оригинальная статья

https://elibrary.ru/bzpjan

# Когнитивные рефреймингн в предвидении и предотвращении мультиплексных угроз критической инфраструктуре

**Панилов Павел Алексеевич**

Московский государственный технический университет им. Н. Э. Баумана, Россия, Москва

eLibrary Author SPIN: 4112-3750

https://orcid.org/0009-0005-7663-5576

Scopus Author ID: 58882092200

panilovp.a@bmstu.ru

**Аннотация:** Статья представляет новый подход к предвидению и предотвращению мультиплексных угроз критической инфраструктуре с использованием когнитивных рефреймингов. В контексте постоянно эволюционирующих угроз разработанная модель ставит своей целью повышение эффективности стратегий предотвращения инцидентов. Цель – предложить графовую модель, где узлы представляют концепции когнитивных рефреймингов, а ребра – связи между ними. Модель включает веса, учитывающие важность каждой концепции, а также дополнительные метрики важности, коэффициенты и взаимодействия. Вычисления весов ребер позволили сформировать граф, отражающий взаимосвязи между концепциями. Представлены сценарии использования модели, подчеркивается ее применимость для улучшения кибербезопасности, реагирования на природные катастрофы и обеспечения бесперебойной работы систем. Модель учитывает динамические факторы, множественные метрики важности, взаимодействия и статистические методы, что делает ее гибкой и адаптивной. Обсуждение включает в себя аспекты усложнения модели, учитывающие дополнительные факторы для повышения точности и адаптивности. Отмечены перспективы применения когнитивных рефреймингов в области критической инфраструктуры. В результате разработанная модель представляет собой новый инструмент для эффективного управления угрозами.

**Ключевые слова:** когнитивные рефрейминги, критическая инфраструктура, безопасность, угрозы, модель вычисления весов, предотвращение угроз, кибербезопасность, бесперебойная работа систем, управление критической инфраструктурой

**Цитирование:** Панилов П. А. Когнитивные рефрейминги в предвидении и предотвращении мультиплексных угроз критической инфраструктуре. *Виртуальная коммуникация и социальные сети.* 2024. Т. 3. № 4. С. 316–325. https://doi.org/10.21603/2782-4799-2024-3-4-316-325

Поступила в редакцию 23.06.2024. Принята после рецензирования 24.09.2024. Принята в печать 30.09.2024.

full article

# Cognitive Reframing in Anticipation and Prevention of Multiplex Threats to Critical Infrastructure

**Pavel A. Panilov**

Bauman Moscow State Technical University, Russian, Moscow

eLibrary Author SPIN: 4112-3750

https://orcid.org/0009-0005-7663-5576

Scopus Author ID: 58882092200

panilovp.a@bmstu.ru

**Abstract:** The article introduces a new cognitive reframing approach to anticipating and preventing multiplex threats to critical infrastructure. In the context of constantly evolving threats, the model may increase the effectiveness of incident prevention strategies. It is visualized as a graph with nodes for concepts of cognitive reframing and edges for the connections between them. The model includes weight values that depend on the importance of each concept,

as well as additional importance metrics, coefficients, and interactions. By calculating the edge weights, the authors developed a graph that illustrates the interrelationships between the concepts. The model can be applied to various scenarios as it improves cybersecurity, responds to natural disasters, and ensures the smooth operation of various systems. The model takes into account dynamic factors, multiple importance metrics, interactions, and statistical methods, which makes it flexible and adaptive. Extra factors could increase the complexity, accuracy, and adaptability of the current model. Cognitive reframing has good prospects in the field of critical infrastructure while the new model proves to be an effective threat management tool.

**Keywords:** cognitive reframing, critical infrastructure, security, threats, weight calculation model, threat prevention, cybersecurity, smooth operation of systems, critical infrastructure management

**Citation:** Panilov P. A. Cognitive Reframing in Anticipation and Prevention of Multiplex Threats to Critical Infrastructure. *Virtual Communication and Social Networks*, 2024, 3(4): 316–325. (In Russ.) https://doi.org/10.21603/2782-4799-2024-3-4-316-325

Received 23 Jun 2024. Accepted after review 24 Sep 2024. Accepted for publication 30 Sep 2024.

## Введение

Критическая инфраструктура в настоящее время чрезвычайно важна. Речь идет об энергосистемах, водоснабжении, транспорте и коммуникациях. Они помогают поддерживать стабильность общества и его безопасность [Панилов, Кокорев 2024: 236; Цибизова и др. 2023: 36; Panilov et al. 2024: 280]. Данные системы все время подвергаются различным угрозам. Это природные катастрофы и кибератаки. Эти угрозы постоянно усложняются и становятся более разнообразными. Возникает необходимость искать методы, которые позволят их предвидеть и предотвратить. Только в этом случае критическая инфраструктура будет устойчивой и надежной.

