Литература:

1. *Дранко О.И., Новиков Д.А., Райков А.Н., Чернов И.В.* Управление развитием региона. Моделирование возможностей. – М.: URSS, ООО «ЛЕНАНД», 2023. – 432 с.

2. *Рисин И.Е., Трещевский Ю.И.* Региональное управление и территориальное планирование. – М.: Издательство «КноРус», 2020. – 270 с.

3. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». – URL: https://base.garant.ru/401425792/ (дата обращения 17.09.2024).

4. Федеральный закон «О безопасности» от 28.12.2010 N 390-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения 17.09.2024).

5. Федеральный закон «О федеральной службе безопасности» от 03.04.1995 N 40-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_6300/ (дата обращения 17.09.2024).

6. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Управление региональной безопасностью на основе сценарного подхода. – М.: ИПУ РАН, 2014. – 163 с.

Ермолаев Е.Д., Феоктистов С.В.

Применимость методов сценарного анализа в сфере информационной безопасности РФ

Аннотация: Технологический прогресс неизбежно влечет за собой появление новых угроз в области информационной безопасности. В данной работе проведен всесторонний анализ актуальности проблемы, что позволило выявить ключевые задачи, стоящие перед государством, и определить факторы, влияющие на информационную безопасность. На основе этих факторов была построена матрица смежности и создана имитационная сценарная модель. Разработки предоставляют исследователям ценные инструменты для

развития эффективных стратегий обеспечения информационной безопасности, которая является критически важной частью национальной безопасности РФ.

Ключевые слова: информационная безопасность, технологический прогресс, имитационное моделирование, сценарный анализ, национальная безопасность

Введение

Современное государство сталкивается с растущими угрозами в сфере информационной безопасности, которые могут иметь серьезные последствия для его стабильности, экономики, обороноспособности и даже национальной безопасности в целом. В этом контексте обеспечение информационной безопасности становится приоритетной задачей для государственных органов и учреждений.

Примером негативных последствий недостаточной информационной безопасности может служить кибератака на государственные институты. В 2017 году Украина столкнулась с кибератакой, известной как "Petya" или "NotPetya", которая серьезно повредила информационные системы многих государственных учреждений, банков и крупных корпораций. Эта атака привела к значительным экономическим потерям и нарушению работы государственных служб.

Актуальность

В качестве примера, в статье [1] авторы поднимают важную проблему информационной безопасности, связанную с использованием криптовалюты. Они указывают на потенциальное влияние криптовалюты на уровень преступности и, следовательно, на социальную безопасность общества. Предполагается, что изменение сферы экономики и финансовых операций через использование криптовалюты может вызвать соответствующую трансформацию правоохранительной системы.

В научной работе [2] авторы подчеркивают важность повышения эффективности управления обеспечением социальной стабильности в России в условиях современной глобализации и развития информационного общества. Они указывают на то, что даже небольшое информационное воздействие может привести к

социальным потрясениям. В такой ситуации методология сценарного анализа становится критически важной, позволяя анализировать различные альтернативные развития событий в условиях неопределенности.

Сценарный подход особенно полезен, когда невозможно создать детальный план мероприятий по обеспечению социальной стабильности из-за ограничений времени. Он обеспечивает информационную поддержку для планирования и реализации мер по противодействию дестабилизирующим угрозам, позволяя анализировать динамику социально-экономических систем и изучать слабоструктурированные проблемы.

В процессе решения подобных задач используется множество параметров и показателей, которые после анализа позволяют оценить уровень социальной напряженности и прогнозировать негативные явления. Однако точные методы решения этих задач сталкиваются с трудностями из-за необходимости обобщения множества данных и сложных процедур анализа.

Сценарный анализ, опирающийся на имитационные модели и аппарат знаковых орграфов, позволяет использовать различные типы данных и решать задачи в условиях неполной информации. Он помогает оценить уязвимость социально-экономических систем, провести анализ текущей ситуации, сформировать прогнозы развития и оценить эффективность управленческих решений в условиях неопределенности.

В монографии [3] были успешно исследованы методологические и практические аспекты повышения уровня безопасности на региональном уровне. Авторы провели анализ основных угроз, стоящих перед региональным развитием, а также рассмотрели особенности процессов управления региональной безопасностью. Особое внимание в докладе уделено сценарному анализу как инструменту для управления социально-экономическим развитием региона и обеспечения его защиты от внешних и внутренних раздражителей.

