначення найбільшої активності, і при виявленні аномального поведінки - відстежувати і повідомляти адміністратора, як факт можливого порушення, зокрема реалізації іншої загрози (імітація роботи співробітника);
3. Обробка кліків і завантажуваних файлів на порталі - контролю і запобігання витоку інформації або завантаження шкідливого ПО;
4. Створення веб-портрета - створення дата сету з можливістю аналізу роботи співробітника, годин його найбільшої продуктивності, його реакції на певні зміни зовнішнього середовища, починаючи від погоди і закінчуючи впливом особистих подій на працездатність для забезпечення комфортного середовища і захищеності даних.

5. Застосування правил політики безпеки, що стосуються веб-активності співробітника.
6. Виявлення написання конфіденційної інформації в листуванні в браузері.

Висновки до розділу 2

Було зроблено порівняння і аналіз основних рішень, які можуть бути використані для аналізу веб-активності користувача. Деякі із них є а) комерційними, із закритим кодом, і недоступні для детального аналізу та адаптації під потреби конкретної установи, що є недоліком б) громіздкими рішеннями, які потребують специфічних знань по коректному їх налаштуванню (наприклад, SIEM, DLP системи, які до того ж, не завжди акцентують свою увагу саме на веб- активності юзера).

З огляду на це , визначено, що найбільш перспективним по організації моніторингу користувача в невеликій організації, яка не має достатньо фінансових та часових ресурсів по придбанню та запровадженню системи моніторингу веб-активності користувачів є а) запровадження модулів моніторингу до існуючого ПЗ з функціями веб-діяльності б) запровадження розширень до браузера. З огляду на це: необхідно визначитись із моделлю, яка буде характеризувати користувацьку поведінку в веб-просторі та виділити ті її характеристики, що слугуватимуть завданням безпеки.

3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ РІШЕНЬ, ЯКІ ДОЗВОЛЯЮТЬ МОНІТОРИТИ ТА КОНТРОЛЮВАТИ ВЕБ-АКТИВНІСТЬ СПІВРОБІТНИКА

3.1 Розробка моделі користувача в веб

Призначені для користувача моделі використовуються для адаптації системи, для персоналізованих відповідей на запити користувачів. Модель повинна бути заснована на концепції користувачів, що описує профілі, які представляють взаємодію між користувачем і застосунком, і відображають різні аспекти їх взаємодії. Мета моделі - створити характеристики користувача, взаємодії, тимчасові і преференційні рекомендації. Модель користувача буде використовуватися в якості основного компонента архітектури інтеграції профілю користувача.

При розробці моделі користувача ми займаємося такими питаннями: хто, що, як, коли, де і чому. Таким чином, набір профілів, що описують користувача, складається з шести різних профілів:

1. Преференційний профіль, чи профіль вподобань - представляє очікування користувачів, який інтерес користувача. Зазвичай він заповнюється завдяки:
    a. тепловим картам;
    b. історії кліків, прокрутки та іншої взаємодії співробітника з ресурсом.
2. Профіль користувача - представляє базові дані користувачів, які представляють собою набір даних про користувача, до яких входять такі пункти:
    a. персональна інформація користувача,
    b. категорія користувача (його робочі обов'язки),
    c. політика веб-сесії (політика сесії та обмеження політики безпеки залежатимуть від перших двох атрибутів) ;
3. Часовий профіль - профіль часових характеристик, включає в себе:
    a. час перебування на певному вікні браузера;
    b. час початку сесії;
    c. час завершення сесії;

d. час опрацювання певного документу/тексту/інформаційного блока (для десктопних застосунків).

4. Просторовий профіль – представляє собою просторові характеристики користувача, та заповнюється в основному даними:
    a. геолокаційної характеристики по IP адресі;
    b. інформація про додаткові проксі сервери;
    c. місце знаходження приладу;
    d. інших просторових характеристик з User-Agent даних.
5. Профіль взаємодії - представляє в основному спосіб взаємодії користувача з застосунком / розширенням. Заповнюється за допомогою:
    a. характеристика ОС;
    b. характеристика веб-браузера(мова, часова зона);
    c. розрішення и параметри екрану;
    d. кількість відкритих вкладок;
    e. наявні системні шрифти;
    f. список допустимих форматів взаємодії;
    g. джерела виконуваного коду на клієнті;
    h. використання cookies з використання JavaScript;
    i. час завантаження URL;
    j. інформація про базовий і графічний процессор;
    k. інформація про заряд батареї;
6. Профіль рекомендації - представляє цілі взаємодії, чому користувач зацікавлений в конкретному застосунку. Профіль створюється на основі інших профілів для розробки рекомендацій для користувача.

В загальному випадку модель поведінки користувача являє собою множину

M= $\{ p_1 \cup p_2 \cup p_3 \cup p_4 \cup \ldots \cup p_k \}$, де p_i – це профіль і-го виду (в даній роботі розглянуто такі профілі як профіль вподобань, особистісний, просторовий, профіль взаємодій, часовий профіль), в свою чергу кожен із профілів p_i характеризується сукупністю атрибутів a_{ij}, які збираються із використанням JavaScript. Тобто

p_i= $\{ a_{i1} \cup a_{i2} \cup a_{i3} \ldots \cup a_{im} \}$, де m – це кількість атрибутів для даного профілю.

Атрибути можуть бути простими (наприклад, середній час сеансу); і комплексними (наприклад, теплова карта типової роботи користувача із веб-ресурсом; перелік заборонених сайтів).

Будемо вважати, що веб- портрет поведінки користувача- це конкретний набір характеристик, які входять до загальної моделі. Тоді функція, яка характеризує ступінь виконання вимог безпеки щодо еталонного портрету користувача (який відповідає типовому безпечному стану), це F=H(P_i, P_i^{secure}), де P_i^{secure} – портрет і-го користувача, який відповідає політиці безпеки; а P_i – це поточне значення портрету і-го користувача. H – функція нечіткого хешування, яка надає відсоток співпадання між портретом безпечної поведінки та портретом поточної поведінки користувача в веб-просторі. P_i^{secure} - формується на протязі певного часу спостережень за користувачем, і засновується на середніх показниках активності користувача та його типових вподобаннях: та діях; а також явних обмеженнях політики безпеки (перелік дозволених дій, ресурсів тощо).

В якості функції нечіткого хешування можна взяти ssdeep (функція із відкритим кодом), тоді портрети (сукупність атрибутів) треба записувати у файл визначеного формату (наприклад, json), і порівнювати між собою. Атрибути типу теплових карт мають переводитись у формат у вигляді двовимірного масиву, який у вигляді числових значень може бути записаний до файлу. Відсоток неспівпадань, який може сигналізувати про небезпечну ситуацію, може становити 40 та вище відсотків (конкретне значення повинно прийматись з урахуванням специфіки роботи співробітника, та ступеня непередбачуваності в його повсякденній роботі з веб-ресурсами).

3.2 Розробка системи моніторингу

Для запровадження системи моніторнгу веб-активності користувача пропонується використовувати наступні засоби:

1. Розроблене розширення (плагін) для браузера (в даній роботі розглянути браузер Chrome версії 70.0.3538.102 (Official Build) (64-bit));
2. Розроблений API та сервер для прийому та обробки даних із розширення.
3. Запровадження деяких компонентів моніторингу діяльності користувача до існуючого клієнт-серверного застосунку, яке використовується в організації (на прикладі ПЗ для розмітки текстів Anafora).

Розробка розширення для браузера складається з під задач:

1. Визначення функціоналу, який можна використати із використанням JS, який можна застосувати для задач безпеки. Загальний перелік функціональностей наведено в п. 3.1, дані функціональності є частинами відповідної моделі веб-активності користувача.
2. Інтеграція розширення до існуючого браузера (на прикладі Chrome версії 70.0.3538.102 (Official Build) (64-bit));
3. Збереження файлів з діями на локальну машину, якщо відсутній зв'язок з сервером;
4. Створення сервера, налаштування отримання даних з браузера;
5. Обробка даних і створення веб-портрета.