Стандартные методы защиты критической инфраструктуры часто сталкиваются с проблемой недостаточной эффективности из-за сложности и многокомпонентности возникающих угроз. Стандартные подходы включают в себя такие методы, как:

- Антивирусное программное обеспечение и системы обнаружения вторжений (IDS) – эти системы помогают выявлять и устранять вредоносное программное обеспечение и подозрительную активность в сети. Однако они могут быть ограничены в своей способности обнаруживать новые, еще не зарегистрированные угрозы.
- Фаерволы и сетевые фильтры – предназначены для контроля и фильтрации сетевого трафика, предотвращая несанкционированный доступ. Несмотря на свою важность, фаерволы могут быть обойдены с использованием сложных атак, таких как обход аутентификации.
- Шифрование данных – применяется для защиты информации от несанкционированного доступа. Тем не менее если ключи шифрования будут скомпрометированы, весь механизм защиты может оказаться под угрозой.
- Регулярное обновление программного обеспечения и патчи – важный аспект защиты, который позволяет устранять уязвимости, обнаруженные в программном обеспечении. Однако этот метод требует постоянного мониторинга и может не успевать за всеми новыми угрозами.

Эти традиционные методы часто оказываются недостаточными, поскольку кибератаки могут быть частью более сложных стратегий, которые включают как цифровые, так и физические компоненты. Например, атака на электросети может сочетать в себе как кибернетическое вмешательство, так и физическое проникновение в ключевые объекты инфраструктуры.

В связи с этим возникает необходимость в новых подходах к управлению рисками. Когнитивный рефрейминг, который изначально разработан в психологии [Chen et al. 2019: 158; Wang et al. 2021: 1785], представляет собой один из таких современных методов. Этот подход дает возможность переосмыслять угрозы, находить новые решения и адаптировать существующие стратегии. Когнитивный рефрейминг помогает взглянуть на проблемы под новым углом, что особенно важно в условиях неопределенности и динамичных изменений в угрозах.

Применение когнитивного рефрейминга в управлении рисками критической инфраструктуры способствует более глубокому пониманию мультикомплексных угроз и разработке эффективных стратегий реагирования. Этот метод позволяет не только

формулировать новые стратегии защиты, но и улучшать взаимодействие между различными заинтересованными сторонами [Казьмина и др. 2023: 42; Карташев, Красовский 2016: 43; Панилов и др. 2023: 50; Трофимов, Саакян 2023: 3339]. Анализ применения когнитивного рефрейминга в этой области поможет выявить его потенциал в предотвращении угроз и предложит рекомендации по его использованию в управлении рисками.

Когнитивный рефрейминг – концепт психологического уровня, который сегодня успешно применяется в разных сферах: в менеджменте, психотерапии, обеспечении необходимой безопасности инфраструктуры и принятии необходимых решений. Данный подход позволяет менять восприятие сложившейся ситуации [Брумштейн и др. 2020: 338; Пролетарский и др. 2017: 69–72]. Он оказывает влияние на применяемые решения и выполняемые действия.

Очень важно обезопасить критическую инфраструктуру. Когнитивный рефрейминг является действенным инструментом, позволяющим анализировать угрозы и существующие сценарии имеющихся рисков [Губанов, Закиров 2015: 35–37]. Этот подход дает возможность выявить свойства угроз, заняться поиском решений или правильно применять имеющиеся стратегии. Есть возможность использовать когнитивные рефреймминги в том случае, если существует нераспределенность или появляются новые угрозы, такие как цепочки событий комплексного характера [Курманбай, Нозирзода 2016: 177].

Для того чтобы использовать когнитивный рефрейминг в кибербезопасности, нужно расширить анализ и в обязательном порядке рассмотреть вероятные сценарии атак. Пример: злоумышленники вполне могут оказаться на объектах критической инфраструктуры: на электростанциях или трансформаторных подстанциях. Обозначенный подход дает возможность обнаружить существующие уязвимости, незамеченные при использовании обычных способов анализа существующих угроз.

Когнитивный рефрейминг дает возможность изучить мотивы злоумышленников. Цели кибератак обычно финансовые: вымогательство или кража данных. При расширенном подходе принимаются во внимание иные мотивы: терроризм или саботаж. Кибератаки рассматриваются не отдельно, а как часть стратегий, которые были тщательно спланированы. В этом случае нужно применять меры безопасности комплексного характера.

Также оцениваются последствия атаки, которая была успешной. Если в электроснабжении возникает сбой, возникают проблемы каскадного характера. Они затрагивают транспорт, водоснабжение, здравоохранение и связь [Валеев, Орлов 2018: 19–20].

Рассмотрим способы применения когнитивного рефрейминга для безопасности инфраструктуры:

- **Учет человеческих факторов**

При традиционных подходах к безопасности учитываются технические аспекты угроз. Это взломы и кибератаки. Когнитивный рефрейминг дает возможность принимать во внимание риски, в основе которых лежат человеческие факторы [Громов и др. 2015]. Операторы могут ошибиться, в процедурах существуют уязвимости – все это чревато рисками. Но классические методы обеспечения безопасности вполне могут их не увидеть. Когнитивный рефрейминг дает возможность выявлять данные уязвимости потенциального характера и создавать стратегии, которые помогут их устранить.

