**Лабораторная работа 1**

**ФИО**

Сенютин Сергей Сергеевич

Ухтверов Матвей Сергеевич

**Topic**

Malware; Center Manifold Theorem; Worms

**Описание предметной области**

Данный топик охватывает такие предметные области, как вредоносное ПО (malware), теорема о центральной многообразии (center manifold theorem) и компьютерные черви (worms). Вредоносное ПО – это программное обеспечение, разработанное для нанесения вреда компьютерным системам и пользователям. Center Manifold Theorem это - теорема из области математики, которая используется для изучения динамики систем, как в природе, так и в компьютерных науках. Компьютерные черви – это малваре, способные автоматически распространяться по компьютерным сетям, проникая в различные узлы и поражая их вредоносным кодом.

**Недостатки (Gap)**

Главным недостатком в противодействии угрозам является большое количество посредственных антивирусов, предоставляющих неполную защиту

**Идея**

Создание универсального антивируса, встроенного в операционную систему.

**Краткий текст обзора**

Задача изучения угрозы вирусов состоит в понимании как им противодействовать. Поэтому анализ принципов работы антивирусов состоит в рассмотрении их алгоритмов нахождения угроз, что и было произведено в данной работе. Опасность вредоносного софта до сих пор актуальна по сегодняшний день,

ежедневно появляются новые разновидности угроз, с которыми борются разработчики антивирусов.

Значительное внимание раньше уделялось изучению “Center Manifold Theorem”. Приближенное решение системы в нормальной форме Пуанкаре использует формулы, вычисляемые из частных производных системы.[[1]](https://www.zotero.org/google-docs/?3R0QdZ) Также представлено новое доказательство существования центрального многообразия в негиперболической точке равновесия векторного поля.[[2]](https://www.zotero.org/google-docs/?hhuo2W) Рассмотрены случайные динамические системы, возникающие при влиянии шума на параметры нелинейных систем. [[3]](https://www.zotero.org/google-docs/?iaoiYB) В заключение, представлена модель Маллинса-Секерки - нелокальная эволюционная модель для гиперповерхностей. Анализ основан на теории центрального многообразия и максимальной регулярности. Таким образом, центральные многообразия связываются с формализмом Маллинса-Секерки.[[4]](https://www.zotero.org/google-docs/?UrhhrJ) Изучение Center Manifold Theorem в 90-х годах пригодилось в кибербезопасности, где эта теорема используется для анализа и понимания поведения устойчивых точек.[[5]](https://www.zotero.org/google-docs/?ckQADK)

На данный момент количество вирусов и других вредоносных программ достигает 200 000 штук, большинство из них являются вариантами уже существующих программ. Также [Ö. A. Aslan и R. Samet](https://www.zotero.org/google-docs/?5iVi69) говорит о использовании проактивных детекторов для обнаружения вредоносных программ без обновления базы данных сигнатур [[2]](https://www.zotero.org/google-docs/?skGLEt). [D. Adjeroh, и S. S. Iyengar](https://www.zotero.org/google-docs/?5iVi69) описывают две методики обнаружения угроз компьютерных червей - на основе сигнатур и на основе аномалий.[[4](https://www.zotero.org/google-docs/?DyHOEg)] Также описывается как можно обнаружить распространяющийся компьютерный червь, исходя из его поведения без воздействия на виртуальные машины облака.[[6], [7], [8]](https://www.zotero.org/google-docs/?WhldOK). Таким образом, в источниках  [[9], [10], [11]](https://www.zotero.org/google-docs/?TrD7tP) представлены различные аспекты угроз компьютерных червей - их разнообразие, моделирование и методы предотвращения.

Главным недостатком антивирусов является их разнообразное количество, представляющих из себя слабый защитный софт, что для пользователя становится трудным в нахождении качественного ПО. В нашей статье мы предлагаем создать мощный, встроенный в операционные системы, антивирус. Убирающий необходимость в использовании сторонних, некачественных антивирусов.