Веб-портрет користувача є конкретним втіленням моделі користувача (п. 3.1), тобто він складається із характеристик профілей: преференційного (профіля вподобань); особистісного, просторового та профіля взаємодій.

3.3 Частини функціоналу моніторингу, які безпосередньо призначені для вирішення завдань безпеки

Складові веб-портрету, які можуть бути використані для задач безпеки та відповідні функціональності, які реалізуються на основі цих складових:

1. Дані про відкриті вкладення (профіль вподобань, профіль взаємодій, профіль часових характеристик). Збір інформації про те, на якій вкладці знаходиться користувач (співробітник); його перебування на вкладці за визначений період часу; дані про домен;
2. Дані про кліки (профіль взаємодій, профіль вподобань). Збір даних про кліки, атрибути цих кліків, – кнопки інтерфейсу, посилання для переходу та скачування даних;
3. Дані про завантажені файли (профіль взаємодій). Збір даних про завантажені файли (які потім мають додатково аналізуватись на відповідність політиці безпеки – розширення файлів, обсяги, вміст тощо);
4. Дані про користувача (особистісний профіль).
5. Збір даних з елементів форми. Визначення – які конфіденційні дані користувач ввів на веб-ресурсі; їх можна збирати і зі сторонніх ресурсів, шляхом додання до розширення скрипту .js, який буде проглядати введені дані до наявних полів у формі, якщо вона існує на сторінці.

Також важливою складовою є можливість запровадження динамічної політики безпеки, яка в режимі реального часу може блокувати, або попереджати співробітника про відвідувані ресурсі, переходи за посиланнями, скачування даних с певних ресурсів чи заповнення своїх credentials на потенційно небезпечних сайтах, наприклад тих, що використовують http протокол, а не https.

Перелік основних видів загроз, де-активуванням яких керувалися при розробці цього розширення:

1. Відкриття небезпечних листів email – може вирішуватися використанням надійного сервісу для пошти, наприклад Gmail;
2. Перехід на ненадійні або небезпечні посилання;
3. Завантаження підозрілих файлів чи програм з інтернету;
4. Загрози типу …. Сторінка, на яку ми посилаємося з використанням target = "_ blank", отримує доступ до сторінки-джерела через об'єкт window.opener. Наприклад, таким чином тільки що відкрита вкладка може змінити window.opener.location, тобто замість попередньої вкладки непомітно довантажити зовсім іншу сторінку. Сама загроза не є небезпечною, але її вирішенням треба надати в реальному часі.
5. Введення своїх конфіденційних даних на незахищених порталах, які потім можуть бути використані сторонніми ресурсами.

3.3.1 Схема запропонованого розширення для браузера

Поділимо функціонал розширення на модулі. Вони показані на рисунку 3.1.

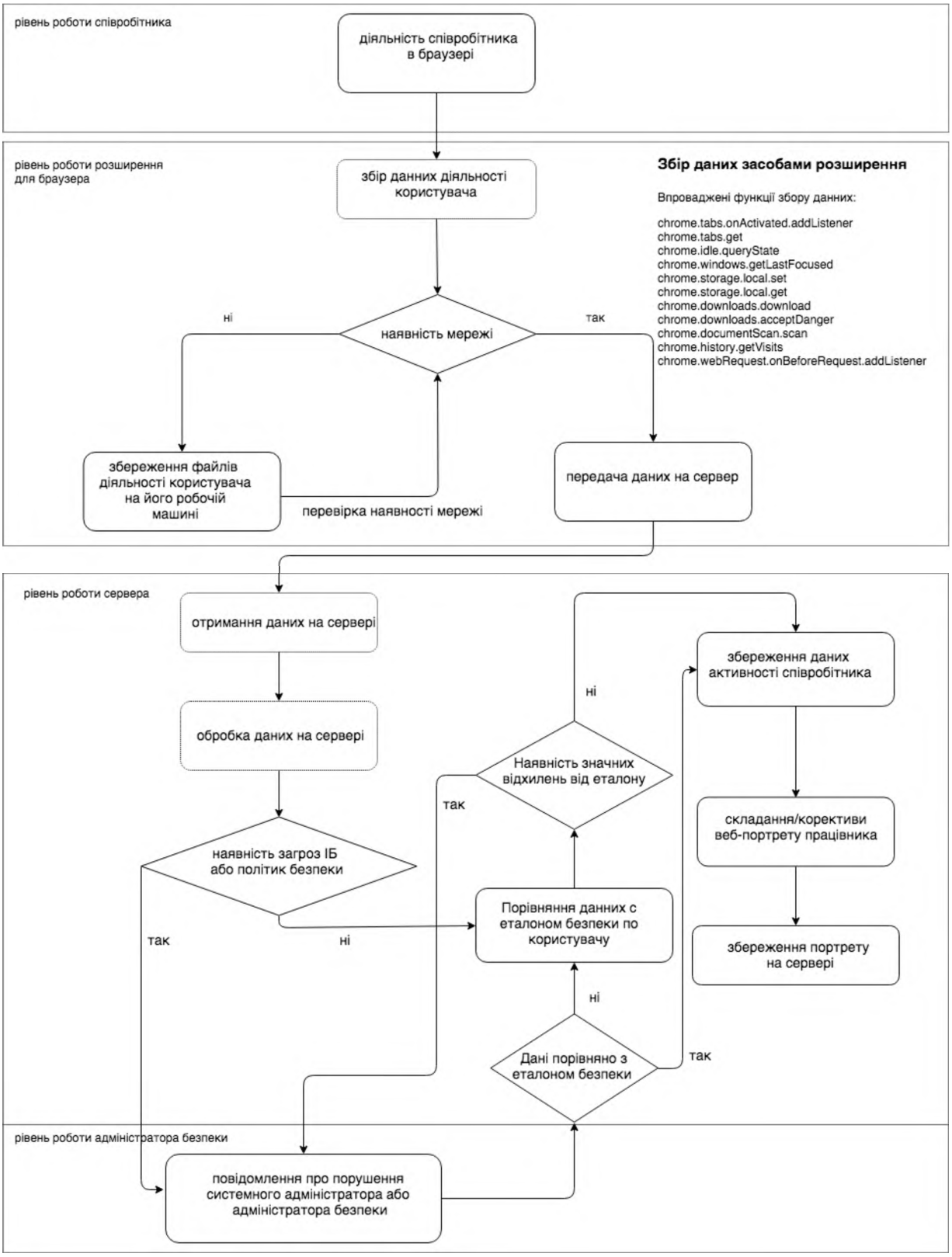

Рисунок 3.1 - Модулі розширення браузера та взаємодія між ними

3.3.2 Розроблене розширення. Приклади можливостей

Розроблене розширення(плагін) включає в себе:

1. Налаштування ip адреси сервера, з яким взаємодіяти;
2. Клієнт отримує sec_policy.json файл від сервера з указанням певних правил політики безпеки, з розділами warning, danger, forbid_format, user_tasks та іншими;
3. Клієнт надсилає дані моніторингу серверу з інтервалом 2 хвилини, з id користувача, та міткою часу.
4. При збереженні файлів, вони дублюються у певну директорію на локальній машині, доступ до якої є у системного адміністратора через локальну мережу, вони зберігаються там зазначений час, після чого потрапляють або до архіву, або видаляються.
5. Складання задач для співробітника, при виконанні яких, вони переводяться в статус «виконано», цей статус і id завдання відправляється також на сервер. Можливість інтерграції з системами планування тасок, такими як Jira чи Trello (поки не реалізовано).
6. Можливість додавання бібліотек з додатковими можливостями, наприклад heatmaps.js для отримання теплових карт активності робітника (поки не реалізовано).
7. Системний адміністратор чи офіцер безпеки може налаштовувати sec_policy.json для задання правил політики безпеки.
8. Сервер отримує файл моніторингу від клієнта, сортує його за міткою часу, визначає чи є пробіли у моніторингу, та створює статистику.
9. Далі ці файли заганяються у програму обробки, де і формується веб-портрет співробітника, який потім може аналізуватися менеджером чи власником підприємства.