- **Понимание сложных цепочек событий**

Когнитивный рефрейминг можно использовать также для того, чтобы понимать взаимосвязи между разными элементами инфраструктуры [Лаптев и др. 2011]. Аналитики изучают влияние одного события на другие. Создается цепная реакция. Это приводит к сбоям в разных системах. Например, если в электросети произошел сбой, это влияет на телекоммуникации или транспорт, что вызывает сбои более масштабного характера. Данное понимание дает возможность создавать стратегии, учитывающие цепочки происходящего. Обеспечивается необходимая устойчивость, которая очень важна, особенно в том случае, если инциденты достаточно крупные.

- **Использование исторических данных**

Когнитивный рефрейминг также включает анализ событий, которые уже произошли. Аналитики пересматривают произошедшие инциденты. Они стремятся понять, могут ли в будущем возникнуть похожие ситуации. Указанный подход позволяет выявлять шаблоны, которые при обычном анализе неочевидны. Предлагаются новые способы, которые позволяют предотвратить возможность повторения таких инцидентов.

- **Учет физической безопасности**

Когнитивный рефрейминг дает возможность изучать связи между физическим доступом к объектам и кибератаками. Злоумышленники могут задействовать уязвимости для получения доступа к системам.



 https://doi.org/10.21603/2782-4799-2024-3-4-316-325

После этого они предпринимают кибератаку. Разрабатываются комплексные меры безопасности, объединяющие физические и технические элементы. Обеспечивается оптимальная защита критической инфраструктуры.

- **Междисциплинарный подход**

Когнитивный рефрейминг позволяет укреплять сотрудничество между госструктурами и организациями. Угрозы анализируются не отдельно. Рефрейминг дает возможность изучать их с разных сторон. Идет эффективный обмен существующей информацией. Действия становятся скоординированными. Такой подход делает меры безопасности более эффективными. Дело в том, что на угрозы очень быстро реагируют. Привлекаются различные ресурсы и экспертизы.

## Методы и материалы

В рамках настоящего исследования методология когнитивного рефрейминга направлена на автоматизированный анализ и адаптацию подходов к защите критической инфраструктуры без привлечения внешней экспертной группы. Этот процесс основан на систематическом сборе данных, их обработке и выявлении новых способов предвидения и предотвращения угроз.

***Сбор информации***. Ключевым этапом является сбор данных из различных источников, таких как мониторинг инфраструктурных систем, анализ инцидентов, а также регистрация аномальных событий. Сбор данных производится с использованием:

- SCADA-системы (Wonderware InTouch) широко применяются для мониторинга и управления промышленными объектами, включая энергосети, транспортные и водоснабжающие инфраструктуры. Эти системы фиксируют состояние ключевых компонентов и регистрируют любые отклонения, позволяя своевременно выявлять угрозы.
- Системы мониторинга сетевой безопасности (Snort) используются для обнаружения вторжений в сети и анализа сетевого трафика. Snort анализирует данные в реальном времени, выявляя аномалии и указывая на возможные кибератаки, что позволяет вовремя реагировать на сетевые угрозы.
- Системы управления журналами событий (Splunk) собирают и анализируют логи серверов, приложений и сетевых устройств. Splunk позволяет обнаруживать подозрительные активности и выявлять системные сбои или попытки несанкционированного доступа, что обеспечивает повышенную безопасность инфраструктуры.

***Анализ данных и идентификация угроз***. После сбора данные обрабатываются с применением методов статистического анализа и машинного обучения. Этот этап позволяет выявить скрытые зависимости и аномалии, которые могут привести к потенциальным угрозам. Особенностью этого подхода является использование когнитивного рефрейминга, который перекомпонует информацию, предлагая новые перспективы для анализа и устранения уязвимостей.

***Графовая модель***. Центральным элементом методологии выступает построение графовой модели, где узлы графа представляют ключевые концепции, такие как восприятие, интерпретация, принятие решений и действия. Ребра графа символизируют связи и взаимодействия между этими концепциями. При этом каждому узлу присваивается определенный вес, отражающий его значимость в процессе обеспечения безопасности, а веса ребер показывают силу взаимодействия между концепциями.

***Расчет весов***. Для того чтобы объективно оценить важность каждой концепции и взаимодействия между ними, используются метрики, которые основаны на частоте инцидентов, уровне риска и вероятности повторных угроз. Веса концепций и связей рассчитываются исходя из динамики изменений системы и позволяют гибко адаптировать меры безопасности в зависимости от ситуации.

***Адаптация модели и переоценка весов.*** Важным аспектом подхода является его способность к адаптации: по мере поступления новых данных и появления угроз, которые не были учтены ранее, веса узлов и ребер могут быть скорректированы. Это позволяет обновлять модель в реальном времени и повышать ее точность при прогнозировании и предотвращении угроз.

Для иллюстрации процесса когнитивных рефреймингов можно использовать граф (рис. 1), который демонстрирует переход от традиционных методов анализа угроз к более гибким и комплексным подходам. Такой граф наглядно показывает, как когнитивные рефрейминги позволяют преобразовать восприятие угроз и стимулировать новые идеи для повышения безопасности [Лавриненко, Гончаренко 2016: 66–70; Скрыпников и др. 2015: 69–72].


**Рис. 1. Граф когнитивных рефреймингов**
**Fig. 1. Cognitive reframing: graph scheme**

Опишем подробнее этот граф.