В работе представлены результаты сценарного исследования, основанные на разработанных мультиграфовых моделях управления региональной безопасностью. Использование сценарного анализа позволило авторам оценить вероятные

последствия различных сценариев развития ситуации и выработать стратегии предотвращения потенциальных угроз.

Все это говорит о незаменимости применения такого инструмента, как сценарный анализ в контексте попытки обеспечить информационную безопасность государства посредством разработки превентивных мер взаимодействия с предполагаемыми опасностями.

В том числе, по мнению авторов, развитие исследований в этой области позволит эффективнее планировать и реализовывать государственную политику России в Арктике. В статье [4] подчеркивается, что для успешного урегулирования конфликтов в арктическом регионе необходимо использовать современные методы информационного управления и сценарный анализ. Эти инструменты позволяют анализировать возможные сценарии развития ситуации и делать прогнозы поведения объектов, что помогает принимать более обоснованные управленческие решения. А в научной работе [5] сценарный анализ помогает авторам в анализе основных групп рисков, угроз и структурных уязвимостей объектов уже инфраструктуры железнодорожного транспорта.

Моделирование

В работах [6-7] представлена подробная постановка модели, выделены факторы, модель приведена к аналитическому базису (построена Жорданова форма матрицы смежности). В данной работе авторы продолжают исследование, заложенное ранее. Одним из результатов [6-7] являлось выделение базисных сценариев развития системы информационной безопасности РФ. Для рассматриваемой модели было обнаружено 5 таких сценариев.

Далее приведен эксперимент, показывающий возможности использования выбранного метода в контексте моделирования возникающих угроз информационной безопасности.

Факторы модели, используемые в машинном аппарате:

1) утечка частной информации,
2) кибератаки заграничные,
3) кибератаки внутренние,
4) интернет,
5) технологическая разведка,
6) жалобы,

7) военная утечка,
8) блокировки,
9) внедрение инноваций,
10) отечественное ПО,
11) международные соглашения,
12) освещение СМИ,
13) взаимодействие отраслей.

Ряд единовременных координированных вражеских кибератак может иметь различные последствия для России. Атаки на критически важные инфраструктурные объекты, такие как энергетические сети, транспортные системы или финансовые учреждения, могут привести к их временной неработоспособности, вызвав серьезные нарушения в экономике и обществе. Возможны также атаки на государственные информационные системы, что может привести к утечке чувствительной информации или нарушению деятельности государственных органов. Например, в 2007 году кибератаки на компьютерные системы Эстонии, которые пришлись на период массовых протестов, привели к тому, что государство, по сути, оказалось парализовано.

В рамках имитационного моделирования в первую очередь решается задача наблюдения (задача прогнозного мониторинга) в сценарии, при котором единовременно производятся кибератаки как изнутри, так и извне России. Каждый такт моделирования в систему подаются единичные импульсы I0 в вершины 2 и 3. Результат моделирования первых 10 тактов можно наблюдать на рисунке 1.

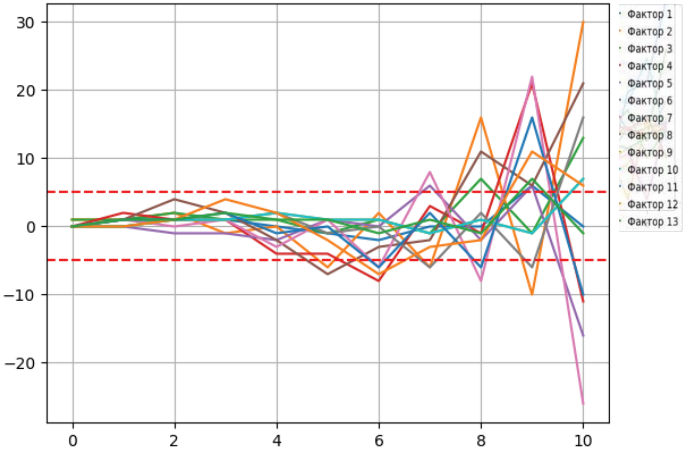

Рисунок 1 – Моделирование 10 тактов сценария «Кибератаки»

Как видно, после 4 такта система приходит в резонанс и теряет устойчивость, при этом потеря устойчивости происходит после отклонения значений факторов более, чем на 5 единиц от базового значения, что отмечено на рисунке красной пунктирной линией. В дальнейшем система так же продолжает терять стабильность, что можно увидеть на рисунке 2.