Файл sec_policy.json з правилами політики безпеки буде виглядати так:

```
{
  "user_id":"782dewu3",
```

```
  "email": "volodymyr.lopukhovych@gmail.com",
  "warning": [ // показує модальне вікно при переході на цей домен
    "stackoverflow.com",
    "developer.chrome.com",
    "facebook.com"
  ],
  "danger": [ // забороняє перехід на домен
    "vk.com",
    "17ebook.com",
    "aladel.net",
    "clicnews.com",
    "dfwdiesel.net",
    "divineenterprises.net"
  ],
  "forbid_format": [ // заборонені формати для завантаження
    "exe",
    "torrent",
    "pif",
    "application",
    "com",
    "jar",
    "bat",
    "scf"
  ],
  "user_tasks": [ // особисті задачі співробітника
    {
      "id": "23qws3",
      "description": "create icon on help page"
    },
    {
      "id": "112qws",
      "description": "refactor help page"
    }
  ],
  "preloading_page": true,
  "double_file_dir_path": "/Users/volod/Backlogs/webtime-tracker/files",
// шлях для дублювання завантаженого файлу
  "check_credentials_input": true // прапор перевірки використовуваного
протоколу при введені credentials
}
```

При зборі інформації, використовуються як функції розширення браузеру, так і функції доданих JavaScript скриптів.

При розробці кожного плагіну створюється файл manifest.json, який задає конфігураційні дані зі сторінками, дозволами та іншою інформацією. У нашому випадку він виглядає так:

```
{
  "manifest_version": 2,
  "name": "Cyber Security",
```

```
  "description": "Lopukhovych magister's diploma project",
  "version": "1.0.0",
  "icons": {
    "16": "icon/favicon16.png",
    "32": "icon/favicon32.png",
    "48": "icon/favicon48.png",
    "128": "icon/favicon128.png"
  },
  "permissions": [
    "tabs",
    // дозволяє отримати URL-адресу, заголовок та значок для цієї
вкладки.
    // Також дозволяє запустити chrome.tabs.executeScript (вставити код
JavaScript на сторінку)
    "downloads",
    // дозволяє отримати такі властивості як:
    // індикація того, чи вважається цей завантаження безпечним або
відомо, що він є підозрілим.
    // Вказує, чи відбувається завантаження, переривання або завершення
завантаження.
    // Чому завантаження було перервано. Отримати файл size, розширення
файлу, абсолютну URL-адресу,
    // з якої було здійснено це завантаження, перед будь-якими
переспрямуваннями та додатковими.
    "documentScan",
    // дозволяє програмам і розширенням переглядати вміст паперових
    // документів на доданому сканері документів
    "idle",
    // дозволяє отримати статус системи, "active", "idle", or "locked"
    "history",
    // дозволяє взаємодіяти з записом браузера відвіданих сторінок.
    // Можна додавати, видаляти та запитувати URL-адреси в історії веб-
перегляду.
    "storage",
    // дозволяє зберігати, отримувати та відслідковувати зміни даних
користувача в хромовому сховищі.
    // працює асинхронно, та швидше ніж localStorage
    "unlimitedStorage",
    // Надає необмежену квоту для зберігання даних клієнтської частини
HTML5,
    //таких як бази даних та локальні файли.
    "notifications",
    // дозволяє створювати розширені сповіщення за допомогою шаблонів і
відображати
    //ці сповіщення користувачам у системному треї
    "topSites",
    //  дозволяє отримати доступ до найпопулярніших сайтів,
    //які відображаються на новій вкладці, використовується для
впровадження нових правил політики безпеки
    "webRequest",
    "webRequestBlocking",
    // права дозволяють спостерігати та аналізувати трафік та
перехоплювати, блокувати або змінювати запити в польоті.
    "http://localhost:8080/",
    "https://www.google.com/"
```

```
  ],
  "options_page": "options/options.html",
// сторінка задання адреси для посилання даних,
// конфігурації завдань та інших даних для співробітника
  "browser_action": {
    "default_icon": {
      "19": "icon/favicon16.png",
      "38": "icon/favicon38.png"
    },
    "default_popup": "popup.html",
    "default_title": "Cyber Security"
  },
  "background": {
    "scripts": [
      "js/constants.js",
      "js/functions.js",
      "js/storage-local.js",
      "js/background.js"
    ],
// скрипти, які виконуються на задньому плані
    "persistent": false
  },
  "offline_enabled": true,
  "optional_permissions": [
    "\u003Call_urls>"
  ],
"content_scripts": [
  {
    "matches": ["http://*/*", "https://*/*"],
    "js": ["myscript.js"]
  // можливість додавати кастомні скрипти чи бібліоткеки,
  // такі як heatmap.js
  }
]

}
```

Сторінка, налаштування конфігураційних даних для серверу має вигляд:

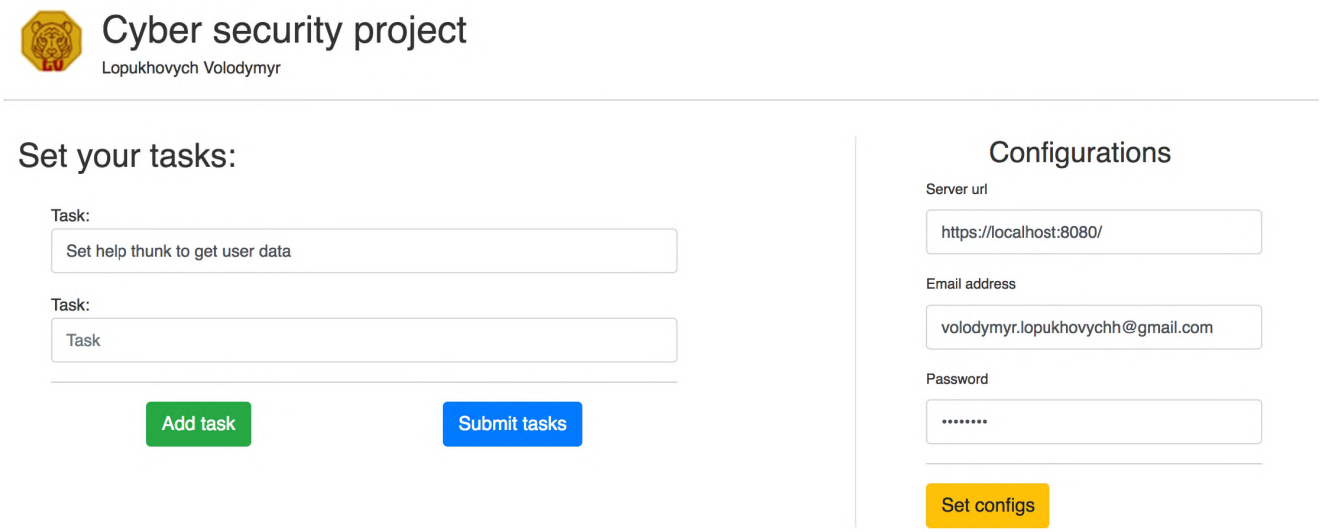

Рисунок 3.2 – Вигляд сторінки налаштування конфігурацій та завдань

Основні функції, які використовуються для збору інформації:

1. `chrome.tabs.onActivated.addListener` – прослуховування подій на активній вкладці;
2. `chrome.tabs.get` – доступ до даних вкладки (домен, час перебування);
3. `chrome.idle.queryState` – прослуховування стану вкладки;
4. `chrome.windows.getLastFocused` – отримуємо останнє активне вікно браузера;
5. `chrome.runtime.getManifest` – отримуємо відомості про застосунок або розширення з маніфесту;
6. `chrome.storage.local.set, chrome.storage.local.get` – робота зі сховищем розширення;
7. `chrome.downloads.download` – робота з завантаженням файлу, налаштуванням опцій;
8. `chrome.downloads.acceptDanger` – запит до користувача про завантаження небезпечного файлу;
9. `chrome.downloads` – модуль підтримує функції pause, resume, cancel, show та інші;

10. `chrome.documentScan.scan` - виконує сканування документа. Після успіху дані PNG будуть передаватися у callback.
11. `chrome.history.getVisits` - отримує інформацію про відвідування URL-адреси.
12. `chrome.webRequest.onBeforeRequest.addListener(callback, filter, opt_extraInfoSpec)` – прослуховування адреси запиту, фільтрація callback, та спеціальний параметр opt_extraInfoSpec, який може містити рядок “blocking”. Процес життєвого циклу запиту, де відбувається попередня обробка, показаний на рисунку 3.3.

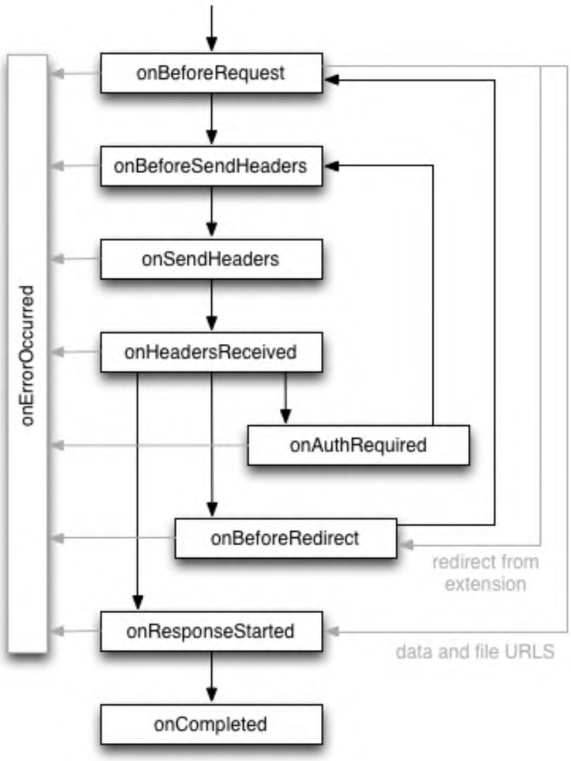

Рисунок 3.3 – Життєвий цикл запиту

Також замість localStorage, використовується chrome.storage API, який зберігає дані у браузері, а не тільки на певній сторінці, підтримує асинхронні запити на читання та запис? Тому працює швидше ніж localStorage.

Операції читання та запис до сховища винесено в окремий модуль storage-local.js. Має такий вигляд:

```
"use strict";
var storageLocal = function () {
```

```
    var save  = function (field, object, callback) {
        var obj = {};
        return obj[field] = JSON.stringify(object),
chrome.storage.local.set(obj, callback), !0
    };
    var load = function (field, object, callback) {
        var obj = {};
        return obj[field] = JSON.stringify(object),
chrome.storage.local.get(obj, function (object2) {
            var obj2 = {};
            obj2[field] = JSON.parse(object2[field]), callback(obj2)
        }), !0
    };
    return {save: save, load: load}
}();
```

У результаті обробки даних за 2 хвилини отримуємо на сервер такий json:


```
[
  {
    "user_id": "782dewu3",
    "email": "volodymyr.lopukhovych@gmail.com",
    "time": "2018-11-23T00:30:24.552000Z",
    "data": {
      "domains": {
        "stackoverflow.com": {
          "name": "stackoverflow.com",
          "status": "allow",
          "action": "access",
          "alltime": {
            "seconds": 441
          },
          "days": {
            "2018-11-23": {
              "seconds": 441
            }
          },
          "activity": {
            "click": [
              {
                "elem": "link",
                "href":
"http://rads.stackoverflow.com/amzn/click/0596517742",
                "value": "JavaScript: The Good Parts"
              },
              {
                "elem": "input",
                "type": "text",
                "value": "es6 features",
                "class": "f-input js-search-field"
```

```
            }
          ]
        }
      },
      "jsonformatter.org": {
        "name": "jsonformatter.org",
        "status": "warning",
        "action": "exit",
        "alltime": {
          "seconds": 1
        },
        "days": {
          "2018-11-23": {
            "seconds": 1
          }
        },
        "activity": {}
      }
    },
    "done_tasks": [
      {
        "id": "23qws3",
        "description": "create icon on help page",
        "status": "done",
        "time": "2018-11-23T00:29:22.552000Z"
      }
    ],
    "warnings": {
      "amount": 1,
      "domains": [
        "jsonformatter.org"
      ]
    },
    "seconds": {
      "alltime": 120
    }
  }
}
]
```

3.3.3 Задачі та схема впровадження модулів моніторингу до існуючого клієнт-серверного застосунку

Запровадження модулів моніторингу до існуючого застосунку є корисним для контролю дій користувача, визначення його активності для тих користувачів, які за професійними обов'язками не використовують браузер, однак, працюють із впровадженим на підприємстві клієнт-серверним програмним забезпеченням. Розглянемо приклад такої ситуації, коли команда розмітників працює над розміткою тексту. Треба запровадити контроль атрибутів їхнього часового профілю.

В якості прикладу системи розмітки розглянемо ПЗ Anafora із відкритим кодом. Задачі та цілі при запровадженні змін в клієнтську частину ПЗ:

1) аналіз вихідного коду ПЗ Anafora;
2) визначення модулів, які відповідальні за необхідні для моніторингу дії (в даному випадку розглянемо дії по сесіям щодо розмітки певних текстів, та дії щодо відмітки тегів);
3) модифікація існуючих функцій;
4) збереження даних моніторингу (тимчасове);
5) відправка їх на сервер для подальшого аналізу і порівняння із а) попередніми результатами б) еталонними результатами в) виявлення відхилень, які можуть слугувати індикаторами а) порушень встановленого режиму роботи; б) навмисних зловживань (прогулів, недбайливості) в) роботи у непризначений час, що може слугувати сигналом про порушення організаційних засад політики безпеки.

Систему моніторингу діяльності користувача в ПЗ Анафора (клієнт-серверний застосунок) реалізовано із використанням JavaScript на стороні клієнта. Використано гілку проекту ПЗ Anafora master, Django 1.11, Python 2.7 (серверна сторона).

Поділимо функціонал застосунку на модулі. Вони показані на рисунку 3.4.

