УДК 37.000

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННУЮ ЭПОХУ

Михалькевич А.В., Кашникова И.В., Желакович И.М.

Институт информационных технологий БГУИР, г. Минск, Республика Беларусь

mihalkevich@bsuir.by, kashnikava@bsuir.by, zhelakovich@bsuir.by

В статье рассматриваются понятия приватности в информационную эпоху. Особое внимание уделяется информационной гигиене, безопасности в интернет и социальных сетях, использованию VPN и Proxy.

Ключевые слова: private; информационная безопасность; vpn; proxy.

В условиях современного информационного общества, характеризующегося постоянным потоком данных из различных источников, влияние информации на жизнь человека становится неотъемлемой частью повседневной жизни. Постоянный неконтролируемый информационный поток приводит к зависимости (от новостей, игр, сериалов, социальных сетей и прочих потоков информации). Также высокая активность в Интернете является повышенным источником рисков различного рода.

Данный обзор направлен на изучение методов обеспечения безопасности в условиях постоянного информационного потока с акцентом на необходимости соблюдения принципов информационной гигиены. Основываясь на предпосылке, что неконтролируемый информационный поток может привести к зависимости от разнообразных источников, рассматриваются практические шаги по регулированию этого потока и минимизации связанных с ним рисков.

Информационная гигиена

Если вы когда-нибудь заполняли формы на сайтах, указывая там личные данные, то вы добровольно передавали персональную информацию. Подобные действия сопровождаются возможностью использования вашей персональной информации третьими лицами, включая компании, правительственные организации, профессионалов в области данных и частных лиц, заинтересованных в приобретении таких данных [1].

Список компаний, которые занимаются сбором таких данных, огромен. Американская некомерческая организация «Privacy rights» собирает информацию о таких компаниях. По ссылке https://privacyrights.org/data-breaches можно скачать базу таких компаний с коротким описанием инцидентов, когда эти данные были получены третьими лицами. Даже в случае, если пользователь избегает предоставления личных данных в публичный доступ, современные технологии позволяют компаниям получать информацию из различных источников, включая электронные письма, чаты, данные о покупках в интернет-магазинах, посещенных веб-сайтах, телефонные разговоры и данные о местоположении. Это создает потенциальную угрозу для конфиденциальности данных, особенно учитывая возможность непреднамеренного нарушения законов, о существовании которых пользователь может не подозревать.

Дополнительно необходимо обратить внимание на хранение личных файлов, фотографий и видеозаписей на компьютере, представляющее потенциальную угрозу приватности. Облачные сервисы, несмотря на свою удобность, ограничивают контроль пользователя над своими данными, возможно даже в случае отсутствия желания делиться этой информацией.

Таким образом, современные практики использования цифровых технологий подчеркивают важность осознанности пользователей относительно безопасности и конфиденциальности их данных в цифровом пространстве.

VPN и Proxy для сокрытия IP-адреса

Для эффективного обеспечения безопасности в онлайн-среде предусмотрены такие инструменты, как виртуальные частные сети (VPN) и прокси-сервера. Они обеспечивают защиту интернет-соединения, хотя механизмы их функционирования и применения имеют свои особенности.

VPN шифруют любые отправляемые и получаемые данные; прокси-серверы этого не делают. Шифрование данных обеспечивает дополнительную безопасность таких конфиденциальных транзакций, как действия в онлайн-банке и покупки в Интернете, а также не позволяет злоумышленникам отследить данные вашей кредитной карты и учетные данные для входа.

В зависимости от способа доступа, и VPN, и прокси-серверы могут замедлять работу в Интернете. Чаще всего более медленными (и менее безопасными) являются бесплатные прокси-соединения, как правило, из-за меньшего количества параметров конфигурации, сокращенной инфраструктуры и неполной поддержки. Скорость VPN зависит от провайдера, однако, как правило, VPN является более быстрым вариантом.

Бесплатные VPN-сервисы, как правило, ограничены по функционалу и могут собирать ваши данные. Платные VPN обеспечивают лучшее шифрование данных и являются более безопасными. Многие прокси-серверы, в отличие от VPN, являются бесплатными. Как правило, VPN – это более дорогой вариант.

VPN работают на уровне операционной системы и перенаправляют весь трафик через VPN-сервер, а прокси-серверы работают на программном уровне и перенаправляют трафик только определенного приложения или браузера. Это означает, что VPN шифруют все действия в интернете, независимо от сайта и приложения, а прокси-серверы в каждый момент времени могут скрыть только один сайт или приложение. В результате VPN обеспечивают большее покрытие.

Большинство провайдеров VPN не регистрируют веб-трафик, чего нельзя сказать о прокси-серверах. Для полной конфиденциальности рекомендуется использовать услуги провайдера VPN с политикой отсутствия журналов. Такие провайдеры не отслеживают и не сохраняют действия пользователей в Интернете. Бесплатные прокси-серверы, напротив, могут регистрировать трафик для продажи данных третьим лицам.

Безопасность общественных сетей

Когда речь идет о подключении к общественным Wi-Fi сетям, важным аспектом является уникальный идентификатор подключаемого устройства – MAC-адрес. Для поддержания анонимности и предотвращения отслеживания, рекомендуется изменять MAC-адрес перед подключением к общественной сети. Однако важно помнить, что после перезагрузки устройства MAC-адрес может восстановиться, поэтому такие действия следует повторять при каждом новом подключении.

