**ФИО**

**Бисултанов У.З , Волянюк М.И**

**TOPIC**

hardware security; intellectual property piracy; obfuscation

**Описание предметной области**

Данный топик охватывает исследования в области безопасности приложений в частности защиты интеллектуальной собственности от пиратства и метода обфускации. Интеллектуальная собственность – результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации предпринимателей и юридичeских лиц. Обфускация - процесс изменения кода программы, в результате которого он приобретает вид, трудный для понимания.

**Недостаток**

Есть примеры применения на практике обфускации для защиты приложений от пиратства, но тем не менее этот способ имеет свои недостатки, например, потеря гибкости кода. Код после обфускации может стать более зависимым от платформы или компилятора. Трудности отладки. Обфускатор не даёт постороннему выяснить, что делает код, но и не даёт разработчику отлаживать его. При отладке приходится отключать обфускатор. Недостаточная безопасность обфускации - наиболее приоритетное направление в совершенствовании защиты интеллектуальной собственности, требующее внедрения новых разработок.

**Идея**

Комбинирование различных техник обфускации и использование метода шифрования. Обновление, улучшение механизмов обфускации и сопротивления атакам и анализу для защиты интеллектуальной собственности.

**Краткий текст обзора**

При решении задачи защиты интеллектуальной собственности посредством обфускации значительное внимание выделяется методу обратной разработки – преобразование машинного кода в язык программирования и исследование последнего на уязвимости [1]-[4], [6]. Публикации на данную тему были актуальны с момента появления компьютера и интернета. За все время было придумано и разработано множество методов, среди которых необходимо выделить такие методы как криптография, Byte Level Manipulation [9], [11], Physical Unclonable Function (PUF) [8], [10], Register Transfer Level (RTL) [7], метод конечных автоматов [4], [5]. Для решения задачи защиты интеллектуальной собственности с использованием обфускации предложен ряд решений, отличающихся вычислительной сложностью и рядом других особенностей.

Решить проблему аппаратной безопасности при цифровой обработке сигналов (DSP) необходимо с помощью аппаратной обфускации[1]. Так в работе Ziebermayr et al. [2] представлена концепция безопасной, эффективной и простой защиты программного обеспечения. Концепция заключается в том, что промышленность может безопасно поставлять программное обеспечение вместе со своими аппаратными продуктами без риска нарушения прав интеллектуальной собственности из-за незаконных копий, обратного проектирования и модификации. Более того, Subhra et al.[11] предлагает методологию запутывания пространства состояний, эффективно блокирует конструкцию на уровне шлюза, и только законный пользователь может разблокировать ее с применением предопределенного ключа в виде последовательности входных векторов. Недостаточная безопасность обфускации - наиболее приоритетное направление в совершенствовании защиты интеллектуальной собственности и является основным недостатком, который был выявлен нами в процессе анализа статей. Данную проблему можно предотвратить посредством комбинирования различных техник обфускации и использования метода шифрования, а также обновления и улучшения механизмов обфускации. Таким образом, данные публикации помогли нам понять преимущества одних методов защиты интеллектуальной собственности над другими и предоставили фундамент для их совершенствования и совмещения друг с другом.

**References**

[1] R. Naveenkumar, ‘Journal of Electronic Testing’, *Hardw. Obfuscation IP Prot. DSP Appl.*, no. 38, pp. 9–20, Mar. 2022, doi: s10836-022-05984-2.

[2] T. Ziebermayr, ‘Proceedings of the 2nd International Conference on Industry 4.0 and Smart Manufacturing (ISM 2020)’, *Prot. Intellect. Prop. Rights Ind. Softw.*, no. 180, pp. 862–866, 2021, doi: 10.1016/j.procs.2021.01.336.

[3] J. Blocklove, ‘Hardware Intellectual Property Protection Through Obfuscation Methods’, Rochester Institute of Technology, 2020. Accessed: Feb. 22, 2024. [Online]. Available: https://repository.rit.edu/cgi/viewcontent.cgi?article=11611&context=theses

[4] M. Fyrbiak, ‘On the Difficulty ofFSM-based Hardware Obfuscation’, *Diffic. OfFSM-Based Hardw. Obfuscation*, no. 3, pp. 293–330, 2018, doi: 10.13154/tches.v2018.i3.293-330.

[5] M. Yousra, ‘USENIX Security Symposium’, *Act. Hardw. Metering Intellect. Prop. Prot. Secur.*, no. 16, pp. 291–306, Aug. 2017, doi: 1362903.

[6] A. Sarah, ‘Comparative Analysis of Hardware Obfuscation for IP Protection’, Florida, USA, 2017. Accessed: Feb. 22, 2024. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3060403.3060495

[7] D. Forte, *State Space Obfuscation and Its Application in Hardware Intellectual Property Protection*, Springer., vol. 1, 1 vols. Florida, USA: Springer International Publishing AG 2017, 2017. Accessed: Feb. 22, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-49019-9\_8

[8] J. Zhang, ‘A Practical Logic Obfuscation Technique for Hardware Security’, Software College, Northeastern University, Shenyang, China, 2015. Accessed: Feb. 22, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7128395

[9] K. Chandan, ‘Proceedings of the 4th International Conference on Eco-friendly Computing and Communication Systems’, *Differ. Obfuscation Tech. Code Prot.*, no. 70, pp. 757–763, 2015, doi: S1877-0509(15)03312-8.

[10] J. Todd McDonald, ‘Proceedings of the 7th International Conference on Information warfare and security university of Washington’, *Examing Trade Hardw.-Based Intellect. Prop. Prot.*, no. 7, pp. 192–202, 23.03 2012.

[11] R. Subhra, ‘Hardware Security through Design Obfuscation’, Case Western Reserve University, EECS - Computer Engineering, 2010. Accessed: Feb. 22, 2024. [Online]. Available: https://etd.ohiolink.edu/acprod/odb\_etd/etd/r/1501/10?clear=10&p10\_accession\_num=case1270133481