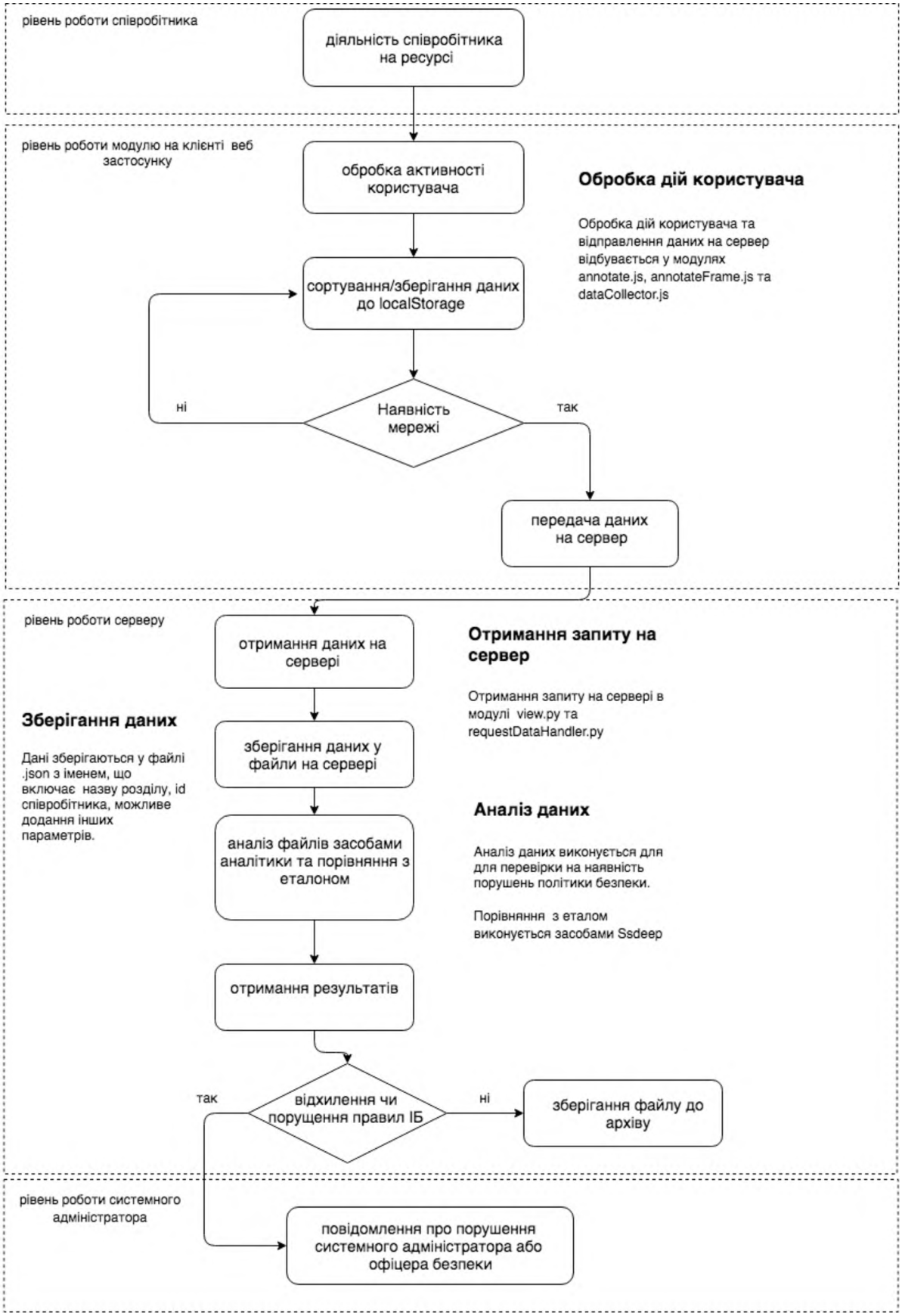

Рисунок 3.4 - Модулі веб застосунку на ресурсі та взаємодія між ними

Основними модулями, які відповідають за розмітку тегів, є модулі annotate.js та annotateFrame.js. До цих модулів був доданий третій модуль dataCollector.js. При зборі часових характеристик розмітки генерується новий об'єкт через функцію addNewObj (див. файл проекту annotate.js, до якого імпортується розроблений dataCollector.js), всередині addNewObj викликається функція, яка створює новий об'єкт з часовими рамками, в цій функції об'єкт зберігається до json файлу і потім весь json зберігається в localStorage з ключем anafora, також дані зберігаються у файл на сервері inprogress (кожні 2 хвилини). Після асинхронного надсилання даних на сервер усі бекап-дані з localStorage стираються. Збереження зареєстрованих даних в json реалізовано в SaveTagFile.

Інформація, яка збирається, являє собою такі характеристики діяльності користувача:

1) початок роботи з текстом;
2) хто є аннотатором, редактором тексту;
3) id кожного поміченого тегу;
4) час розмітки тегу;
5) кількість символів тегу та їх позиція у тексті;
6) кількість слів у тегу;
7) до якої категорії з наявних відноситься даний тег.

Цією розробкою продемонстровано достатню ефективність запровадження засобів моніторингу у існуючі програмні застосунки із відкритим кодом. Перевагами такого рішення є 1) гнучкість 2) швидкодія 3) розширені можливості по збору інформації моніторингу у відповідності до професійних задач співробітника. Хоча проект ПЗ Анафора використовується в організаціях, в яких не ставляться суворі вимоги щодо моніторингу діяльності користувача, але такі рішення з моніторингу можуть ефективно аналогічно застосовуватись у відповідних клієнт-серверних застосунках банківських клієнт-серверних систем; систем режимних установ, із підвищеними вимогами щодо контролю організаційних засад політики безпеки.

3.3.4 Клієнтська частина модуля моніторингу існуючого клієнт-серверного застосунку

При виборі тегу чи інших реєстрованих подіях метод фіксує абсолютний час (внутрішній час linux-подібних систем, у мілісекундах).

Примітка: час початку роботи прив'язаний до початку сесії користувача в Anafora. Час закінчення роботи – прив'язаний до відмітки "Mark as completed".

Для налаштування збереження реєстрованих статистичних даних потрібно прописати шляхи збереження файлу: в папці проекту anaphora файл url.files, де треба прописати ще один url (по зразку вже існуючого для стандартних файлів розмітників, тількі з іншим іменем (напр. на доданок до вже існуючого url SaveFile – SaveTagFile з тими ж параметрами налаштувань проекту)). Шляхи url доступні в urls.py, views.py.

У файл json формату метод повертає:

- Час початку сесії startSessionDate (поле може зустрічатись більше за один раз, при поновленні сторінки користувачем, тому використовуємо його перше входження);
- кортеж виду <text_id:annotator_id:word_lenght:tagging_time> (cortege": "3@e@doc23@admin:9:1537883610733);
- абсолютний час попереднього та поточного кліку clickDate (вибору тегу);
- час виділення слова textSelectionTime (час початку, час завершення та різниця між ними);
- тип дії (click);
- кількість слів у словосполученні, якому присвоєно дану категорію wordsNumber (може бути більше за одне);
- позицію словосполучення position (початок, кінець);
- тип документа type;
- ідентифікатор тексту у вигляді 3@e@doc23@admin;
- а також в останньому кортежі – відмітка про час завершення сесії endSessionDate (в незавершеному варіанті розмітки може бути відсутня).

Приклад виводу файла FR00045.json:


```
[
 {
  "startSessionDate": 1537883606771,
  "cortege": "3@e@doc23@admin:9:1537883610733",
  "clickDate": [
   0,
   1537883610733
  ],
  "annotator": "admin",
  "textSelectionTime": [
   1537883609993,
   1537883610220,
   227
  ],
  "selectingType": "click",
  "wordsNumber": 1,
  "position": [
   263,
   272
  ],
  "symbolNumber": 1224,«
  "type": "Medication/Intervention",
  "id": "3@e@doc23@admin"
 },
 {
  "cortege": "4@e@doc23@admin:9:13785",
  "annotator": "admin",
  "textSelectionTime": [
   1537883628772,
   1537883629008,
   236
  ],
  "selectingType": "click",
  "wordsNumber": 1,
  "id": "4@e@doc23@admin",
  "position": [
   348,
   357
  ],
  "type": "Disease/Disorder",
  "clickDate": [
   1537883616161,
   1537883629946
```

```
  ]
 },
 {
  "endSessionDate": 1537883636109
 }
]
```


(Примітка: зазвичай якщо textSelectionTime менше 220, то це подвійний клік, якщо більше – то слово обиралось веденням миші)

Таким чином, у файлі будуть розташовані часові відмітки часу, які використовуватимуться для обчислення часу на проставляння певного тегу.

