ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ ОБНАРУЖЕНИЯ КИБЕРПРЕСТУПНОСТИ ПУТЕМ МОНИТОРИНГА И АНАЛИЗА ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Кодирова Севинч
магистрантка Ташкентского университета
информационных технологий имени Мухаммада аль-Хорезми

Аннотация:
Данное исследование посвящено анализу и оценке методов и средств обнаружения киберпреступности, основанных на мониторинге и анализе процессов в компьютерных сетях. С увеличением угроз кибербезопасности в современном мире необходимо разработать эффективные инструменты для выявления и противостояния киберпреступным активностям. Цель исследования состоит в оценке эффективности методов мониторинга и анализа процессов в компьютерных сетях для выявления киберпреступности, а также в разработке рекомендаций по оптимизации и улучшению существующих подходов.

Ключевые слова: Киберпреступность, Информационная безопасность, Мониторинг, Анализ процессов, Компьютерные сети, Кибератаки

Введение

Современное информационное общество сталкивается с постоянно увеличивающимися угрозами киберпреступности, которые оказывают серьезное влияние на стабильность и безопасность информационных систем. Киберпреступники все более совершенствуют свои методы атак, используя сложные технические средства для несанкционированного доступа к конфиденциальным данным, распространения вредоносных программ и дестабилизации инфраструктуры сети.

Цель данного исследования состоит в проведении анализа методов и средств обнаружения киберпреступности, основанных на мониторинге и анализе процессов в компьютерных сетях. Эффективное обнаружение киберугроз требует не только разработки новых технологий, но и совершенствования существующих методов, учета последних тенденций в развитии киберпреступности и адаптации к изменяющемуся ландшафту угроз.

Задачи исследования включают в себя:

Анализ методов мониторинга компьютерных сетей для выявления аномалий и потенциальных инцидентов кибербезопасности.

Исследование методов анализа процессов в компьютерных сетях с целью выявления характерных признаков киберпреступных действий.

Изучение интегрированных методов мониторинга и анализа для повышения эффективности обнаружения киберпреступности.

Оценка программных и аппаратных средств, используемых для обнаружения киберугроз, с выявлением их преимуществ и недостатков.

Основные аспекты киберпреступности

Основные аспекты киберпреступности

Определение киберпреступности

Киберпреступность представляет собой комплекс противоправных действий, совершаемых в информационной среде с использованием современных информационно-коммуникационных технологий. Она включает в себя различные виды преступлений, такие как кибератаки, кибершпионаж, мошенничество, распространение вредоносного программного обеспечения и другие. Киберпреступность наносит ущерб индивидуальным пользователям, компаниям, правительствам и обществу в целом.

Типы киберпреступности

Кибератаки Кибератаки включают в себя различные виды нападений на информационные системы, например, DDoS-атаки, атаки на веб-приложения, взломы, фишинг и другие. Они направлены на нарушение работы системы, кражу данных или даже уничтожение информации.

Кибершпионаж Кибершпионаж представляет собой противоправные действия, направленные на получение конфиденциальной информации, такой как государственные секреты, коммерческие тайны или личные данные. Этот вид киберпреступности часто ассоциируется с государственными акторами и киберразведкой.

Мошенничество Кибермошенничество включает в себя обман и мошеннические действия с использованием интернета. Это может включать финансовые мошенничества, аферы с банковскими картами, фальшивые лотереи, финансовые пирамиды и другие аферы.

Распространение вредоносного программного обеспечения Этот вид киберпреступности включает создание, распространение и запуск вредоносных программ, таких как вирусы, троянские кони, шпионское программное обеспечение и рекламное ПО. Они используются для несанкционированного доступа к системам, кражи данных и дестабилизации работы компьютерных сетей.

Последствия киберпреступности

Финансовые потери Киберпреступность приводит к огромным финансовым потерям для компаний и частных лиц. Это включает в себя потерю средств, кражу личных данных, расходы на восстановление систем и компенсации пострадавшим.

Угроза национальной безопасности Кибератаки и кибершпионаж могут представлять серьезную угрозу национальной безопасности государства, кражу государственных тайн, а также дестабилизировать работу критической инфраструктуры.

Ущемление личной конфиденциальности Киберпреступники могут получить доступ к личным данным, таким как социальные номера, финансовые данные, медицинская информация и другие, что приводит к ущемлению личной конфиденциальности и возможным последующим злоупотреблениям.

Заключение

В современном информационном обществе киберпреступность представляет серьезную угрозу для конфиденциальности, целостности и доступности информации. Ее разнообразие и сложность постоянно увеличиваются, требуя непрерывного развития и совершенствования методов и средств обнаружения и противодействия. Настоящее исследование было направлено на анализ основных аспектов киберпреступности и методов ее обнаружения через мониторинг и анализ процессов в компьютерных сетях.

В результате проведенного анализа были выделены основные типы киберпреступности, включая кибератаки, кибершпионаж, мошенничество и распространение вредоносного программного обеспечения. Каждый из этих видов киберпреступности представляет определенные угрозы для организаций, государства и отдельных граждан.

Также были рассмотрены основные последствия киберпреступности, включая финансовые потери, угрозу национальной безопасности и ущемление личной конфиденциальности. Эти последствия подчеркивают необходимость эффективного противодействия киберугрозам.

В рамках исследования были рассмотрены методы обнаружения киберпреступности через мониторинг и анализ процессов в компьютерных сетях. Особое внимание уделено интеграции методов мониторинга и анализа для повышения эффективности обнаружения киберпреступности. Программные и аппаратные средства также были рассмотрены в контексте обнаружения киберугроз.

Исследование демонстрирует, что обнаружение киберпреступности требует комплексного подхода, включающего в себя как технические методы, так и оценку организационных и человеческих аспектов. Стремительное развитие технологий требует постоянного обновления и совершенствования методов борьбы с киберпреступностью.

Литература

1. Anderson, R., & Moore, T. (2009). Information security economics: The economics of information security and privacy. Springer.
2. Dhillon, G., & Moores, T. T. (2001). Internet banking risks: The information security aspect. Information Management & Computer Security, 9(1), 24-31.
3. Goodrich, M. T., & Tamassia, R. (2011). Introduction to computer security. Pearson Education.
4. Rouse, M. (2018). What is cybercrime? - Definition from WhatIs.com. Retrieved from https://whatis.techtarget.com/definition/cybercrime

5. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
6. Whitman, M. E., & Mattord, H. J. (2019). Principles of information security. Cengage Learning.
7. Zeadally, S., & Baig, Z. (2017). Cybercrime and Cybersecurity in the Global South. Springer.
8. Zhang, X., Sharif, H., Lee, W., Liao, Q., & Wang, X. (2011). Cybercasing the joint: On the risk of publishing location traces. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 639-650).