Технические науки

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Андрияхов Я.В., Сверчков Р.В.

ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Москва, e-mail: yarik-and@mail.ru

Научный руководитель: Микрюков А.А.

Киберустойчивость является неотъемлемой составляющей современной парадигмы информационной безопасности, представляя собой многоуровневую систему мер, направленных на обеспечение целостности, доступности и конфиденциальности данных в условиях постоянно усложняющихся киберугроз.

Актуальность задачи определяется необходимостью перехода в рамках реализации нового национального проекта «Экономика данных и трансформация государственного управления» и в условиях интенсивных деструктивных воздействий к новой парадигме обеспечения безопасности информационных ресурсов компаний, включающей тесно связанные между собой процессы обеспечения кибербезопасности, поддержания функционала защищаемых информационных ресурсов и непрерывности автоматизации бизнес-процессов. Компании, работающие с большими объемами данных и критически важной инфраструктурой, подвергаются повышенному риску деструктивных воздействий, способных нарушить непрерывность их работы. Традиционные механизмы защиты информации, фокусирующиеся на превентивных мерах, более не обеспечивают полного спектра защиты от современных угроз. В этом контексте возникает необходимость в разработке и применении подходов, которые не только предотвращают атаки, но и гарантируют оперативное восстановление и минимизацию ущерба [1].

Киберустойчивость включает в себя ряд взаимосвязанных составляющих: кибербезопасность, отказоустойчивость и непрерывность функционирования: Особое значение в обеспечении надежности инфраструктуры приобретает катастрофоустойчивость, направленная на минимизацию последствий инцидентов и ускорение восстановления функциональности системы после сбоев. В статье рассматриваются ключевые принципы киберустойчивости и катастрофоустойчивости, направленные на минимизацию последствий инцидентов, быстрое восстановление функциональности систем и поддержание их высокой доступности. Обоснована необходимость интеграции данных принципов для повышения уровня готовности к восстановлению и обеспечения непрерывности предоставления услуг пользователям.

Катастрофоустойчивость как составная часть киберустойчивости

Катастрофоустойчивость (disaster recovery) предполагает обеспечение готовности системы к восстановлению после сбоев, отказов, катастроф или целенаправленных кибератак [2]. В рамках киберустойчивости катастрофоустойчивость играет важную роль, так как инциденты, будь то кибератака или физическая катастрофа, могут привести к полному или частичному выходу системы из строя, и поэтому для минимизации ущерба важно учитывать такие параметры, как допустимый время потери данных (RPO) и целевое время восстановления (RTO) (рис. 1).

Рис. 1. Соотношение времени восстановления/время потери данных [4]

Это особенно актуально для Критической информационной инфраструктуры (КИИ), где такие инциденты могут привести к тяжелым последствиям для общества и экономики [3].

Катастрофоустойчивость обеспечивается реализацией комплексного подхода, направленного на поддержания готовности системы к быстрому восстановлению и минимизации времени простоя после инцидента. Ниже представлено влияние каждого компонента на коэффициент готовности (КГ), определяющий уровень доступности критической инфраструктуры, где КГ отражает долю времени, в течение которого система остаётся доступной:

1. Резервный план восстановления обеспечивает оперативный запуск процедуры восстановления при сбоях, что минимизирует время простоя и увеличивает КГ. Наличие детализированных планов сокращает среднее время восстановления (MTTR) [5].

2. Резервное копирование данных позволяет уменьшить вероятность потери данных и позволяет оперативно восстанавливать их при инцидентах, что сокращает время простоя и поддерживает КГ на высоком уровне. Копии данных следует регулярно обновлять и хранить на внешних устройствах, чтобы не зависеть от основных хранилищ.

3. Георезервирование – это распределение центров обработки данных по разным географическим локациям, что позволяет избежать полной остановки системы при локальных сбоях или катастрофах. Оно поддерживает высокое значение КГ за счет автоматического переключения на рабочие узлы.

4. Микросервисная архитектура и дублирование микросервисов на разных площадках увеличивает избыточность системы, что позволяет оперативно перенаправлять запросы на дублирующие сервисы в случае сбоя. Это решение снижает MTTR и повышает КГ.

5. Синхронизация и согласованность данных – это поддержание консистентности данных между географически разнесёнными узлами, что позволяет избежать потери информации, сохраняя целостность данных и предотвращая их несоответствие. Это решение повышает надёжность инфраструктуры, что положительно сказывается на КГ.

