**Лабораторная работа 1**

# **Topic**

Anonymous Networks; Anonymity; Traffic Analysis

# **Описание предметной области**

Данный топик охватывает исследования в области анонимности в интернете, в частности обеспечение анонимности и безопасности сетей и защита от анализа трафика с целью сбора информации.

Анонимность — способ остаться незамеченным во Всемирной сети.

Анонимные сети — компьютерные сети, созданные для достижения анонимности в Интернете и работающие поверх глобальной сети.

Анализ трафика — это процесс перехвата и изучения сообщений с целью извлечения информации из шаблонов в общении. ­­­­­

# **Недостаток (Gap)**

Опуская главную проблему анонимности в его использовании в преступной деятельности, обеспечение конфиденциальности требует многоуровневое шифрование, что увеличивает объём трафика, время отклика и потерю пропускной способности. Главной же угрозой систем безопасности является постоянно совершенствующиеся методы анализа трафика, что увеличивает риск нарушения приватности пользователей.

# **Идея**

Создание новой интернет-архитектуры.

# **Краткий текст обзора**

Анонимные сети, такие как Tor, I2P и другие играют ключевую роль в обеспечении приватности и анонимности пользователей в интернете, их основные методы описаны в статье [11]. Они работают путем маршрутизации трафика через различные узлы, что делает сложным отслеживание и идентификацию конечного пользователя, что исследуется в статье [6]. Эти сети также обеспечивают многоуровневое шифрование данных и скрывают IP-адреса, позволяя поддерживать высокий уровень анонимности.

Однако, несмотря на преимущества анонимных сетей, в исследованиях приведены методы анализа трафика, которые могут быть использованы для обхода анонимности и идентификации пользователей. Например, в одной из статей [7] на примере Tor демонстрируется возможность обычному злоумышленнику совершить атаку и снизить анонимность сети. Также точка обмена интернет-трафиком (Internet eXchange, IX), к которому подключается Tor, может быть использована для анализа трафика [10]. Что более важно, начиная с 2010-ых гг. сайты начали блокировать Tor, что ограничивает его использование для обычных пользователей [5].

На данный момент проблема с обеспечением анонимности и безопасности решается с помощью совершенствования существующих протоколов безопасности и анонимных сетей [2], [3], [8]. Также имеется предложение по созданию новой анонимной сети [12] или изменению методов анонимизации [9]. Однако проблему можно попытаться решить иным путём. Суть идеи – создание другой интернет-архитектуры, которая позволит исключить использование узлов с числовыми данными. Это позволит обеспечить высокую анонимность пользователей, так как в таком случае будет сложно отследить источник и идентифицировать его.

Таким образом, на данный момент предложено множество различных вариантов решения проблемы с анонимностью и анализом трафика. Стоит учитывать, что подобные исследования быстро становятся неактуальными ввиду постоянной «технологической гонки» в сфере кибербезопасности.

# **Источники**

[1] S. DiBenedetto, P. Gasti, G. Tsudik, и E. Uzun, «ANDaNA: Anonymous Named Data Networking Application». arXiv, 2012 г.

[2] J. Kong и X. Hong, «ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks». 2003 г.

[3] A. Kate, G. M. Zaverucha, и U. Hengartner, «Anonymity and security in delay tolerant networks», *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, Nice, France: IEEE, 2007, сс. 504–513. doi: 10.1109/SECCOM.2007.4550373.

[4] R. Dingledine и N. Mathewson, «Anonymity Loves Company: Usability and the Network Eﬀect», в *Security and Usability: Designing Secure Systems That People Can Use*, O’Reilly Media, 2005.

[5] S. Khattak *etc.*, «Do You See What I See? Differential Treatment of Anonymous Users», в *Proceedings 2016 Network and Distributed System Security Symposium*, San Diego, CA: Internet Society, 2016, сс. 547–561. doi: 10.14722/ndss.2016.23342.

[6] N. Feamster и R. Dingledine, «Location diversity in anonymity networks», в *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, Washington DC USA: ACM, 2004, сс. 66–76. doi: 10.1145/1029179.1029199.

[7] S. J. Murdoch и G. Danezis, «Low-Cost Traffic Analysis of Tor», в *2005 IEEE Symposium on Security and Privacy (S&P’05)*, Oakland, CA, USA: IEEE, 2005, сс. 183–195. doi: 10.1109/SP.2005.12.

[8] D. Sy, R. Chen, и L. Bao, «ODAR: On-Demand Anonymous Routing in Ad Hoc Networks», в *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Sysetems*, Vancouver, BC, Canada: IEEE, 2006, сс. 267–276. doi: 10.1109/MOBHOC.2006.278565.

[9] S. Yu, G. Zhao, W. Dou, и S. James, «Predicted Packet Padding for Anonymous Web Browsing Against Traffic Analysis Attacks», *IEEE Trans.Inform.Forensic Secur.*, vol. 7, issue 4, сс. 1381–1393, 2012, doi: 10.1109/TIFS.2012.2197392.

[10] S. J. Murdoch и P. Zieliński, «Sampled Traffic Analysis by Internet-Exchange-Level Adversaries», в *Privacy Enhancing Technologies*, т. 4776, N. Borisov и P. Golle, Ред., в Lecture Notes in Computer Science, vol. 4776., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, сс. 167–183. doi: 10.1007/978-3-540-75551-7\_11.

[11] J. Ren и J. Wu, «Survey on anonymous communications in computer networks», *Computer Communications*, т. 33, вып. 4, сс. 420–431, ­2010, doi: 10.1016/j.comcom.2009.11.009.

[12] A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, и G. Danezis, «The Loopix Anonymity System», *SEC’17: Proceedings of the 26th USENIX Conference on Security Symposium*, сс. 1199–1216, 2017.