3.3.5 Серверна частина модуля моніторингу існуючого клієнт-серверного застосунку

Час на проставляння тегу обчислюється на серверному боці шляхом аналізу файлу з переданими даними за формулою:

TagDefinitionTime = ClickDate(Current) - Clickdate (Prev)) – ReadingTime * Number_of_Chars_between_these_ two_words, де readingTime – приблизна швидкість читання одного символу даним користувачем.

Для точного визначення часу на визначення певної категорії треба заміряти, скільки часу витрачає розмітник на читання тексту довжини m символів, і підрахувати, скільки припадає на один символ. В запропонованій реалізації прототипу цей час дорівнює 1 мс. Але якщо розмітник взагалі не читатиме цей відрізок тексту, одразу побачить наступне слово, і привласнить йому категорію – тоді ми одержимо від'ємний результат. Для запобігання цьому в процесі підрахунку середнього від'ємні значення приймаються нульовими.

Дані по середньому часу по всіх розмітниках по всіх текстах, у форматі кортежів виду <tag:average_tagging_time2> реалізуються на боці сервера шляхом одержання даних з файлів json та відповідних обчислень.

Приклад результатів розрахунків:

FR00016.txt:

For all text and all annotators:
Medication/Intervention:3953.0
Disease/Disorder:13776.0
For all text and ONE annotators:
admin:Medication/Intervention:3953.0
admin:Disease/Disorder:13776.0
Worked time of each text:
doc23:1224:29338

Бачимо, що суттєво більше часу витрачається на категорію Disease/Disorder.

Підрахунок кількості символів у тексті, зчитування відповідного часу розмітки у FR00045.json як різниці EndSessionDate-StartSessionDate. Вивід у форматі:

<tag:average_tagging_time2>

Підрахунок часу, витраченого на роботу із документами, їх розмітку, може дати інформацію про дотримання регламенту робочого часу, сумлінність працівника; що непрямо впливає на організаційні моменти політики безпеки. При роботі із документами, які мають гриф “конфіденційно” чи “таємно” і містять важливу інформацію, контроль робочого часу та способу роботи з документом є рекомендованим для запобігання зловживаннями в робочий час, контролю порушень обробки даних.

Висновки до розділу 3

Запропоновано характеристики моделі веб-активності користувача; які формують портрет веб-активності користувача. Запропоновано схему моніторингу дій користувача а) шляхом запровадження розширення для браузера; б) шляхом запровадження модуля моніторингу до існуючого прикладного клієнт-серверного застосунку.

Визначено характеристики моделі, які можуть використовуватись для контролю порушень політики безпеки, встановленої для користувачів (співробітників)

організації. Розроблено відповідні програмні рішення. Проведені практичні експерименти засвідчили про працездатність цих рішень.

В ході дослідження можливостей JavaScript було визначено перелік основних функцій, які доцільно використовувати для збору інформації про користувача в цілях моніторингу його веб-активності.

4 РОЗРОБКА СТАРТАП ПРОЕКТУ

Використання ідеї моніторингу працівника підприємства має широке застосування як серед компаній, які працюють за принципами звичайних методологій, так і для тих, хто починає використовувати Scrum. Цей підхід був розроблений не тільки для того, щоб менеджеру або власнику підприємства було зручно відстежувати діяльність співробітників на робочому місці, а й для того, щоб самі співробітники могли використовувати цей застосунок для поліпшення своєї продуктивності і своїх результатів роботи.

4.1 Опис ідеї стартап-проекту

Ідея: Впровадження технологій моніторингу веб-активності користувача з застосуванням інструментів JavaScript.

Напрями застосування:

1. Компанії малого бізнесу до 200 чоловік, які вже працюють або хочуть перейти на роботу по методиці scrum.
2. Компанії середнього або великого бізнесу.
3. Державні органи, робоче середовище яких переведено в веб.
4. Банки, які хочуть відстежувати роботу штатних співробітників.

Вигода для власників даних підприємств:

1. Забезпечення захисту даних і інших цінних ресурсів.
2. Підвищення продуктивності і ріст співробітників;
3. Мінімізація випадків витоку конфіденційної інформації;
4. Моніторинг та відстеження аномальної активності співробітників;
5. Дотримання правил політики безпеки.

4.2 Визначення сильних та слабких сторін ідеї проекту

Будемо класифікувати ідею за такими характеристиками:

1. Економічна;
2. Технічна;
3. Естетична - інтерфейс, зручність, не заважає роботі співробітника;
4. Ергономічна;
5. Забезпечення безпечного середовища;
6. Швидкість досягнення результату;
7. Надійність.

Таблиця 4.1 - Сильні і слабкі сторони ідеї проекту

№ п/п	Характеристики ідеї	Слабка сторона	Сильна сторона
1	Ергономічна	Нема коштів на маркетинг і немає клієнтів для пошуку і формування ринку збуту	Дешева реалізація, гнучкість розробки і рішення безпосередніх завдань безпеки.
2	Технічна	Підтримка обмеженої кількості браузерів	Використання великого набору функціоналу і можливість гнучкого налаштування.
3	Естетична	немає	не заважає виконанню завдань, можливість розробки інтерфейсу безпосередньо під клієнта.
4	Ергономіна	немає	Можливість налаштування потрібних функцій під будь-які вимоги адміністратора і співробітника.

Кінець таблиці 4.1

5	Безпечне оточення	немає	Оточення повністю налаштовується системним адміністратором, також є можливість консультацій з боку продукту.
6	Швидкість досягнення результату	немає	Швидке впровадження, що складається з 2 кроків 1. Установка і настройка DLP системи на локальній мережі. 2. Установка розширення для браузера і введення адреси сервера.
7.	Надійність	Збої у роботі можуть вплинути на справність і коректність роботи системи	Ніяк не впливає на роботу розширення для браузера. При відсутності мережі усі логи зберігаються на машину співробітника, а при відновленні роботи - відправляються на сервер.

4.3 Засоби і послідовність дій для впровадження ідеї

Для впровадження ідеї в підприємство потрібна група розробників:

1. Backend developers - розробники для збору даних з браузера співробітників підприємства і збереження їх в файлах для аналізу. При виявленні порушень політик безпеки в уже оброблених файлах автоматизують функцію оповіщення адміністратора безпеки або системного адміністратора.
2. Frontend developers - розробка розширення і впровадження в браузер.
3. Data analytics - розробники для обробки даних, складання звітів і статистики з даних, зібраних з клієнтів.
4. Системний адміністратор або адміністратор безпеки - відповідає за настройку DLP системи + вирішення проблеми порушення безпеки безпосередньо зі співробітниками підприємства.

Необхідні технічні засоби для впровадження ідеї стартапу:

1. Робочі машини для команди розробників;
2. Машини для обробки даних;

4.4 Технологічна здійсненність ідеї проекту

Таблиця 4.2 - Технологічна здійсненність ідеї проекту

№ п/п	Етап розробки	Наявність технології	Доступність технологій і здійсненність завдання
1	Збір даних з працівників і відправка на сервер	Технології існують, а параметри і перелік потрібних даних вказано в розділі 2.	Технологія доступна. Завдання здійсненна при наявності фахівців.
2	Збір даних на сервері і збереження в потрібному форматі для аналітики	Технологія існує.	Технологія доступна. Завдання здійсненна.
3	Аналіз даних, складання статистики та результатів	Технологія існує.	Технологія доступна, потрібні особливі фахівці для виконання цього завдання.