Узлы (концепции):

- *Когнитивные рефреймингги*: этот узел представляет понятие когнитивных рефреймингов как общей концепции.
- *Изменение восприятия*: этот узел представляет идею изменения способа восприятия информации.
- *Интерпретация*: этот узел представляет этап интерпретации, где происходит анализ и понимание информации.
- *Решения*: этот узел отражает этап принятия решений, который основывается на интерпретации информации.
- *Действия*: этот узел представляет этап действий, которые следуют за принятием решений.

Ребра (связи):

- Ребро между *Когнитивными рефреймингами* и *Изменением восприятия* указывает на связь между общей концепцией когнитивных рефреймингов и этапом изменения восприятия информации.
- Ребро между *Изменением восприятия* и *Интерпретацией* указывает на переход от изменения восприятия к этапу интерпретации и анализа.
- Ребро между *Интерпретацией* и *Решениями* отражает переход от анализа и интерпретации к этапу принятия решений.
- Ребро между *Решениями* и *Действиями* представляет связь между этапом принятия решений и последующими действиями.

## Результаты

Предложим математическую модель для вычисления весов ребер в графе когнитивных рефреймингов. Эта модель учитывает важность каждой концепции (узла) и взаимодействие между ними [Гарифуллина, Исавнин 2021: 469–470].

Пусть $W_{AB}$ обозначает вес ребра между узлами A и B, где A и B – это концепции (узлы) в графе. Тогда вес ребра может быть выражен как произведение трех факторов:

$$W_{AB} = (\alpha_1 * W_A * M_{A1} + \alpha_2 * W_A * M_{A2} + \alpha_3 * W_A * M_{A3}) * (\beta_1 * W_B * M_{B1} + \beta_2 * W_B * M_{B2} + \beta_3 * W_B * M_{B3}) * F_{AB}$$

Где:

$W_{AB}$ – вес ребра между концепциями A и B,

$W_A$ – вес (значимость) концепции A,

$W_B$ – вес (значимость) концепции B,

$M_{A1}$, $M_{A2}$, $M_{A3}$ – дополнительные метрики важности для концепции A,

$M_{B1}$, $M_{B2}$, $M_{B3}$ – дополнительные метрики важности для концепции B,

$\alpha_1$, $\alpha_2$, $\alpha_3$ – коэффициенты важности для метрик A,

$\beta_1$, $\beta_2$, $\beta_3$ – коэффициенты важности для метрик B,

$F_{AB}$ – фактор взаимодействия между концепциями A и B.

$W_A$ определяется как взвешенная комбинация разных метрик важности. Предусматривается она для концепции A. Формула выглядит так:

$$W_A = \alpha * \text{Метрика1}_A + \beta * \text{Метрика2}_A + \gamma * \text{Метрика3}_A$$

При этом α, β, γ являются коэффициентами, которые отражают важность каждой метрики в оценке концепции. Эти коэффициенты определяются на основе анализа исторических данных.

$\text{Метрика1}_A$ напрямую связана с интенсивностью и количеством применения способов когнитивных рефреймингов. Они используются в системах, с помощью которых осуществляется управление безопасностью. $\text{Метрика1}_A$ определяется по данным о частоте применения когнитивных рефреймингов и числе обученных сотрудников, полученным из отчетов и систем мониторинга безопасности, таких как SIEM-системы (Security Information and Event Management), например Splunk (2024).

$\text{Метрика2}_A$ применяется для измерения результативности и эффективности использования рефреймингов с точки зрения безопасности. Это число тех инцидентов, которые удалось предотвратить, а также существенное уменьшение времени, которое



 https://doi.org/10.21603/2782-4799-2024-3-4-316-325

требуется на то, чтобы отреагировать на существующие угрозы. Источники данных включают внутренние отчеты инцидентов и системы управления инцидентами, такие как ServiceNow (2024).

Метрика$3_A$ позволяет отразить объединение когнитивных рефреймингов в необходимую систему обеспечения безопасности критической инфраструктуры. Это оценка адаптивности и гибкости реакции системы на постоянно меняющиеся угрозы. Также она определяет успешность внедрения во все процессы когнитивных рефреймингов. Используются данные из систем управления безопасностью Palo Alto Networks (2024).

$W_B$ – вес (определенная значимость) узла B: данным фактором определяется значимость концепции. Приведенная модель может использоваться аналогично вышеописанной нами модели $W_A$:

$$W_B = \alpha * \text{Метрика}1_B + \beta * \text{Метрика}2_B + \gamma * \text{Метрика}3_B$$

Метрика$1_B$: оценивает интеграцию концепции с существующими технологиями. Источники данных включают отчеты о совместимости и внедрении технологий, например из платформ типа IBM Security (2024).

Метрика$2_B$: измеряет влияние концепции на решения по безопасности. Используются внутренние отчеты по управлению безопасностью и результаты оценки эффективности решений из платформы McAfee (2024).

Метрика$3_B$: оценивает влияние концепции на риски безопасности. Источники данных включают анализ изменений уровня риска на основе данных о кибератаках и уязвимостях из базы данных CVE (2024).

Метрики важности (дополнительные), которые предусмотрены для концепции A:

$M_{A1}$ – позволяет оценить стабильность и длительность концепция A, применяется с точки зрения управления необходимой безопасностью. Она включает длительность применения концепции.

