Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Михальков
Николай Васильевич

Методика идентификации пользователя интернет ресурсов

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук
по специальности 98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Богуш В.А.
д.ф-м.н., профессор

Минск 2019

ВВЕДЕНИЕ

Современный этап развития инфокоммуникационных услуг, сервисов и приложений информационно-телекоммуникационных сетей (ИТКС) общего пользования, в том числе Интернет, характеризуется появлением средств и методов, обеспечивающих анонимность пользователей в сети, а проблема их идентификации является одной из наиболее обсуждаемых представителями правоохранительных ведомств и экспертным сообществом.

Использование средств анонимизации, с одной стороны, обеспечивает пользователям возможность получения услуг связи и доступа к информационным ресурсам без раскрытия содержания передаваемых данных и личности потребителя, но, с другой стороны, статистика показывает, что более 70 % зафиксированных фактов применения средств анонимизации в сети Интернет использовалось для посещения запрещенных сайтов, ведения переписки незаконного характера (в том числе террористической направленности), организации виртуальных атак на информационные ресурсы коммерческих организаций и органов государственной власти. К тому же за последние три года количество пользователей, применяющих технологии анонимизации в сети Интернет, увеличилось вдвое.

Однако с учетом того, что применяемые на сегодня средства и методы анонимизации используют алгоритмы криптографических преобразований гарантированной стойкости, хранение зашифрованных данных пользователей без их привязки к конкретным узлам и устройствам сети на практике не дает желаемых результатов, а научно-технические решения в области идентификации логических соединений для подобных условий до сих пор не разработаны. Следует отметить, что в данной работе под *логическим соединением* понимается взаимосвязь, обеспечиваемая некоторым уровнем эталонной модели взаимодействия открытых систем, между двумя логическими объектами смежного верхнего уровня с целью обмена данными. Целью данной работы является разработка и апробация методики, обеспечивающей получение сведений о доступной информации о персональном компьютере пользователя для его уникальной идентификации.

Объектом исследования является программное обеспечение, используемое типовыми пользователями интернета на своих персональных компьютерах.

Предметом исследования являются методы и способы извлечения идентифицирующей информации с персонального компьютера пользователя.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке и апробации методики, обеспечивающей получение сведений о доступной информации о персональном компьютере пользователя для его уникальной идентификации.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Выполнить анализ типового программного обеспечения, используемого пользователями
2. Проанализировать методы и способы организации сбора идентифицирующей информации
3. Разработать и апробировать методику сбора идентифицирующей информации

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XVII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2019).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 2 статьи в сборниках материалов конференций.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, четырех глав, заключения и библиографического списка. Общий объем диссертации 67 страниц, 25 наименований в библиографическом списке.

Во введении приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится общее описание методов идентификации пользователей в информационно-телекоммуникационных сетях, содержащих средства анонимизации. Также проанализированы методы идентификации пользователя инфокоммуникационных услуг в сети Интернет.

Вторая глава посвящена методу идентификации на основе модели вероятностной связи. Проанализированы модели разнородного трафика и проблемы их применения. Обоснован выбор признакового пространства для решения задачи идентификации в сетях с анонимизацией. Разработан метод идентификации на основе вероятностной связи.

В третьей главе описывается алгоритм обработки эмпирических данных профилей логических соединений в сетях с анонимизацией при идентификации пользователей. Приведено обоснование исходных данных для построения алгоритма обработки эмпирических данных профилей логических соединений. Исследованы свойства разработанного алгоритма.

В четвертой главе проведена экспериментальная оценка эффективности алгоритма обработки эмпирических данных профилей логических соединений в сетях с анонимизацией при идентификации пользователей. Эксперимент проводился с использованием 2 различных ИТКС, обеспечивающих анонимный доступ пользователей, архитектура которых включала один прокси-сервер и цепочку из 3 прокси-серверов. В каждом повторении эксперимента изменялось количество пользователей в диапазоне от 10 до 250. Для перехвата пакетов, передаваемых по сети, использовался программный продукт WireShark версии 2.0.4.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

На сегодняшний день использование инфокоммуникационных услуг, предоставляемых по средствам глобальной сети Интернет, является повсеместной практикой, доступной как крупным компаниям, так и обычным пользователям. Возможность беспрепятственного обмена информацией привлекает внимание, как законопослушных граждан, так и злоумышленников, чья деятельность направлена на деструктивные воздействия с целью реализации виртуальных атак. Как правило, они осуществляются с применением различных средств анонимизации, позволяющих скрыть идентификационные данные. Использование данных средств может представлять непосредственную угрозу национальной безопасности.

Разработан метод идентификации на основе модели вероятностной связи, описывающей профили логического соединения ИТКС, содержащей средства анонимизации пользователей. Натурные эксперименты показали, что предложенный метод идентификации на основе модели вероятностной связи, описывающей профили логического соединения ИТКС, позволяет повысить точность идентификации при большом количестве соединений.

Для проверки гипотез об идентичности сравниваемых профилей с эталонным разработана решающая процедура отнесения анализируемого профиля логического соединения к одному из известных классов по принципу ближайшего соседа на основе расстояние Кульбака–Лейблера.

В связи с вышеизложенным, в рамках диссертационной работы решена актуальная задача, направленная на совершенствование методов идентификации логических соединений пользователей в ИТКС, содержащих средства анонимизации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 - А. Михальков Н.В. Влияние настроек браузера и операционной системы, установленных на персональном компьютере пользователя, на его идентификацию / Н.В. Михальков, Т.В. Борботько// Комплексная защита информации: Мат. XXIII науч.-практ. конф. / Москва: Медиа Группа «Авангард», 2018. С. 135-136. (22-24 мая 2018 г.).

2 - А. Михальков Н.В. Методика идентификации пользователя интернет ресурсов / Н.В. Михальков, Т.В. Борботько // Технические средства защиты информации: тезисы докладов XVII Белорусско-российской научно-технической конференции, Минск, 11 июня 2019г. / БГУИР; редкол : Т.В. Борботько [и др.]. – Минск, 2019. – С. 45.