ПРИМЕНЕНИЕ МЕТОДОВ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ В КИБЕРБЕЗОПАСНОСТИ

Тургунов Нозимжон Абдуманнопович
Доктор физико-математических наук, доцент, Академия Министерства внутренних дел Республики Узбекистан, Ташкент
Курбонова Фируза Зариповна
Доктор философии по техническим наукам, доцент, Академия Министерства внутренних дел Республики Узбекистан, Ташкент
Каримов Дилшод Исматович
Преподаватель кафедры точных наук Академия Министерства внутренних дел Республики Узбекистан, Ташкент

https://doi.org/10.5281/zenodo.22846200

Аннотация. Активное развитие цифровых технологий и информационной инфраструктуры сопровождается увеличением числа киберугроз, что повышает актуальность применения математических методов их анализа и прогнозирования. В работе рассмотрены возможности математического моделирования при оценке киберрисков, исследовании компьютерных сетей, прогнозировании кибератак и выборе рациональных способов защиты информации. Проанализировано применение теории вероятностей, математической статистики, теории графов, методов оптимизации и теории игр, а также их интеграция с технологиями искусственного интеллекта и машинного обучения. Сделан вывод о высокой эффективности математического моделирования при решении современных задач кибербезопасности.

Ключевые слова: кибербезопасность, математическое моделирование, информационная безопасность, теория вероятностей, теория графов, теория игр, искусственный интеллект, машинное обучение, оценка рисков.

1. Введение

Цифровизация государственного управления, экономики и других сфер сопровождается увеличением количества киберугроз, включая несанкционированный доступ к данным, распространение вредоносного программного обеспечения, DDoS-атаки и фишинговые кампании. В этих условиях возрастает потребность в методах, позволяющих оценивать

киберриски, прогнозировать развитие атак и обосновывать выбор средств защиты.

Математическое моделирование является эффективным инструментом обеспечения кибербезопасности. Оно используется для анализа информационных систем, исследования кибератак и оценки эффективности средств защиты. Интеграция с технологиями искусственного интеллекта и машинного обучения повышает точность прогнозирования и принятия решений.

Цель исследования — проанализировать возможности применения методов математического моделирования в кибербезопасности, рассмотреть наиболее распространённые модели оценки угроз и рисков, а также определить перспективы их дальнейшего развития.

2. Теоретические основы математического моделирования

Математическое моделирование является одним из основных методов научного исследования, позволяющим описывать реальные процессы с помощью математических моделей, анализировать функционирование информационных систем, прогнозировать развитие киберугроз и оценивать последствия возможных атак. Его применение обеспечивает проведение вычислительных экспериментов, исследование устойчивости информационной инфраструктуры и количественную оценку киберрисков без воздействия на реальные объекты [1,2,3].

При построении моделей применяются теория вероятностей, математическая статистика, теория графов, теория игр, методы оптимизации, теория принятия решений и стохастические процессы [4,7]. Эффективность модели определяется её соответствием исследуемому объекту и корректностью выбранных методов анализа [3,5].

Развитие математического моделирования связано с использованием технологий искусственного интеллекта и машинного обучения, которые позволяют обрабатывать большие объёмы данных, выявлять аномалии и прогнозировать новые киберугрозы [7,8]. Интеграция математических и интеллектуальных методов расширяет возможности современных систем кибербезопасности [6,9].

3. Математические модели, применяемые в системах кибербезопасности

Современная кибербезопасность требует применения математических методов, позволяющих исследовать киберугрозы, прогнозировать возможные атаки и разрабатывать эффективные механизмы защиты информационных систем. Для решения этих задач используются графовые модели, вероятностно-статистические методы, марковские процессы, теория игр и методы математической оптимизации.

3.1. Графовые модели анализа компьютерных сетей

Теория графов является одним из основных математических методов исследования структуры компьютерных сетей. В графовой модели устройства сети представляются вершинами, а каналы передачи данных — рёбрами, что позволяет анализировать топологию, связность и устойчивость информационной инфраструктуры [2,5].

Графовые модели широко применяются при исследовании распространения кибератак. Они позволяют выявлять уязвимые участки сети, прогнозировать возможные маршруты распространения вредоносного программного обеспечения и определять критически важные узлы с использованием показателей центральности (Degree, Betweenness и Closeness Centrality) [5,8].

3.2. Вероятностно-статистические модели

Высокая неопределённость процессов возникновения киберугроз обусловливает применение методов теории вероятностей и математической статистики. Эти методы используются для оценки вероятности реализации кибератак, анализа статистических закономерностей функционирования информационных систем и прогнозирования потенциальных угроз [1,6].

Вероятностные модели применяются при разработке систем обнаружения вторжений (Intrusion Detection Systems, IDS), оценке киберрисков и анализе компьютерных инцидентов. На основе статистических данных формируются модели нормального поведения пользователей и сетевых устройств, а отклонения от них рассматриваются как признаки возможной несанкционированной активности [7,8].