$M_{A2}$ – позволяет отразить, как концепции A удалось приспособиться к постоянно меняющимся угрозам и условиям. Оценивается гибкость и эффективность реакции концепции A на меняющиеся сценарии и условия.

$M_{A3}$ – дает оценку эффективности проводимого обучения с применением концепции A. Идет оценка практических результатов, которых удалось достичь при управлении необходимой безопасностью критической инфраструктуры. Оценивается процент успешного использования тех навыков и знаний, которые были получены.

Метрики важности (дополнительные), предусмотренные для концепции B:

$M_{B1}$ – используется для измерения объединения данной концепции с существующими в настоящее время технологиями и методами, которые применяются в системе безопасности. Этот фактор чрезвычайно важен, т. к. он определяет эффективность.

$M_{B2}$ – дает оценку того, как концепция B влияет на те решения, которые принимаются при управлении безопасностью. Она включает различные изменения, которые происходят в решениях под влиянием концепции B.

$M_{B3}$ – позволяет оценить, каким образом концепция B влияет на риски в важном контексте обеспечения безопасности инфраструктуры. Она включает обязательную оценку меняющегося уровня риска при применении концепции, а также определенное увеличение или снижение.

$F_{AB}$ – фактор, отражающий взаимодействие двух вышеописанных нами концепций. Он оказывает на них влияние и определяет их действенность и важность. Он помогает оценить влияние комбинации описанных концепций на управление безопасности и ее улучшение.

Эта модель позволяет получить точные веса для ребер в графе когнитивных рефреймингов, что помогает визуализировать и анализировать влияние различных концепций на безопасность критической инфраструктуры. Результаты расчетов весов ребер продемонстрированы на графе (рис. 2).

Вес концепции *Когнитивные рефреймингги* самый большой. Именно это свидетельствует о том, что она чрезвычайно важна. Указанная идея является основной. Она помогает менять восприятие и интерпретировать полученную информацию. Данная концепция – основа для других. С ее помощью удается создать контекст, чтобы анализировать и управлять безопасностью.

Вес *Изменения восприятия* меньше. Данная концепция подразумевает, что нужно обязательно менять определенное восприятие той или иной сложившейся ситуации. Это шаг в описанном нами процессе рефреймингов. Он важен, хотя и весит меньше.

*Интерпретация* весит достаточно много. Это является признаком ее значимости. Данной концепцией предполагается понимание и анализ имеющейся информации. Она чрезвычайно важна при изменении рамок познания.

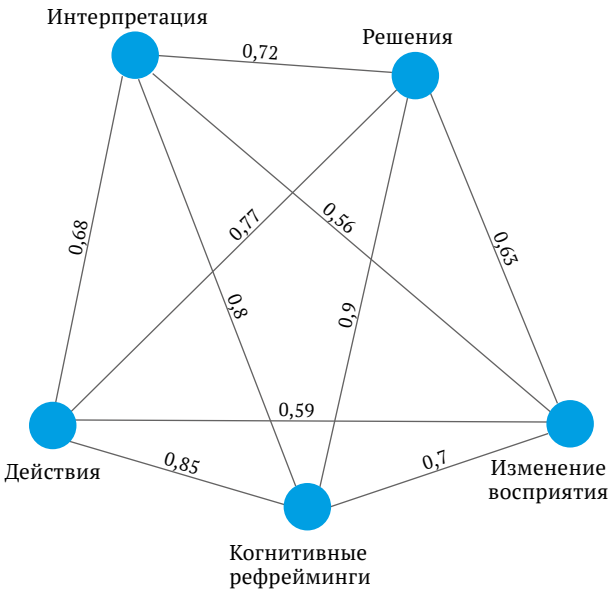


**Рис. 2. Граф когнитивных рефреймингов с весами**
**Fig. 2. Cognitive reframing with weight values: graph scheme**

*Решения* – одна из основных концепций, используемых в когнитивных рефреймингах. На этом этапе принимаются решения. Первоначально информация интерпретируется и анализируется. С ее помощью удается подчеркнуть, что принимаемые решения – основной элемент, позволяющий управлять безопасностью инфраструктуры.

*Действия* не менее важны, но они не так значимы, как *Решения*, т. к. первоначально принимаются решения, а потом начинаются действия. Обуславливаются они принятыми первоначально решениями.

Граф дает возможность визуализировать не только эти концепции, но и их связи. Весами ребер определяется их значения и связи. С его помощью можно понять, как использовать данные концепции, для того чтобы анализировать и управлять безопасностью инфраструктуры. При этом придается больший вес главным этапам меняющихся рамок.

Рассмотрим вероятные сценарии применения когнитивных рефреймингов для защиты критической инфраструктуры. В их основе лежит модель, учитывающая определенные веса описываемых концепций. Для сценариев берутся в расчет требования и угрозы, характерные для разных типов инцидентов. Каждый сценарий включает в себя этапы:

- Идентификация проблемной области: определение типа угроз или рисков, требующих применения когнитивных рефреймингов (например, киберугрозы, природные катастрофы или сбои в работе систем).
- Определение ключевых этапов анализа и реагирования: выделение этапов, таких как когнитивные рефреймингги, изменение восприятия, интерпретация, решения и действия, которые будут оцениваться в контексте выбранной проблемы.
- Присвоение весов этапам: оценка важности каждого этапа в контексте сценария для определения их относительного влияния на общий процесс управления рисками.