Безопасность общественных компьютеров

При использовании общественных компьютеров, особенно в интернет-кафе, встает проблема обеспечения минимальных полномочий пользователей. Принцип «минимальных полномочий» подразумевает предоставление пользователю только необходимого минимума прав для выполнения задачи. Однако часто общественные компьютеры имеют права системного администратора, что позволяет устанавливать любое программное обеспечение, а это нарушает принцип «минимальных полномочий» и повышает риск того, что кто-то уже установил вредоносную программу. Такие программы достаточно сложно выявить. А это

значит, что все логины и пароли, которые вы вводите на интернет-ресурсах в общественных компьютерах, могут стать известны третьим лицам.

В связи с этим, рекомендуется использовать личные точки доступа или, в случае необходимости, принимать меры по обеспечению конфиденциальности при использовании общественных компьютеров. При использовании общественных компьютеров важно соблюдать осторожность при вводе личной информации. Закрытие сессий, удаление сохраненных данных и избегание хранения личных файлов на таких устройствах снижают риск утечки конфиденциальной информации.

Безопасные фотографии и файлы

В контексте безопасности фотографий и файлов важным аспектом является управление метаданными. Примером может служить стандарт EXIF, Стандарт EXIF, встроенный в фотографии, может содержать разнообразную информацию, включая геолокацию, дату, и модель камеры. Эти данные представляют потенциальную угрозу конфиденциальности. Применение активных шагов, таких как удаление или изменение метаданных перед публикацией, а также бережное отношение к выбору контента для онлайн-публикаций, являются важными шагами для обеспечения личной безопасности и предотвращения раскрытия личных данных.

Опасные социальные сети

В контексте безопасности социальных сетей, важно отметить, что даже при наличии попыток обеспечения конфиденциальности на платформах, таких как Facebook, Google и Instagram, существуют потенциальные угрозы, связанные с использованием передовых технологий [2]. Например, применение технологии распознавания лиц на Facebook может привести к раскрытию личной информации, так как платформа старается идентифицировать людей на загруженных фотографиях. Такие данные могут быть использованы злоумышленниками для несанкционированного доступа к личной информации.

Google, в свою очередь, осуществляет не только определение местоположения и распознавание лиц, но также персонализирует рекламу и поисковую выдачу на основе собранных данных. Этот процесс может представлять потенциальную угрозу приватности, поскольку создается детализированный профиль пользователя.

Важным моментом является осознание пользователем возможных рисков и принятие мер предосторожности. Рекомендуется воздерживаться от предоставления правдивой персональной информации в профилях социальных сетей и внимательно следить за настройками конфиденциальности. Введение ложных данных может снизить вероятность раскрытия личной информации. Однако, несмотря на предпринятые меры предосторожности, важно понимать, что абсолютной гарантии безопасности в сфере онлайн-коммуникаций не существует.

Банковские карты

Особое внимание следует уделять безопасности банковских карт. Естественно, данные банковских карт нельзя передавать третьим лицам. Но чтобы защититься от мошеннических транзакций (например, списания большей суммы) этого недостаточно.

Рекомендуется заводить две банковские карты, привязанные к различным счетам. Одна – обычная, пластиковая, вторая – виртуальная. Для расчетов в сети использовать только виртуальную карту, на которую предварительно переводится необходимая для транзакции сумма. Основные средства следует хранить на другой карте, данные которой никогда не использовать в сети.

Заключение

Существует еще ряд важных аспектов в области информационной безопасности, с которыми необходимо более детально разобраться. Это включает в себя безопасность умных домов и интернета вещей, аспекты защиты в современных автомобилях, безопасность общественного транспорта и многие другие.

Пристальное внимание следует уделять информированию и защите персональных данных наиболее уязвимых слоев населения – несовершеннолетних, пенсионеров и лиц с

особыми потребностями. Именно они чаще всего являются объектами самых различных видов мошенничества и недобросовестного сотрудничества [3].

Кроме того, организации и компании, которые собирают и хранят нашу персональную информацию, также должны принимать меры по ее защите. Они должны использовать современные технологии шифрования и механизмы контроля доступа, чтобы предотвратить несанкционированный доступ к нашей информации.

В целом, защита персональной информации является важным аспектом нашей жизни в информационную эпоху. Мы должны быть осторожными и проактивными в отношении нашей персональной информации, чтобы защитить нашу личную жизнь и конфиденциальность данных.

Литература

1. Защита персональных данных в интернете [Электронный ресурс]. – Режим доступа: https://beseller.by/blog/zashchita-personalnykh-dannykh-belarus/. – Дата доступа: 12.11.2023.

2. Что важно знать о защите персональных данных [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2022/november/72150/. – Дата доступа: 12.11.2023.

3. Детям о персональных данных [Электронный ресурс]. – Режим доступа: https://cpd.by/populyarnoye-na-sayte/detyam-o-personalnyh-dannyh/. – Дата доступа: 12.11.2023.

SECURITY OF PERSONAL DATA IN THE INFORMATION AGE

Mikhalkevich A.V., Kashnikova I.V., Zhelakovich I.M.

Institute of Information Technologies BSUIR, Minsk, Republic of Belarus

The article examines the concepts of privacy in the information age. Particular attention is paid to information hygiene, security on the Internet and social networks, the use of VPN and Proxy.

Key words: private; information security; vpn; proxy.