ПЕРЕЛІК ПОСИЛАНЬ

1. Чеканін О.Ю., Жданова О.Г. Модель загроз для оцінки безпеки автомобіля // Матеріали науково-практичної конференції «Інформатика та обчислювальна техніка ІОТ-2018». – м. Київ.: НТУУ «КПІ ім. Ігоря Сікорського», 23-24 квітня 2018.

2. A. Saad and U. Weinmann, “Automotive software engineering and concepts,” in GI Jahrestagung, pp. 318–319, Frankfurt, Germany, September-October 2003.

3. E. Nickel, “IBM automotive software foundry,” in Press Conference on Computer Science in Automotive Industry, Frankfurt University, Frankfurt, Germany, September 2003.

4. Kaspersky, E.: Viruses are coming aboard?, Viruslist.com – Режим доступу до ресурсу: http://www.viruslist.com/en/weblog?discuss=158190454&return=1.

5. [Електроний ресурс] Car-2-Car Communication Consortium (June 2008), http://www.car-2-car.org/

6. Hackers remotely kill a jeep on the highway—with me in it. – Режим доступу до ресурсу: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

7. Lang, A., Dittmann, J., Kiltz, S., Hoppe, T.: Future Perspectives: The Car and its IPAddress - A Potential Safety and Security Risk Assessment. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007. LNCS, vol. 4680. Springer, Heidelberg (2007).

8. Tobias Hoppe, Stefan Kiltz, and Jana Dittmann: Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures.

9. Guide to Intrusion Detection and Prevention Systems (IDPS) – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-94/final.

10. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security, Min-Joo Kang, Je-Won Kang.

11. Design and implementation of an intrusion detection system (IDS) for in-vehicle networks, Noräs Salman, Marco Bresch.

12. A Neural Network based system for Intrusion Detection and attack classification, Basant Subba , Santosh Biswas, Sushanta Karmakar

13. Neural Network based Intrusion Detection Systems, Sodiya A.S, Ojesanmi O.A, Akinola O.C, Aborisade O.

14. Neural Network Based Intrusion Detection System for Critical Infrastructures Ondrej Linda, Todd Vollmer, Milos Manic.

15. Журнал Хакер 03 /194/ 2015, с.16-19.

16. Bus Systems – Режим доступу до ресурсу: https://automotive.softing.com/en/standards/bus-systems.html

17. Bosch CAN Specification version 2.0, Robert Bosch Gmbh, Postfach 50, D-7000 Stuttgart.

18. ISO 17987. Road vehicles - Local Interconnect Network (LIN) Part 1-7. ISO 17987:2016. Geneva, Switzerland: Internation Organization for Standardization, 2016.

19. ISO 17458. Road vehicles - FlexRay communications system Part 1-5. ISO 17458-5:2013. Geneva, Switzerland: Internation Organization for Standardization, 2013.

20. MOST Specification Rev 2.5 10/2006.

21. G Leen, D Heffernan, Expanding Automotive Electronic Systems, Computer, 3518893Jan. 2002 – Режим доступу до ресурсу: http://ltodi.est.ips.pt/malves/Gaveta/tme/can-automoveis.PDF

22. Technical Papers on the Development of Embedded Electronics, 6th Edition – Режим доступу до ресурсу: https://vector.com/portal/medien/cmc/marketing_items/ web/91102.pdf

23. ISO/IEC 7498-1. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994. Geneva, Switzerland: Internation Organization for Standardization, 1994.

24. Система виявлення атак – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IDS

25. Зоріна Т.І.

26. Системи виявлення і запобігання атак в комп’ютерних мережах / Т.І. Зоріна // Вісник Східноукраїнського національного університету імені Володимира

Даля. - 2013. - № 15(1). - С. 48-52. - Режим доступу: http://nbuv.gov.ua/UJRN/VSUNU_2013_15%281%29__9

27. Intrusion Detection Systems – Режим доступу до ресурсу: http://www.vce-download.net/study-guide/comptia-securityplus-2.4.1-intrusion-detection-systems.html

28. Сигнатура атаки – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.

29. Штучна нейронна мережа – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа.

30. Прогнозування за допомогою нейронних мереж – Режим доступу до ресурсу: wiki.tntu.edu.ua/Прогнозування_за_допомогою_нейронних_мереж.