### Первый сценарий: Кибербезопасность

С помощью когнитивных рефреймингов можно увеличить кибербезопасность инфраструктуры. Применяя вычисление весов концепций, есть возможность определить существующие этапы, в ходе которых анализируются вероятные киберугрозы:

- Когнитивные рефреймингги (вес: 1,0): основная концепция, устанавливающая контекст, позволяющий анализировать существующие киберугрозы.
- Изменение восприятия (вес: 0,7): специалистами пересматривается восприятие общего характера существующих киберугроз, а также вероятных сценариев происходящих событий.
- Интерпретация (вес: 0,8): на данном этапе аналитиками анализируются полученные данные. Дается их определенная интерпретация. Делается это для того, чтобы выявить существующие уязвимости и паттерны.
- Решения (вес: 0,9): после интерпретации специалистами принимаются определенные решения, дающие возможность предотвратить угрозы и правильно на них реагировать.
- Действия (вес: 0,85): в этот момент делаются определенные шаги, которые позволяют реализовать принятые решения и обеспечить необходимую кибербезопасность.

### Второй сценарий: Возможность управлять природными явлениями

Катастрофы в природе способны оказать существенное влияние на критическую инфраструктуру. Рефреймингги помогают управлению существующими рисками:

- Когнитивные рефреймингги (вес: 1,0): основа, формирующая фундамент, помогающий анализировать природные катастрофы.
- Изменение восприятия (вес: 0,7): на этом этапе пересматривается восприятие условий и возможных угроз.



 https://doi.org/10.21603/2782-4799-2024-3-4-316-325

- Интерпретация (вес: 0,8): анализируются данные о землетрясениях, погоде и иных явлениях в природе. Это позволяет предвидеть возможные последствия.
- Решения (вес: 0,9): после того как данные проанализированы, принимаются те или иные решения о тех мерах, которые нужно предпринять. Определяется, как правильно реагировать на катастрофы в природе.
- Действия (вес: 0,85): идет воплощение принятых решений в определенные действия. В данном случае обеспечивается защита населения и критической инфраструктуры.

**Третий сценарий: Обеспечивается бесперебойная работа**

Когнитивные рефреймингы помогают обеспечить бесперебойную работу всей инфраструктуры:

- Когнитивные рефреймингы (вес: 1,0): первый значимый этап, обеспечивающий структуру, чтобы анализировать и управлять системами.
- Изменение восприятия (вес: 0,7): на этом этапе статус систем пересматривается. Выявляются угрозы потенциального характера.
- Интерпретация (вес: 0,8): идет интерпретация всех данных о том, в каком состоянии находится оборудование. Это дает возможность прогнозировать поломки и вероятные сбои в работе.
- Решения (вес: 0,9): осуществляется принятие необходимых решений о мерах, с помощью которых можно исключить вероятность сбоев и гарантировать непрерывную работу.
- Действия (вес: 0,85): на данном этапе специалисты действуют с той целью, чтобы восстановить нормальную работу всех систем и устранить сбои.

В сценариях, несмотря на различия в типах угроз, одинаковые веса для этапов объясняются следующим образом:

- Основная роль этапов: этапы *Когнитивные рефреймингы* (вес: 1,0), *Изменение восприятия* (вес: 0,7), *Интерпретация* (вес: 0,8), *Решения* (вес: 0,9) и *Действия* (вес: 0,85) играют критическую роль в любом сценарии. Высокий вес назначается основным этапам, формирующим основу анализа, тогда как средние и более низкие веса соответствуют этапам адаптации, интерпретации данных и реализации решений.
- Универсальность: одинаковые веса для этапов подчеркивают их универсальную значимость в различных сценариях. Например, этап *Интерпретация* (вес: 0,8) одинаково важен для анализа данных в любом контексте, будь то киберугрозы или природные катастрофы. Это позволяет сохранить консистентность в подходах к анализу и управлению рисками.
- Стандартизация подхода: использование одинаковых весов упрощает сравнение и интеграцию результатов различных сценариев. Это поддерживает универсальные стандарты и обеспечивает более комплексный и согласованный подход к управлению угрозами и рисками.

Описанные сценарии наглядно демонстрируют применение когнитивных рефреймингов, для того чтобы улучшить безопасность, управлять максимально действенно критической инфраструктурой, а также своевременно реагировать на постоянно меняющиеся условия. Применение этого современного подхода позволяет повышать необходимую надежность и устойчивость всех значимых систем.

## Заключение

В статье рассматривается использование когнитивных рефреймингов для предотвращения и прогнозирования угроз. Критическая инфраструктура очень важна, она поддерживает функции общества. Уязвимость перед разными рисками приводит к тому, что возникает необходимость постоянно совершенствовать способы управления и защиты.