Использование методов математической статистики повышает точность классификации инцидентов, снижает число ложных срабатываний и обеспечивает более объективную оценку защищённости информационных систем.

3.3. Современные математические модели в кибербезопасности

В кибербезопасности математические модели применяются для анализа киберугроз, прогнозирования атак и выбора эффективных способов защиты. Марковские модели используются для оценки киберинцидентов, а теория игр — для разработки стратегий противодействия и управления киберрисками.

Методы математической оптимизации применяются для рационального распределения ресурсов и выбора эффективных средств защиты с использованием линейного и динамического программирования, генетических алгоритмов и многокритериальной оптимизации [3,4,6,9].

Современное развитие математического моделирования связано с интеграцией технологий искусственного интеллекта и машинного обучения. Использование нейронных сетей, методов глубокого обучения и интеллектуального анализа данных повышает эффективность обнаружения новых видов атак, анализа больших объёмов информации и прогнозирования киберугроз [6,9]. Комплексное применение перечисленных методов способствует повышению устойчивости информационных систем и эффективности обеспечения кибербезопасности [2,4,6].

4. Практическое применение математического моделирования в кибербезопасности

Методы математического моделирования применяются в кибербезопасности для анализа информационных систем, оценки киберрисков, прогнозирования атак и выбора средств защиты. В системах IDS/IPS они совместно с методами статистического анализа и алгоритмами машинного обучения используются для выявления аномальной активности и обнаружения кибератак [1,3,8,9].

Математическое моделирование также применяется при количественной оценке киберрисков, прогнозировании развития компьютерных инцидентов и исследовании поведения нарушителей. Использование марковских моделей, временных рядов и технологий искусственного интеллекта способствует повышению точности прогнозирования и эффективности принятия решений [8,9].

Методы математической оптимизации обеспечивают рациональное распределение ресурсов и выбор эффективных средств защиты. Интеграция математических моделей с технологиями искусственного интеллекта повышает эффективность современных систем кибербезопасности [2,4,6,9].

5. Современные тенденции развития математического моделирования в кибербезопасности

Развитие киберугроз требует совершенствования методов математического моделирования. Современные исследования направлены на интеграцию математических моделей с технологиями искусственного интеллекта, машинного обучения и анализа больших данных, что повышает точность обнаружения угроз и прогнозирования кибератак [6,9].

Перспективными направлениями являются применение технологии Digital Twin для моделирования информационной инфраструктуры, использование концепции Zero Trust Architecture при оценке уровня доверия пользователей и устройств, а также внедрение методов Deep Learning и Big Data Analytics для анализа сетевого трафика и выявления аномальной активности [6,9].

Заключение

Проведённое исследование подтвердило, что математическое моделирование занимает важное место в обеспечении кибербезопасности. Использование графовых моделей, вероятностных методов, марковских процессов, теории игр и методов оптимизации позволяет анализировать угрозы, оценивать уровень риска и выбирать наиболее эффективные способы защиты информационных систем. Современное развитие данного направления связано с объединением математических моделей и технологий искусственного интеллекта, что повышает качество обнаружения и прогнозирования кибератак. Дальнейшие исследования целесообразно направить на разработку интеллектуальных моделей, цифровых двойников и новых методов оптимизации, способных повысить устойчивость информационных систем к современным угрозам.

REFERENCES:

1. Абдукодиров А.А. Основы информационной безопасности. – Ташкент: Fan va texnologiyalar, 2020. – 256 с.

2. Йулдашев Б.Б. Кибербезопасность и защита информации. – Ташкент: O‘zbekiston, 2021. – 312 с.

3. Каримов С.С. Основы математического моделирования. – Ташкент: Университет, 2019. – 284 с.

4. Alpcan T., Başar T. Network Security: A Decision and Game-Theoretic

Approach. Cambridge University Press, 2011. – 404 p.

5. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Edition. Pearson, 2023. – 864 p.

6. Bishop M. Computer Security: Art and Science. 2nd Edition. Addison-Wesley, 2019. – 1184 p.

7. Manshaei M.H., Zhu Q., Alpcan T., Başar T., Hubaux J.-P. Game Theory Meets Network Security and Privacy // *ACM Computing Surveys*. – 2013. – Vol. 45(3). – Article 25.

8. Wang P., Lu Z. Game-Theoretic Cyber Attack Modeling for Network Security // *Computers & Electrical Engineering*. – 2020. – Vol. 87. – Article 106785.

9. Gençoğlu M.T., Koçak T. Mathematical Modeling of Cyber Attacks Using Artificial Intelligence Techniques // *IEEE Access*. – 2022. – Vol. 10. – P. 86541–86558.