References

[[1] J. Escher & G. Simonett, «A Center Manifold Analysis for the Mullins–Sekerka Model», *J. Differ. Equ.*, т. 143, by. 2, сс. 267–292, march. 1998, doi: 10.1006/jdeq.1997.3373.](https://www.zotero.org/google-docs/?5iVi69)

[[2] Ö. A. Aslan & R. Samet, «A Comprehensive Review on Malware Detection Approaches», *IEEE Access*, т. 8, сс. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.](https://www.zotero.org/google-docs/?5iVi69)

[[3] P. Boxler, «A stochastic version of center manifold theory», *Probab. Theory Relat. Fields*, т. 83, by. 4, сс. 509–545, dec. 1989, doi: 10.1007/BF01845701.](https://www.zotero.org/google-docs/?5iVi69)

[[4] Y. Ye, T. Li, D. Adjeroh, и S. S. Iyengar, «A Survey on Malware Detection Using Data Mining Techniques», *ACM Comput. Surv.*, т. 50, by. 3, с. 41:1-41:40, jun. 2017, doi: 10.1145/3073559.](https://www.zotero.org/google-docs/?5iVi69)

[[5] Z. Zhang & T. Zhao, «Bifurcation analysis of an e-SEIARS model with multiple delays for point-to-group worm propagation», *Adv. Differ. Equ.*, т. 2019, by. 1, с. 228, jun. 2019, doi: 10.1186/s13662-019-2164-7.](https://www.zotero.org/google-docs/?5iVi69)

[[6] A. Pratama & F. A. Rafrastara, «Computer Worm Classification», *Int. J. Comput. Sci. Inf. Secur.*, т. 10, сс. 21–24, april. 2012.](https://www.zotero.org/google-docs/?5iVi69)

[[7] S. Biedermann & S. Katzenbeisser, «Detecting Computer Worms in the Cloud», in *Open Problems in Network Security*, т. 7039, J. Camenisch & D. Kesdogan, red., in Lecture Notes in Computer Science, vol. 7039. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, сс. 43–54. doi: 10.1007/978-3-642-27585-2\_4.](https://www.zotero.org/google-docs/?5iVi69)

[[8] L.-P. Song, Z. Jin, G.-Q. Sun, J. Zhang, & X. Han, «Influence of removable devices on computer worms: Dynamic analysis and control strategies», *Comput. Math. Appl.*, т. 61, by. 7, сс. 1823–1829, april. 2011, doi: 10.1016/j.camwa.2011.02.010.](https://www.zotero.org/google-docs/?5iVi69)

[[9] B. Hassard & Y. H. Wan, «Bifurcation formulae derived from center manifold theory», *J. Math. Anal. Appl.*, т. 63, by. 1, сс. 297–312, march. 1978, doi: 10.1016/0022-247X(78)90120-8.](https://www.zotero.org/google-docs/?5iVi69)

[[10] A. Vanderbauwhede & S. A. Van Gils, «Center manifolds and contractions on a scale of Banach spaces», *J. Funct. Anal.*, т. 72, by. 2, сс. 209–224, jun. 1987, doi: 10.1016/0022-1236(87)90086-3.](https://www.zotero.org/google-docs/?5iVi69)

[[11] E. Gandotra, D. Bansal, & S. Sofat, «Malware Analysis and Classification: A Survey», *J. Inf. Secur.*, т. 2014, feb. 2014, doi: 10.4236/jis.2014.52006.](https://www.zotero.org/google-docs/?5iVi69)

[[12] J. Kinder, S. Katzenbeisser, C. Schallhart, & H. Veith, «Proactive Detection of Computer Worms Using Model Checking», *IEEE Trans. Dependable Secure Comput.*, т. 7, by. 4, сс. 424–438, oct. 2010, doi: 10.1109/TDSC.2008.74.](https://www.zotero.org/google-docs/?5iVi69)

[[13] D. Ucci, L. Aniello, & R. Baldoni, «Survey of machine learning techniques for malware analysis», *Comput. Secur.*, т. 81, сс. 123–147, march 2019, doi: 10.1016/j.cose.2018.11.001.](https://www.zotero.org/google-docs/?5iVi69)