Когнитивные рефреймингы дают возможность пересмотреть классические подходы к анализу и восприятию информации, удается решать проблемы по-другому. Математическая модель позволяет вычислить вес концепций. При этом принимаются во внимание взаимосвязи и значимость. Указанная модель приспосабливается к разным сценариям, и помогает выявить этапы анализа существующих угроз.

Имеются разные сценарии применения когнитивных рефреймингов. Они помогают защитить критическую инфраструктуру. Речь идет о том, что нужно повысить кибербезопасность, управлять последствиями катастроф и обеспечить работу систем без перебоев. Эти примеры демонстрируют применение данного подхода для эффективного управления инфраструктурой.

Когнитивные рефреймингы – инструмент перспективного характера, который дает возможность прогнозировать и предотвращать угрозы. Их использование позволяет обществу справляться

с существующими рисками. Обеспечивается безопасность и надежность всех систем. Стоит продолжать исследование в данной сфере. Важно совершенствовать защиту инфраструктуры и правильно этим управлять. При этом нужно учитывать, что угрозы часто меняются, они непредсказуемы.

**Конфликт интересов:** Автор заявил об отсутствии потенциальных конфликтов интересов в отношении исследования, авторства и / или публикации данной статьи.

**Conflict of interests:** The author declared no potential conflicts of interests regarding the research, authorship, and / or publication of this article.

## Литература / References

Брумштейн Ю. М., Молимонов Д. А., Кривенко А. И., Гроцкая А. Ю. Системный анализ целей, направлений и технических решений для исследования процессов зрительного восприятия и памяти человека. *Физика и радиоэлектроника в медицине и экологии – ФРЭМЭ'2020*: XIV Междунар. науч. конф. (Владимир-Суздаль, 1–3 июля 2020 г.) Владимир: ВлГУ, 2020. С. 336–341. [Brumstein Yu. M., Molimonov D. A., Krivenko A. I., Grotskaya A. Y. System analysis of goals, directions and technical solutions for the study of human visual perception and memory processes. *Physics and radioelectronics in medicine and ecology – FRAME'2020*: Proc. XIV Intern. Sci. Conf., Vladimir-Suzdal, 1–3 Jul 2020. Vladimir: VSU, 2020, 336–341. (In Russ.)] https://elibrary.ru/tqnwdi

Валеев Р. Р., Орлов С. П. Организация систем информационной безопасности на основе компьютерной системы поддержки принятия решений. *Наука и мир*. 2018. № 6-1. С. 16–21. [Valeev R. R., Orlov S. P. The organization of information security systems on the basis of the computer decision support system. *Nauka i mir*, 2018, (6-1): 16–21. (In Russ.)] https://elibrary.ru/ucugkd

Гарифуллина Л. А., Исавнин А. Г. Оценка актуальности и эффективности интеграции искусственных нейронных сетей в системах информационной безопасности. *Modern Science*. 2021. № 3-2. С. 467–472. [Garifullina L. A., Isavnin A. G. Assessing the relevance and effectiveness of the integration of artificial neural networks in information security systems. *Modern Science*, 2021, (3-2): 467–472. (In Russ.)] https://elibrary.ru/ohqnom

Громов Ю. Ю., Елисеев А. И., Дидрих В. Е., Уланов А. О. Математическое обеспечение системы контроля состояния надежности и безопасности сетецентрической информационной системы. *Информация и безопасность*. 2015. Т. 18. № 4. С. 602–607. [Gromov Yu. Yu., Eliseev A. I., Didrikh V. E., Ulanov A. O. Mathematical support monitoring systems reliability and security of network-centric information system. *Information & Security*, 2015, 18(4): 602–607. (In Russ.)] https://elibrary.ru/vadqbn

Губанов В. П., Закиров И. Ф. Методы анализа уязвимостей информационных систем. *Информационные технологии и вычислительные системы*. 2015. № 2. С. 31–39. [Gubanov V. P., Zakirov I. F. Methods of vulnerability analysis of information systems. *Information technologies and computing systems*, 2015, (2): 31–39. (In Russ.)]

Казьмина И. В., Потудинский А. В., Крючков Р. А. Обеспечение информационной безопасности на высокотехнологичных предприятиях ОПК. *Цифровая и отраслевая экономика*. 2023. № 3. С. 40–46. [Kazmina I. V., Potudinsky A. V., Kryuchkov R. A. Ensuring information security at high-tech enterprises in the military-industrial. *Tsifrovaia i otraslevaia ekonomika*, 2023, (3): 40–46. (In Russ.)] https://elibrary.ru/osiian

Карташев Е. Н., Красовский В. С. Информационная безопасность современного предприятия ОПК. *Вопросы защиты информации*. 2016. № 4. С. 41–46. [Kartashev E. N., Krasovskiy V. S. Information security of a modern enterprise engaged in defense-industrial sector. *Voprosy zashchity informatsii*, 2016, (4): 41–46. (In Russ.)] https://elibrary.ru/xehnrp

Курманбай А. К., Нозирзода Ш. С. Разработанная система критериев информационной безопасности при внедрении информационных систем. *Новая наука: От идеи к результату*. 2016. № 5-2. С. 175–178. [Kurmanbai A. K., Nozirzoda S. S. A new system of information security criteria in information systems. *Novaia nauka: Ot idei k rezultatu*, 2016, (5-2): 175–178. (In Russ.)] https://elibrary.ru/vzgjzn

Лавриненко А. А., Гончаренко В. М. Методы анализа графов в задачах информационной безопасности. *Информационные технологии и вычислительные системы*. 2016. № 3. С. 63–70. [Lavrinenko A. A., Goncharenko V. M. Methods of graph analysis in information security problems. *Information technologies and computing systems*, 2016, (3): 63–70. (In Russ.)]