4.5 Аналіз можливостей запуску проекту

При аналізі ринку враховувалися такі характеристики як:

1. Наявність безпосередніх і непрямих конкурентів;
2. Легкість розробки і впровадження в порівнянні з конкурентами;
3. Динаміка ринку;
4. Наявність обмежень для входу на ринок.

4.6 Фактори загроз

Таблиця 4.3 - Аналіз фактору загроз

№ п/п	Фактор	Зміст загрози	Способи рішення
1	Цінова конкуренція	Коливання цін на ринку	Пошук варіантів зниження вартості послуг
2	Зниження попиту на продукт	Поява альтернативи	Розширення, поліпшення функціоналу та оптимізація впровадження, підтримки
3	Зміна API браузера	Падение функционала, привязанное к API	Своєчасне оновлення додатка
4	Закриття підприємства	При зупинці діяльності, підприємство припиняє співпрацю	Пошук нових клієнтів

4.7 Фактори можливостей

Таблиця 4.4 - Аналіз фактору можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція стартапу
1	Поява нових технологій аналізу за допомогою JavaScript	Розширення спектру можливостей для аналізу користувача і додавання методів забезпечення безпеки	Впровадження нових технологій, оптимізація і стабілізація роботи програми
2	Розширення можливостей браузера	Додавання зручності і сегментів, де можна застосовувати application	Розширення сегмента застосування, пошук клієнтів
3	Збільшення кількості бізнес процесів в веб	Новим гравцям потрібні такі додатки для моніторингу активності користувача і забезпечення безпеки	Пошук таких підприємств і надання своїх послуг
4	Поява нових технологій аналізу для моніторингу та забезпечення безпеки даних	Можливість впровадити ці технології в існуюче розширення або розробка нових рішень	Вивчення цих технологій і їх інтеграція з існуючими рішеннями

4.8 Аналіз конкуренції

Таблиця 4.5 - Аналіз конкуренції на ринку

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники конкурентних продуктів	Клієнти
	- Застосунки віддаленого моніторингу на ПК - DLP і SIEM системи - Розробники подібних систем	- JavaScript модулі, що мають схожий функціонал; - компанії, що забезпечують інформаційну безпеку	- Компанії десктопних застосунків по ІБ; - компанії розробки DLP і SIEM систем - компанії розробки веб модулів	- Великі IT компанії; - Середні та дрібні IT - компанії; - Банки; - Держ. підприємства - Підприємства мають роботу в інтернеті
Висновки	Присутній велика пряма конкуренція	Косвеннная конкуренція працює більше в інших напрямках і лише частково усуває проблеми, які вирішує цей проект	Постачальники - досить великі продукти, при цьому на їхньому боці досвід і надійність, але на стороні проекту - гнучкість і зручність.	Клієнти рано чи пізно будуть використовувати схожі засоби. Потрібно вчасно зайти на ринок.

4.9 Аналіз конкуренції

Таблиця 4.6 - Фактори конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1	Ціна и інші витрати	Ціна варіюється для різних типів клієнтів (з упором на зручність, надійність, захищеність, а також в залежності від розміру підприємства і його фінансових можливостей)
2	Гнучкість налаштувань	На відміну від конкурентів, наш продукт має больую гнучкість і можливість розробити і настої систему в залежності від різних параметрів.
3	Універсальність	На відміну від інших конкурентів, система використовує кошти браузера, який працює однаково на всіх ОС

Кінець таблиці 4.6

4	Надійність	На відміну від інших виробників, система стійка до збоїв мережі і інших проблем, зберігаючи дані і звіти на локальній машині, а при стабілізації передавати їх на сервер.
5	Зручність	Вимагає лише встановити програму на Ваш браузері і введення адреси сервера в локальній мережі.

4.10 Аналіз клієнтів

Таблиця 4.7 - Потенційні клієнти

№ п/п	Цільова група клієнтів	Готовність клієнтів застосувати продукт	Попит в сегменті	Інтенсивність конкуренції в сегменті	Простота входу в групу
	Великі підприємства	Клієнти потребують продукті такого типу і готові його використовувати	Високий попит в зв'язку з необхідністю оптимізації бізнес процесів і запобігання витоку інформації	Висока конкуренція в сегменті через необхідність настройки стабільного оточення і впровадження готового продукту	Складно увійти в сегмент, тому що більшість клієнтів мають достатньо коштів для покупки більш складних систем, які має доступ до всієї ОС, а не тільки браузера
	Середні підприємства	Клієнти потребують продукті такого типу, але поки не всі готові його використовувати	Попит середнього рівня.	Високий рівень конкуренції	Є складність з входом даний сегмент, але простіше, ніж на ринок з великими підприємствами
	Малі підприємства	Не всі потенційні клієнти потребують продукт	Середній попит у зв'язку з непотрібністю використання подібних програм	Середній рівень конкуренції	Є складнощі з виходом на ринок, але більше пов'язані не з конкуренцією, а з готовністю клієнтів використовувати продукт.

Кінець таблиці 4.7

	Банки	Не всі потенційні клієнти потребують продукт	Середній попит	Низький рівень конкуренції	Є складнощі з виходом на ринок, але більше пов'язані не з конкуренцією, а з готовністю клієнтів використовувати продукт.
	Державні структури	Не всі потенційні клієнти потребують продукт	Низький попит	Низький рівень конкуренції	Є складнощі з виходом на ринок, але більше пов'язані не з конкуренцією, а з готовністю клієнтів використовувати продукт.

4.11 Стратегія позиціонування

При виборі стратегії стартапу і виході на ринок, потрібно спиратися на:

- Місія - коротке визначення сенсу існування IT підрозділу;
- Цілі - напрямки діяльності;
- Завдання - дії, спрямовані на досягнення цілей;
- Тактики - особливі дії по виконанню завдань;
- KPI - показники, що дозволяють оцінити досягнення при виконанні завдань.

При оцінці можливостей була обрана стратегія диференціації. Якщо говорити про ризики, то маркетингова стратегія має орієнтацію на:

- Максимальний ефект незалежно від ризиків;
- Мінімальні ризики при відсутності великих очікувань;
- Різноманітні комбінації, в яких можуть виступати ці два підходи.

Оскільки продукт є інноватором на ринку, то є сенс розвивати його і впроваджувати на всіх можливих сфери і просувати його вже там, де він буде мати максимальний успіх. При Цьому потрібно сформулювати стратегію позиціонування.

Таблиця 4.8 - Стратегія позиціонування

№ п/п	Вимоги аудиторії до товару	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Отримання послуг з розробки та впровадження продукту на машини підприємства. Отримання знань і консультацій від фахівців з інформаційної безпеки і оптимізації бізнес процесів. Мінімізація фінансових витрат і збільшення продуктивності співробітників. Забезпечення захищеності даних і інших елементів, які мають цінність.	Стратегія диференціації.	Використання сильних сторін та можливостей рішення	Моніторинг користувачів, оптимізація та впровадження захищеності даних. Складання веб-портрета користувача. Впровадження дотримань політик безпеки в браузер.

Таблиця 4.9 - Визначення установки ціни на послуги і продукт

п/п	Рівень цін на розробку продукту	Рівень цін на додаткові послуги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу	Услуги на консультування та супервайзінг
	40000 ум.од	10000 ум.од, дополнительно обсуждаются	Будь-який рівень доходу	Ціна підписки на пітдримку існуючого ПЗ– 2000 ум.од	Від 500 ум.од

Таблиця 4.10 - Система збуту

№ п/п	Поведінка клієнтів при замовленні послуг	Функції збуту, які має виконувати постачальник товару	Використання посередників	Оптимальна система збуту
	Надання переліку проблем з якими зіткнулося підприємство. Обговорення та прийняття одного з варіантів вирішення проблеми. Допомога і супутніх при впровадженні рішення на підприємство	Допомога і надання рішень проблем безпеки. Консультація при налаштуванні захищеної корпоративної середовища і політик безпеки. Впровадження або допомога при впровадженні продукту в робочий процес підприємства. Підтримка побажанням.	Чи не передбачає використання посередників при здійсненні послуг.	Залучення партнерів та посередників при пошуку і формуванні каналів збуту.

