**Лабораторная работа 1 ОНИ**

**ФИО**

Рыжков М.А. (группа 6112)

**Topic**

Computer Security; Social Responsibility; Impact Assessment

**Описание предметной области**

Компьютерная безопасность на сегодняшний день является одним из ключевых аспектов информационной безопасности, направленных на защиту компьютерных систем и информации от несанкционированного доступа, утечек и повреждений. Социальная ответственность в этом контексте означает понимание и осознание важности обеспечения безопасности в сети для всех участников. Оценка воздействия, в свою очередь, представляет собой процесс анализа и прогнозирования возможных последствий для общества в случае нарушения компьютерной безопасности и играет важную роль в разработке эффективных стратегий защиты и противодействия угрозам.

**Недостаток**

Все рассмотренные в статьях методы обеспечения безопасности не устойчивы к появлениям новых видов угроз.

**Идея**

Предлагается подход, основанный на концепции непрерывного мониторинга и анализа угроз.Этот подход предусматривает применение автоматизированных систем мониторинга с использованием искусственного интеллекта.

**Краткий текст обзора**

В сфере компьютерной безопасности значительное внимание уделяется различным методам защиты от кибератак и угроз информационной безопасности. Особый интерес исследователей привлекали методы, основанные на анализе уязвимостей [[1], [2]](https://www.zotero.org/google-docs/?WpSO4O) и сценариях атак. Например, для оценки безопасности используется метод моделирования атак[[3]](https://www.zotero.org/google-docs/?Pdoot0), а для создания новых систем защиты используется метод сбора и сортировки информации об уже совершенных атаках [[4], [5], [6]](https://www.zotero.org/google-docs/?6LtZko). Однако эти методы затрагивают только техническую часть вопроса. Немаловажным фактором обеспечения информационной безопасности является социальная ответственность и человеческий аспект[[7]](https://www.zotero.org/google-docs/?L5x1nb). Например, компании, которые берут на себя ответственность за хранение данных о пользователях, должны руководствоваться именно социальная ответственность. Об этом достаточно подробно написано в статье [[8]](https://www.zotero.org/google-docs/?HiLLAp). К сожалению, закон не успевает за развитием технологий. В результате компании стараются соответствовать закону, а не технологиям, из-за этого появляются “пробелы” в безопасности [[9]](https://www.zotero.org/google-docs/?Ov2HlW).

В статье [[5]](https://www.zotero.org/google-docs/?CM796l) рассматривается оценка воздействия кибератак с помощью виртуальной местности (VTAC) в качестве примеров ее работы используются только смоделированные атаки. Еще одним методом оценки безопасности безопасности является алгоритм, основанный на использовании графов атак[[6]](https://www.zotero.org/google-docs/?rBmjtS). Для упрощения процесса принятия решений с использованием визуализации информации применяется InfoVis[[10]](https://www.zotero.org/google-docs/?HgI9bE). Все перечисленные методы не могут оперативно адаптироваться к появлению новых видов угроз.

В моей статье я предлагаю новые методы оценки безопасности, моделирования угроз и оценки рисков, которые будут использовать автоматизированные системы мониторинга с применением искусственного интеллекта.

References

[[1] Q. S. Qassim, N. Jamil, M. Daud, A. Patel, и N. Ja’affar, «A review of security assessment methodologies in industrial control systems», *Inf. Comput. Secur.*, т. 27, вып. 1, сс. 47–61, 2019, doi: 10.1108/ICS-04-2018-0048.](https://www.zotero.org/google-docs/?7ImV45)

[[2] H. Nissenbaum, «Where Computer Security Meets National Security1», *Ethics Inf. Technol.*, т. 7, вып. 2, сс. 61–73, 2005, doi: 10.1007/s10676-005-4582-3.](https://www.zotero.org/google-docs/?7ImV45)

[[3] D. M. Nicol, «Modeling and Simulation in Security Evaluation», *IEEE Secur. Priv. Mag.*, т. 3, вып. 5, сс. 71–74, 2005, doi: 10.1109/MSP.2005.129.](https://www.zotero.org/google-docs/?7ImV45)

[[4] J. Gao, B. Zhang, X. Chen, и Z. Luo, «Ontology-based model of network and computer attacks for security assessment», *J. Shanghai Jiaotong Univ. Sci.*, т. 18, вып. 5, сс. 554–562, 2013, doi: 10.1007/s12204-013-1439-5.](https://www.zotero.org/google-docs/?7ImV45)

[[5] B. J. Argauer и S. J. Yang, «VTAC: virtual terrain assisted impact assessment for cyber attacks», представлено на SPIE Defense and Security Symposium, B. V. Dasarathy, Ред., Orlando, FL, 2008, с. 69730F. doi: 10.1117/12.777291.](https://www.zotero.org/google-docs/?7ImV45)

[[6] I. Kotenko и E. Doynikova, «Security Assessment of Computer Networks Based on Attack Graphs and Security Events», в *Information and Communication Technology*, т. 8407, Linawati, M. S. Mahendra, E. J. Neuhold, A. M. Tjoa, и I. You, Ред., в Lecture Notes in Computer Science, vol. 8407. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, сс. 462–471. doi: 10.1007/978-3-642-55032-4\_47.](https://www.zotero.org/google-docs/?7ImV45)

[[7] D. Besnard и B. Arief, «Computer security impaired by legitimate users», *Comput. Secur.*, т. 23, вып. 3, сс. 253–264, 2004, doi: 10.1016/j.cose.2003.09.002.](https://www.zotero.org/google-docs/?7ImV45)

[[8] T. Tsiakis, «Contribution of corporate social responsibility to information security management», *Inf. Secur. Tech. Rep.*, т. 14, вып. 4, сс. 217–222, 2009, doi: 10.1016/j.istr.2010.05.001.](https://www.zotero.org/google-docs/?7ImV45)

[[9] J. Boeken, «From compliance to security, responsibility beyond law», *Comput. Law Secur. Rev.*, т. 52, с. 105926, 2024, doi: 10.1016/j.clsr.2023.105926.](https://www.zotero.org/google-docs/?7ImV45)

[[10] D. J. Ferreira, N. Mateus-Coelho, и H. S. Mamede, «Methodology for Predictive Cyber Security Risk Assessment (PCSRA)», *Procedia Comput. Sci.*, т. 219, сс. 1555–1563, 2023, doi: 10.1016/j.procs.2023.01.447.](https://www.zotero.org/google-docs/?7ImV45)