6. Балансировка нагрузки и автоматическое перераспределение реализует поддержку высокой производительности системы, равномерно распределяя запросы. В случае сбоя на одной из площадок нагрузка перераспределяется на доступные узлы, снижая вероятность полной остановки системы и повышая КГ [6].

7. Репликация данных и мониторинг в реальном времени – постоянная репликация данных и мониторинг позволяют оперативно реагировать на сбои и автоматизировать переключение на резервные узлы, что минимизирует MTTR и увеличивает КГ.

8. Непрерывность работы критических функций – поддерживает работу жизненно важных процессов даже в условиях аварий, минимизируя потерю функциональности.

Реализацией георезервирования является использование микросервисной архитектуры, при которой микросервисы системы дублируются на нескольких площадках (рис. 2).

На рисунке 2 показана архитектура георезервирования, при которой микросервисы и базы данных системы распределены между двумя центрами обработки данных (ЦОД 1 и ЦОД 2). Каждый ЦОД содержит идентичные микросервисы и базы данных, обеспечивая дублирование функциональности на каждой площадке. Балансировщики нагрузки и данных распределяют запросы между микросервисами и базами данных, обеспечивая высокую доступность и непрерывность работы системы. Такая схема позволяет системе продолжать работу даже при выходе из строя одного из центров обработки данных.

Это позволяет обеспечить избыточность и устойчивость системы. Для того чтобы дублированные микросервисы корректно функционировали, необходимо синхронизировать их работу. Это достигается благодаря отдельным серверам синхронной записи данных, что гарантирует согласованность данных между разнесёнными центрами. Также критически важным условием является обеспечение непрерывной сетевой связности между площадками, что позволяет поддерживать постоянный обмен данными и координировать работу микросервисов на уровне архитектуры [7].

Географическое распределение системы предполагает размещение её центров обработки данных и вычислительных узлов в разных географических регионах. Это разнесение инфраструктуры позволяет защитить систему от сбоев, вызванных локальными инцидентами, такими как природные катастрофы или локальные кибератаки, поскольку один отказавший узел не влияет на работу других узлов, расположенных в других регионах.

При штатном функционировании система с географическим распределением в режиме балансировки нагрузки равномерно распределяет запросы и данные между разнесёнными микросервисами [8]. Это решение не только повышает общую производительность системы, но и снижает нагрузку на каждый отдельный узел, что улучшает её надёжность и скорость отклика. В случае аварийного сбоя на одной из площадок система автоматически перераспределяет нагрузку на оставшиеся доступные узлы, обеспечивая бесперебойность работы сервисов и минимизируя воздействие на пользователей даже в условиях частичной утраты инфраструктуры.

Рис. 2. Архитектура георезервирования

Таким образом, георезервирование не только повышает общую устойчивость системы, но и способствует её гибкости и масштабируемости. Это особенно важно для критических информационных систем, где любые сбои могут привести к серьёзным последствиям, включая потерю данных, снижение уровня обслуживания или даже нарушение работы национально значимых процессов.

Для обеспечения согласованности данных и доступности сервисов используется механизм репликации, при котором данные синхронно копируются на несколько узлов или центров данных. Важно также использование алгоритмов мониторинга и автоматического переключения на резервные ресурсы в реальном времени, что позволяет системе моментально реагировать на инциденты без вмешательства человека.

Модельные расчеты, проведённые в рамках нашего исследования, демонстрируют, что последовательное внедрение таких мер, как резервное копирование, георезервирование, балансировка нагрузки и репликация данных, позволяет значительно повысить коэффициент готовности информационной инфраструктуры. В таблице 1 приведены модельные значения коэффициента готовности для различных комбинаций реализованных мер, где базовый показатель для систем без специальных мер составляет 95 %, а комплексный подход позволяет достичь значения 99,9%.

На рисунке 3 показан экспоненциальный рост показателя КГ при реализации каждой новой меры, что подчёркивает значительный эффект интеграции дополнительных защитных механизмов.

Аналогичным образом, модельные расчеты показывают, что среднее время восстановления (MTTR) существенно сокращается с внедрением соответствующих мер.

Из таблицы 2 наглядно видно, что MTTR для систем без резервного копирования составляет 6–12 часов, а при использовании комплексного подхода данный показатель снижается до 0.1–0.3 часа.

Рисунок 4 демонстрирует снижение MTTR при последовательной реализации мер, что особенно критично для обеспечения непрерывности бизнес-процессов.