4.12 Стратегія маркетингових комунікацій

При формуванні маркетингових комунікацій, основний упор буде робитися на таких кроках:

1. Дослідження роботи потенційних клієнтів і сфер їх діяльності для максимальної захищеності всіх її внутрішніх процесів і настройки їх стабільної роботи, які можуть бути забезпечені стартап проектом.
2. Використання каналів інтегрованих маркетингових комунікацій.
3. Використання сильних сторін продукту і надання широкого спектру послуг для потенційного клієнта.
4. Використання соціальних і медіа можливостей.
5. Впровадження опцій не пов'язаних з безпекою.

Висновки до розділу 4

Після проведеного аналізу, оцінки ризиків та підрахунку ймовірності реалізації, був зроблений висновок, що проект має високу можливість успішної комерціалізації і виходу на ринок. Обґрунтуваннями для такого рішення є високий рівень попиту на оптимізацію і посилення безпеки робочих процесів усередині підприємств, а також низьку вартість, що збільшує цільову аудиторію. Стартап проект має хороші шанси і перспективи для реалізації шляхом надання команди розробників, працюючи за технологією outstaffing, надання команди розробників компаніям, при цьому гарантуючи конфіденційність, захищеність даних і інших інформаційних одиниць при роботі в підприємстві. Альтернативним джерелом реалізації є навчання працівників підприємства, і їх супервайзінг при розробці та впровадженні даної технології. Я вважаю, що є перспектива просування і розвитку даного проекту.

ВИСНОВКИ

1. Було виконано аналіз існуючих тенденцій в моніторингу користувача для вирішення завдань безпеки: визначено основні підходи та засоби моніторингу, в тому числі веб-активності користувачів, аспекти їх використання і впровадження, та можливість впливу на інформаційну захищеність.
2. Проаналізовані існуючі рішення для реалізації моніторингу, проведено порівняльний аналіз можливостей: представлені порівняльні таблиці та зведені характеристики з зазначенням переваг та недоліків існуючих рішень та їх можливостей.
3. Виділено основні підходи до реалізації механізмів моніторингу та його напрямки при використанні контролю веб-активності співробітника підприємства. В тому числі проаналізовано можливості існуючих сервісів, платформ, які можуть використовуватись для задач моніторингу веб-активності.
4. Запропоновано засоби JavaScript, які можуть бути використані для вирішення задач моніторингу. Виділено показники, які можуть бути включені до веб-портрету користувача для виявлення його типової поведінки, оточення та вподобань – для подальшого виявлення відхилень від його звичайної поведінки. Використання цих засобів може бути двостороннім: 1) з точки зору організації-власника веб-ресурсу, з яким працюють в тому числі й працівники цієї організації (для захисту від ботів та запобігання DDoS, які маскуються під запити легітимних працівників) 2) з точки зору організації, працівники якої здійснюють доступ до зовнішніх веб-ресурсів (задля контролю дій працівників згідно встановленої політики безпеки використання зовнішніх ресурсів).
5. Запропоновано склад портрета веб-активності користувача, який складається із профілю вподобань, профілю базових даних, часового профілю, просторового профілю та профілю взаємодій;
6. Запропоновані рішення, які дозволяють контролювати активність працівника із використанням браузера: розроблено прототипи рішень, які контролюють веб-

активність співробітника компанії, забезпечують дотримання політики безпеки в реальному часі. За допомогою цих засобів формується веб-портрет користувача; поточний стан якого порівнюється із еталонним (що відповідає політиці безпеки). Запропоновано відповідні схеми збору та обробки даних.

7. Виконано аналіз практичних переваг запропонованих рішень: визначено, що розроблені рішення мають ряд переваг порівняно із вже існуючими (динамічність та можливість швидко змінювати та додавати новий функціонал; наявність можливостей щодо моніторингу активності користувача, актуальних саме для безпеки інформації) та містять необхідні якості, що дозволяють зайняти своє місце у певних сегментах на ринку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 Контроль роботи співробітників: види, методи, помилки [Електронний ресурс] – Режим доступа: https://sales-generator.ru/blog/kontrol-raboty-sotrudnikov/

2 Як контролювати роботу працівників: типові проблеми, помилки і методи їх подолання [Електронний ресурс] – Режим доступа:http://openstud.ru/blog/for-businessmen/howto-control-personnel/

3 Кращі системи контролю працівників та обліку робочого часу 2018 [Електронний ресурс] – Режим доступа: https://employee-monitoring-software.ru/

4 Kickidler. New perception of personnel work[Електронний ресурс] – Режим доступа: https://www.kickidler.com/

5 Top 10 Best Free Employee Monitoring Software 2018 [Електронний ресурс] – Режим доступа: https://www.spyzie.com/employee-tracking/top-10-best-free-employee-monitoring-software.html

6 Анатомія аналітики від Google [Електронний ресурс] – Режим доступа: https://habr.com/company/kaspersky/blog/334292/

7 10 хитрощів Google Analytics [Електронний ресурс] – Режим доступа: https://habr.com/company/icontext/blog/93851/

8 Clicktale documentation [Електронний ресурс] – Режим доступа: https://www.clicktale.com/solutions/

9 Clicktale Review [Електронний ресурс] – Режим доступа: https://uxmag.com/articles/clicktale-review

10 Segment.io Documentation [Електронний ресурс] – Режим доступа: https://segment.com/docs/

11 Mouseflow reveals why your visitors aren't converting into customers [Електронний ресурс] – Режим доступа: https://mouseflow.com/

12 Mouseflow Reviews [Електронний ресурс] – Режим доступа: https://www.trustradius.com/products/mouseflow/reviews

13 Click, Eye tracking, and Attention Scroll Heat Maps using SeeVolution [Електронний ресурс] – Режим доступа: https://www.seevolution.com/?tab=heat-maps

14 SeeVolution Pricing, Features, Reviews & Comparison of Alternatives [Електронний ресурс] – Режим доступа: https://www.getapp.com/business-intelligence-analytics-software/a/seevolution/

15 What Is A Website Tracking System [Електронний ресурс] – Режим доступа: https://help.opentracker.net/article/94-what-is-a-website-tracking-system

16 Top 5 best data loss prevention software in 2017 [Електронний ресурс] – Режим доступа: https://www.techradar.com/news/top-5-best-data-loss-prevention-services

17 SIEM: відповіді на типові запитання [Електронний ресурс] – Режим доступа: https://habr.com/post/172389/

18 SIEM ДЛЯ ЧАЙНИКОВ [Електронний ресурс] – Режим доступа: https://bakotech.ua/uploads/ckeditor/files/SIEM-for-Beginners-RU.PDF

19 Chrome getting started tutorial [Електронний ресурс] – Режим доступа: https://developer.chrome.com/extensions/getstarted

20 Chrome developer extensions [Електронний ресурс] – Режим доступа: https://developer.chrome.com/extensions/devguide

21 Chrome sample extensions [Електронний ресурс] – Режим доступа: https://developer.chrome.com/extensions/samples

22 Chrome Cross-Origin XMLHttpRequest [Електронний ресурс] – Режим доступа: https://developer.chrome.com/extensions/xhr

23 Chrome Declare Permissions [Електронний ресурс] – Режим доступа: https://developer.chrome.com/extensions/declare_permissions