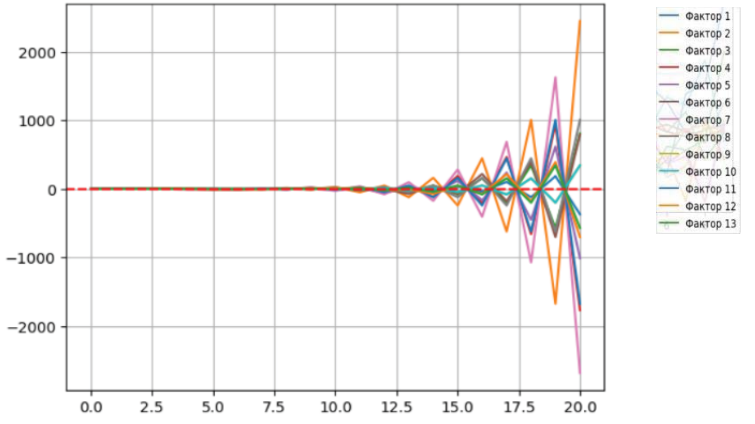

Рисунок 2 – Потеря стабильности системы

Как видно, результат прогноза развития системы при активации сценария «Кибератаки» – деструктивное воздействие приводит к выходу системы из строя и потери ей стабильности. Потеря устойчивости системы происходит на 4 такте моделирования.

Заключение

Разработанная сценарная имитационная модель в совокупности с возможностью её применения на практике обладает потенциалом для использования в будущих исследованиях, направленных на обеспечение информационной безопасности. Учитывая текущие тенденции технологического развития, данная модель представляет собой важный инструмент для анализа и повышения уровня защищенности информационных систем. Это позволит своевременно реагировать на возникающие угрозы и обеспечивать устойчивое развитие информационной инфраструктуры страны.

Литература:

1. *Тимошенко А.А., Фейзов В.Р., Чернов И.В.* Сценарный подход к исследованию направлений регулирования сферы криптовалют в Российской Федерации // Российский журнал правовых исследований. – 2023. – Т. 10, № 2 – С. 20-30.

2. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Информационное управление обеспечением социальной стабильности как основы общественного и государственного развития. – М.: ИПУ РАН, 2019. – 211 с.

3. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Управление региональной безопасностью на основе сценарного подхода. – М.: ИПУ РАН, 2014. – 163 с.

4. *Кульба В.В., Шульц В.Л., Шелков А.Б., Чернов И.В.* Сценарный анализ в управлении информационной поддержкой процессов предупреждения и урегулирования конфликтных ситуаций в Арктике // Национальная безопасность/Nota bene. – 2013. – № 1. – С. 62-152. – URL: http://e-notabene.ru/nb/article_301.html (дата обращения 10.10.2024).

5. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Методология управления техногенной безопасностью объектов инфраструктуры железнодорожного транспорта на основе индикаторного подхода // Тренды и управление. – 2013. – № 3 – С. 4-23.

6. *Феоктистов С.В., Ермолаев Е.Д.* Факторы, влияющие на информационную безопасность Российской Федерации, как основа для сценарного моделирования / Проблемы управления безопасностью сложных систем: материалы XXXI Международной научной конференции (ПУБСС'2023, Москва). – М.: ИПУ РАН, 2023. – С. 160-166.

7. *Чернов И.В., Ермолаев Е.Д., Феоктистов С.В.* Выделение базисных режимов динамики факторов, влияющих на информационную безопасность Российской Федерации / Проблемы управления безопасностью сложных систем: материалы XXXI Международной научной конференции (ПУБСС'2023, Москва). – М.: ИПУ РАН, 2023. – С. 166-173.

Plotnikov N.I.

Principal components soft computing in strategic management

Abstract: A new approach to strategic management is proposed, based on qualitative methods of surveying an organization using the method of soft computing. There are many examples of assessing risk states of an organization. A comparison of traditional analysis and business planning, empirical models and the method of the analysis of principal components of business activity is shown. The advantage of assessing by groups of indicators is the simplicity of identifying the states of individual resources of the organization. The application of the calculation method allows the use of a minimum indicators in the analysis of the organizational activity. The new approach enables qualitative diagnostics, risk assessment and strategic decision making.

Keywords: strategic management, soft computing, risk estimation, efficiency, safety, principal components

Introduction

Well-known modern theories and methods of strategic management contain diagnostics of the state of organizations, analysis, development of guidelines, planning for the implementation of the goal. A new