Таблица 1

Влияние внедренных мер на коэффициент готовности (КГ)

Внедренные меры	Коэффициент готовности (КГ), %
Без мер по катастрофоустойчивости	95.0
Резервное копирование	96.5
Георезервирование	97.8
Балансировка нагрузки	98.6
Репликация данных	99.3
Комплексный подход	99.9

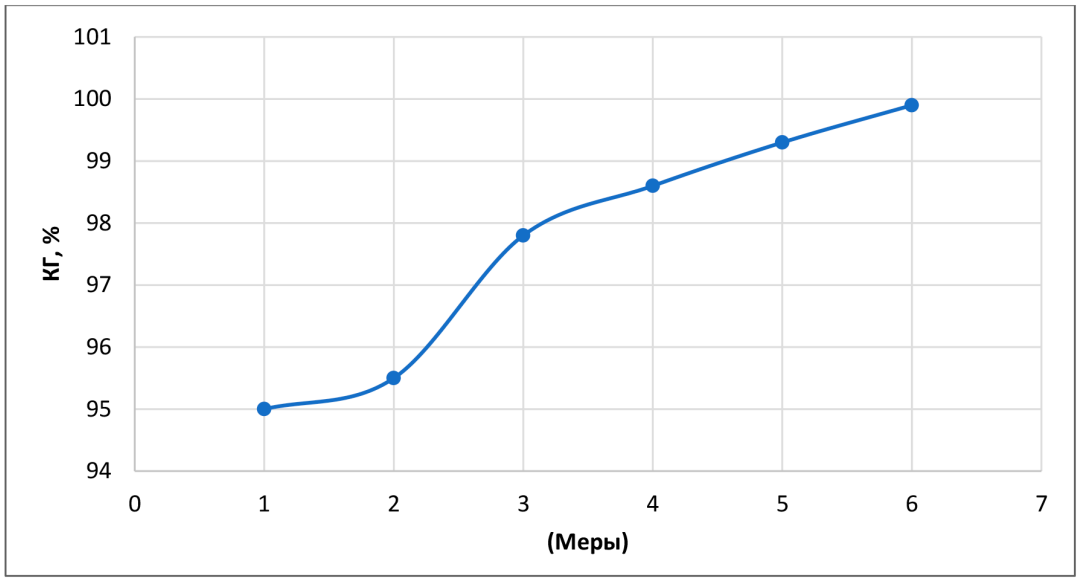

Рис. 3. Зависимость коэффициента готовности (КГ) от количества реализованных мер

Таблица 2

Влияние реализованных мер на среднее время восстановления (MTTR)

Внедренные меры	Среднее время восстановления (MTTR), часы
Без резервного копирования	6 – 12
С резервным копированием	3 – 6
С георезервированием	1 – 3
С автоматическим переключением	0.5 – 1
Комплексный подход	0.1 – 0.3

Модельные данные подтверждают, что комплексный подход способствует значительному повышению коэффициента готовности до 99,9 % и сокращению времени восстановления до минимальных значений, что является залогом эффективной защиты информационной инфраструктуры.

Таким образом, показано, что предложенные меры существенно способствуют повышению показателя катастрофоустойчивости информационной инфраструктуры. Они обеспечивают минимизацию последствий инцидентов, сокращение времени восстановления и повышение устойчивости к сбоям информационной инфраструктуры. Реализация указанных мероприятий обеспечивает не только защищенность критически важные данные, но и поддержание высокой доступности ключевых бизнес-процессов, что особенно важно в условиях нарастающих киберугроз.