Лаптев В. Н., Сидельников О. В., Шарай В. А. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах. *Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета*. 2011. № 72. С. 76–85. [Laptev V. N., Sidelnikov O. V., Sharaj V. A. Application of the method of the inductive forecasting of states for detecting of computer attacks in information-telecommunication systems. *Polythematic Online Scientific Journal of Kuban State Agrarian University*, 2011, (72): 76–85. (In Russ.)] https://elibrary.ru/oiuett

Панилов П. А., Кокорев А. В. Эволюционные алгоритмы оптимизации управления безопасностью критической инфраструктуры на основе когнитивных карт. *Информатизация и информационная безопасность правоохранительных органов,* ред. А. В. Бецков. М.: АУ МВД РФ, 2024. С. 232–238. [Panilov P. A., Kokorev A. V. Evolutionary algorithms for optimizing critical infrastructure security management based on cognitive maps. *Informatization and information security of law enforcement agencies*, ed. Betskov A. B. Moscow: AM MIA RF, 2024, 232–238. (In Russ.)] https://elibrary.ru/bpcwno

Панилов П. А., Цибизова Т. Ю., Чернега Е. В. Разработка алгоритма управления когнитивными функциями в интеллектуальных системах безопасности. *Известия Тульского государственного университета. Технические науки*. 2023. № 10. С. 47–61. [Panilov P. A., Tsibizova T. Yu., Chernega E. V. Development of an algorithm for managing cognitive functions in intelligent security systems. *Izvestiya Tula State University. Technical sciences*, 2023, (10): 47–61. (In Russ.)] https://doi.org/10.24412/2071-6168-2023-10-47-48

Пролетарский А. В., Скворцова М. А., Терехов В. И. Гибридная интеллектуальная система оценки рисков на основе неструктурированной информации. *Нейрокомпьютеры: разработка, применение*. 2017. № 1. С. 66–74. [Proletarsky A. V., Skvortsova M. A., Terekhov V. I. Hybrid intelligent system for risk assessment based on unstructured data. *Neurocomputers: development, application*, 2017, (1): 66–74. (In Russ.)] https://elibrary.ru/yhwrez

Скрыпников А. В., Чернышова Е. В., Яценко Ю. И. Разработка алгоритма автоматического выделения априорных признаков системы информационной безопасности. *Теория и практика современной науки*: XVII Междунар. науч.-практ. конф. (Москва, 8–9 апреля 2015 г.) М.: Институт стратегических исследований, 2015. С. 65–74. [Skrypnikov A. V., Chernyshova E. V., Yatsenko Yu. I. A new algorithm for automatic identification of a priori features of an information security system. *Theory and practice of modern science*: Proc. XVII Intern. Sci.-Prac. Conf., Moscow, 8–9 Apr 2015. Moscow: Institut strategicheskikh issledovanii, 2015, 65–74. (In Russ.)] https://elibrary.ru/tqfvoj

Трофимов О. В., Саакян А. Г. Цифровизация и проблемы обеспечения информационной безопасности на предприятиях оборонно-промышленного комплекса Российской Федерации. *Креативная экономика*. 2023. Т. 17. № 9. С. 3331–3344. [Trofimov O. V., Saakyan A. G. Digitalization and the problems of ensuring information security in the military-industrial companies of the Russian Federation. *Creative Economy*, 2023, 17(9): 3331–3344. (In Russ.)] https://doi.org/10.18334/ce.17.9.119149

Цибизова Т. Ю., Панилов П. А., Кочешков М. А. Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования. *Известия Тульского государственного университета. Технические науки*. 2023. № 6. С. 33–41. [Tsibizova T. Yu., Panilov P. A., Kocheshkov M. A. Monitoring the security of the information security system of the critical information infrastructure based on cognitive modeling. *Izvestiya Tula State University. Technical sciences*, 2023, (6): 33–41. (In Russ.)] https://doi.org/10.24412/2071-6168-2023-6-33-41

Chen J., Zou Y., Wen Y. Blockchain-based internet of things and edge computing for resilient critical infrastructure. *IEEE Network*, 2019, 33(1): 156–165.

Panilov P., Tsibizova T., Voskresensky G. Methodology of expert-agent cognitive modeling for preventing impact on critical information infrastructure. *High-performance computing systems and technologies in scientific research, automation of control and production*: Proc. 13 Intern. Conf., Barnaul, 19–20 May 2023. Cham: Springer, 2024, 276–287. https://doi.org/10.1007/978-3-031-51057-1_21

Wang Q., Guo C., Wu H. A deep learning-based cybersecurity risk assessment approach for smart factories. *IEEE Transactions on Industrial Informatics*, 2021, 17(3): 1783–1793.