31. Cannady, J. (1998) Artificial Neural Networks for Misuse Detection. National Information Systems Security Conference, 368-381.

32. Експертні системи – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Експертні_системи.

33. Wolf, M., Weimerskirch, A., Wollinger, T.: State of the Art: Embedding Security in Vehicles. EURASIP Journal on Embedded Systems 2007, 16 (2007); Article ID 74706, 16 pages, 2007. doi:10.1155/2007/74706

34. Ed Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk 2015 – Режим доступу до ресурсу: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

35. K. Koscher et al., “Experimental security analysis of a modern automobile,” in Proceedings — IEEE Symposium on Security and Privacy, 2010, pp. 447–462

36. Циклічний надлишковий код – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Циклічний_надлишковий_код.

37. RFC2828. Shirey, R., "Internet Security Glossary", RFC 2828, DOI 10.17487/RFC2828, May 2000.

38. ISO/IEC, "Information technology - Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008.

39. Winsen, Stijn van, “Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles”, 2017 – Режим доступу до ресурсу: http://essay.utwente.nl/71792/.

40. Dr. Charlie Miller, Chris Valasek, “Adventures in Automotive Networks and Control Units” – Режим доступу до ресурсу: http://illmatics.com/car_hacking.pdf.

41. S. Checkoway et al., “Comprehensive experimental analyses of automotive attack surfaces”. In Proceedings of the 20th USENIX Conference on Security, SEC’11.

42. ISO 26262. Road vehicles – Functional safety. ISO 26262:2012. Geneva, Switzerland: Internation Organization for Standardization, 2012.

43. Draft NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

44. The STRIDE Threat Model – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

45. David Ward, Ireri Ibara, and Alastair Ruddle. “Threat Analysis and Risk Assessment in Automotive Cyber Security.” In: SAE International Journal of Passenger Cars-Electronic and Electrical Systems 6.2 (2013), pp. 507–513. ISSN: 1946-4622. DOI: doi:10.4271/2013-01-1415.

46. Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, 2015 – Режим доступу до ресурсу: https://www.govtrack.us/congress/bills/106/hr5164/text.

47. Defcon: Hacking Tire Pressure Monitors Remotely – Режим доступу до ресурсу: https://www.networkworld.com/article/2231495/cisco-subnet/defcon---hacking-tire-pressure-monitors-remotely.html.

48. Mauw, S., Oostdijk, M.: Foundations of Attack Trees. In Won, D., Kim, S., eds.: ICISC. Volume 3935 of LNCS., Springer (2005) 186–198.

49. Ishtiaq Roufa et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”. ISBN: 888-7-6666-5555-4.

50. Attack Surface Analysis Cheat Sheet – Режим доступу до ресурсу: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.

51. Pratyusa K. Manadhata, “An Attack Surface Metric”, November 2008.

52. AUTOSAR FO Release 1.3.0 Glossary – Режим доступу до ресурсу: https://www.autosar.org/fileadmin/user_upload/standards/foundation/1-3/AUTOSAR_TR_Glossary.pdf.

53. Real-Time Systems, Stefan M. Petters – Режим доступу до ресурсу: http://www.cse.unsw.edu.au/~cs9242/08/lectures/09-realtimex2.pdf

54. Ключевые рекомендации по глубокому обучению (Часть 2) – Режим доступу до ресурсу: http://datareview.info/article/eto-nuzhno-znat-klyuchevyie-rekomendatsii-po-glubokomu-obucheniyu-chast-2.

55. The Python Tutorial – Режим доступу до ресурсу: https://docs.python.org/3/tutorial/index.html

56. python-can – Режим доступу до ресурсу: https://python-can.readthedocs.io/en/stable/.

57. NumPy – Режим доступу до ресурсу: http://www.numpy.org/.

58. TensorFlow – Режим доступу до ресурсу: https://www.tensorflow.org/.

59. Keras: The Python Deep Learning library – Режим доступу до ресурсу: https://keras.io/.

60. SocketCAN – Режим доступу до ресурсу: https://www.kernel.org/doc/Documentation/networking/can.txt.

61. Виключення (нейронні мережі) – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Виключення_(нейронні_мережі).

62. Adam: A Method for Stochastic Optimization, Diederik Kingma, Jimmy Ba – Режим доступу до ресурсу: https://arxiv.org/abs/1412.6980v8.s