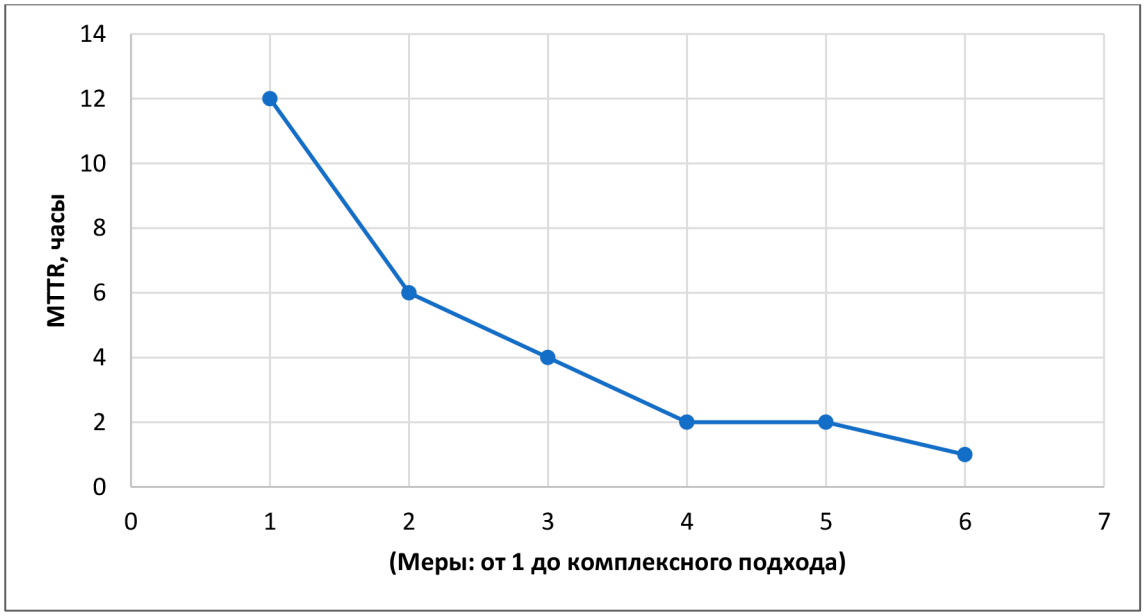

Рис. 4. Снижение среднего времени восстановления (MTTR) в зависимости от реализованных мер

Список литературы

1. Буховец А.Г., Бирючинская Т.Я., Горностаев А.К. Устойчивость аттрактора систем рандомизированных функций // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2024. № 2. С. 5-14.

2. Трушкин К.А. О переводе КИИ на доверенные программно-аппаратные комплексы // Безопасность информационных технологий. 2024. Т. 31. № 3. С. 45-52.

3. Бородин А.В. Киберустойчивость критических информационных инфраструктур // Информационная безопасность систем. 2024. № 5. С. 17-24.

4. Сафедата. Обеспечение безопасности облачных сервисов: проблемы и решения // Хабр. 2015. URL: https://habr.com/ru/companies/safedata/articles/273947/ (дата обращения: 10.01.2025).

5. Акутин А.С., Бровко А.В. Реализация алгоритма доказательства с нулевым разглашением в технологии цифровой личности // Вестник ВГУ. 2024. № 2. С. 113-122.

6. Назаров И.И. Повышение уровня надёжности информационных систем // Киберленинка. 2024. № 3. С. 11-18.

7. Иванов С.В., Кравцов М.Л. Катастрофоустойчивость информационных систем на базе микросервисной архитектуры // Информационные технологии. 2024. № 5. С. 29-36.

8. Зайцев П.А. Методы обеспечения отказоустойчивости в распределенных системах // Вестник Московского государственного университета. 2024. С. 50-58.

КОНТРОЛЬ ТЕПЛОВЫХ ПАРАМЕТРОВ НАПРЯЖЕННО-ДЕФОРМИРОВАННОГО СОСТОЯНИЯ ЭЛЕМЕНТОВ АЭС НА БАЗЕ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ

Бадеев В.А., Бадеева Е.А.

Пензенский государственный университет, Пенза, e-mail: vladbadeev4464@gmail.com

Научный руководитель: Бадеева Е.А.

Для измерения различных параметров защитной оболочки АЭС в процессе ее строительства и эксплуатации преимущество отдается искробезопасным волоконно-оптическим информационно-измерительным системам (ВОИИС) в состав которой обязательное включение датчиков температуры (ВОДТ). Так, в процессе строительства АЭС температура цемента в основании защитной оболочки изменяется в диапазоне 0 … плюс 90 °С. Есть ситуации, когда температура изменяется в диапазоне минус 30 … плюс 90 °С. Проектировщики АЭС предполагают различные эксплуатационные режимы: нормальный режим, режим нарушения нормальной эксплуатации (режимы «малая течь», «большая течь», нарушение теплового отвода) и аварийный режим. В условиях нормальной эксплуатации в межоболочном пространстве температура от 10 до 60 °С при мощности поглощенной дозы до $1{,}19 \cdot 10^{-6}$ Гр/ч. При нарушении нормальной эксплуатации температура бетона повышается до 85…90 °С при мощности поглощенной дозы до 1,0 Гр/ч [1-3].

Использование для установки известных датчиков в цемент защитных гильз от воздействия высокого давления ведет к большой до 5…10 % погрешности измерений. При установке таких датчиков в затвердевающий цемент их корпус и внутренние элементы будут испытывать большие деформации, например уровень деформации корпуса ВОДТ сравним с диапазоном измерения датчика, который определяется изменением расстояния между отражателем и торцом оптических волокон, соответственно все метрологические характеристики, полученные в процессе градуирования и калибровки датчика, существенно изменятся. Конструкция