ВЕБ-ПЛАТФОРМА ДЛЯ КОНТРОЛЯ НАД ИСПОЛЬЗОВАНИЕМ ЛИЧНЫХ ДАННЫХ

Чечко В.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Киселевский О.С. – канд. техн. наук, доцент

Данная работа призвана рассмотреть современный метод защиты персональных данных, что позволит усовершенствовать контроль над использованием информации сторонними субъектами.

В настоящее время бизнес-моделью значительного числа сайтов является предоставление бесплатного контента в обмен на персональные данные. Большинство пользователей не выступает против данных требований и легко соглашается с условиями. Однако после этого они не могут в полной мере следить за тем, кто именно получает доступ к информации, а также лишены возможности контролировать её дальнейшее распространение в пользу третьих лиц. Прежде чем приступить к решению данной проблемы, необходимо выяснить сущность понятия «персональные данные» [1].

Персональные данные – это любая информация, относящаяся к идентифицированному или поддающемуся идентификации физическому лицу («субъекту данных», то есть к человеку). Идентифицированное физическое лицо – это человек, идентификатор (имя, номер телефона, личный номер, логин и так далее) которого имеется среди данных.

Проанализировав особенности регистрации и хранения информации на различных сайтах, можно сделать вывод о том, что система защиты персональных данных нуждается в оптимизации. Одним из возможных способов решения данного вопроса является разработка специализированной веб-платформы, которая поможет избежать утечки сведений, предоставленных интернет-порталам. Пользователям будет предоставлена возможность отследить действия сторонних субъектов с возможностью блокировки их доступа к информации. В частности, можно будет узнать:

– для каких целей используются личные данные;
– кому и в какие страны они передаются;
– откуда получены (источники данных);
– информацию о важных решениях, которые принимаются автоматически[2].

С разрешения пользователя веб-платформе предоставляется доступ к сетевым аккаунтам на электронном устройстве с целью отслеживания посещённых сайтов. В дальнейшем будет производиться инкрементное резервное копирование персональных данных из интернет-порталов на сервер. При его использовании сначала делается полное резервное копирование, затем каждый файл, который был изменен, копируется каждый раз заново.

Далее вся информация преобразовывается при помощи ассиметричного шифрования. Под асимметричным шифрованием понимаются алгоритмы, при использовании которых данные шифруются и дешифруются разными, но математически связанными ключами – открытым и секретным соответственно. Открытый ключ сохраняется на портале и при шифровании им информации всегда можно получить исходные данные путем применения секретного ключа. Секретный ключ, необходимый для дешифрования информации, известен только пользователю. Структурная схема работы асимметричных криптосистем наглядно отображена на рисунке 1[3].

Рисунок 1 – Структурная схема работы асимметричных криптосистем

Полученные сведения при помощи их IP-адреса отслеживаются на предмет использования посторонними субъектами.

Таким образом, при помощи данной веб-платформы будет осуществлена надёжная защита и хранение персональных данных с возможностью их отслеживания.

Список использованных источников:

1. dev.by/ [Электронный ресурс]. – Режим доступа: https://dev.by/news/internet-challenges-by-tim-berners-lee – Дата доступа: 31.12.2021.

2. data-privacy-office.com/ [Электронный ресурс]. – Режим доступа: https://data-privacy-office.com/what-is-gdpr/#GDPR – Дата доступа: 31.12.2021.

3. wiki.merionet.ru/ [Электронный ресурс]. – Режим доступа: https://wiki.merionet.ru/seti/58/obzor-metodov-bezopasnogo-xraneniya-dannyx-na-servere/ – Дата доступа: 31.12.2021.