УДК 004.056

Давлетова Д.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ПОСТРОЕНИЕ МОДЕЛИ ДУБЛИРОВАНИЯ ПОДСИСТЕМ В ЗАЩИТЕ ИНФОРМАЦИИ

Аннотация. Защита информации является критически важной задачей во многих областях деятельности человека – от бизнеса до государственного управления. Одним из способов повышения надежности защиты информации выступает дублирование подсистем, обеспечивающих безопасность информационных ресурсов. Данная работа посвящена построению модели дублирования подсистем в защите информации.

Ключевые слова: защита информации, дублирование подсистем, построение модели.

Метод дублирования подсистем является эффективным способом повышения надежности и устойчивости информационных систем перед внешними угрозами и внутренними сбоями. Однако простое внедрение дублирующих механизмов недостаточно для полноценного совершенствования системы защиты информации [1]. Необходимо учитывать ряд аспектов и направлений развития:

1. Избыточность аппаратных ресурсов.

Следует использовать избыточные серверы, базы данных, сетевые устройства и другие компоненты инфраструктуры, работающие параллельно. Например, активация механизма горячего резерва позволяет мгновенно переключаться на запасной узел при отказе основного компонента.

Основные преимущества: повышается доступность системы, сокращается время реакции на аварийные ситуации.

2. Географическая распределенность дублируемых узлов.

Размещение дублирующих элементов в различных географических зонах, удаленных друг от друга. Это снижает риск одновременного отказа нескольких ключевых узлов вследствие природных катастроф, атак хакеров или иных чрезвычайных ситуаций.

Основные преимущества: устойчивость к локальным происшествиям, улучшенная защита от внешних воздействий.

3. Мониторинг и автоматическое обнаружение неисправностей.

Автоматизированные инструменты постоянного мониторинга состояния каждого узла позволяют своевременно выявлять отклонения и предупреждать инциденты еще до возникновения серьезных проблем. [2-3]

Основные преимущества: быстрое реагирование на неисправности, минимизация риска потери данных и нарушений непрерывности бизнеса.

4. Регулярные проверки готовности дублированных решений.

Проведение периодического тестирования дублирующих подсистем путем планового отключения основных компонентов имитирует реальные условия эксплуатации и проверяет работоспособность резервных ресурсов.

Основные преимущества: постоянная готовность дублирующих элементов, своевременное выявление слабых мест и недостатков архитектуры.

Для успешного внедрения метода дублирования подсистем в системах защиты информации важно соблюдать определенные шаги и подходы. Ключевые этапы процесса внедрения:

Этап 1: Анализ существующей инфраструктуры.

Перед внедрением метода дублирования необходимо провести детальный аудит текущих технических ресурсов и архитектурных особенностей вашей системы. Проверить состояние используемых физических и виртуальных серверов, сетей, хранилищ данных и прочих компонентов. Определить слабые места и наиболее уязвимые участки сети. Оценить потенциальные угрозы и риски, связанные с авариями, взломами и отказами оборудования.

Этап 2: Выбор стратегии дублирования.

Существует несколько стратегий дублирования подсистем, каждая из которых имеет свои особенности и подходит для конкретных сценариев:

Активно-пассивная стратегия: один экземпляр постоянно функционирует, а второй ожидает своей очереди активации в случае аварии первого.

Активно-активная стратегия: оба экземпляра функционируют одновременно, распределяя нагрузку между собой.

Географически распределенная система: дублируемые ресурсы находятся в разных географических точках, уменьшая влияние локальных происшествий.

Этап 3: Проектирование архитектуры.

Проектировать архитектуру стоит таким образом, чтобы минимизировать возможные точки отказа и обеспечить быстрое переключение между основными и резервными элементами. Использовать специализированные решения для балансировки нагрузки и автоматического перенаправления трафика при выходе одного из узлов из строя. Применять механизмы хранения конфигураций и протоколов взаимодействия между элементами системы.

Этап 4: Тестирование и проверка.

После разработки проекта необходимо провести тщательное тестирование дублирующей системы:

Имитация реальных условий работы, проверка возможности быстрого перехода на резервные узлы, отработка сценария запуска при возникновении неполадок в основной системе.

Тестирование должно выявить любые недостатки и убедиться в работоспособности системы в экстремальных ситуациях.

Этап 5: Внедрение и мониторинг.

Важно контролировать процесс миграции данных и настроек, регулярно проверять корректность функционирования дублирующих элементов. Следует настроить системы мониторинга для оперативного выявления отклонений и ошибок, а также организовать процедуры регулярного анализа состояния системы и внесения изменений по мере необходимости.

Рекомендации по успешному внедрению.

Выбор оптимального уровня дублирования. Не обязательно дублировать абсолютно все оборудование, можно выбрать важные модули и системы, требующие повышенной защищенности.

Обучение персонала. Сотрудники, обслуживающие инфраструктуру, должны четко понимать принципы работы дублированных систем и уметь быстро реагировать на нестандартные ситуации.

Постоянное улучшение процессов. После завершения этапа внедрения следует продолжать анализировать работу системы, вносить необходимые усовершенствования и устранять возникающие проблемы.

Модель дублирования подсистем в защите информации представляет собой организационно-техническое решение, направленное на обеспечение непрерывности работы информационной системы даже при частичном выходе из строя отдельных ее компонентов. Такая модель основывается на принципе наличия дополнительного оборудования или программных модулей, готовых принять на себя выполнение функций вышедших из строя элементов. [3]

Ключевые элементы модели дублирования подсистем:

1. Основной рабочий модуль.

Это первичный ресурс, обеспечивающий нормальное функционирование информационной системы. Обычно это сервер, база данных, сетевое устройство или другое важное звено IT-инфраструктуры.

2. Резервный модуль.

Дополнительный компонент, аналогичный основному рабочему модулю, готовый немедленно заменить последний в случае его отказа. Существует две основных формы резервирования:

Горячий резерв: модуль постоянно готов к работе и подключен к сети, ожидая сигнала о переходе в активный режим.

Холодный резерв: резервный модуль отключен и должен пройти процедуру подготовки к запуску перед началом полноценной работы.

3. Система обнаружения неисправностей.

Специальный механизм контроля и диагностики, отслеживающий состояние обоих модулей. Он способен оперативно фиксировать

возникновение проблем в основном рабочем модуле и инициировать переход на резервный элемент.

4. Механизм переключения.

Механизм переключения определяет порядок действий при обнаружении неисправности. Возможны различные сценарии:

Автоматический перенос нагрузки на резервный модуль без участия оператора.

Предупреждение администратора о возникшей проблеме с возможностью ручного принятия решения.

Типовые схемы реализации моделей дублирования:

1. Active-Passive схема («основной + горячий резерв»).

Основной рабочий модуль активно обрабатывает запросы пользователей, пока резервный находится в состоянии ожидания. При выходе из строя основного модуля нагрузка сразу переходит на резервный, поддерживая непрерывность обслуживания.

Пример реализации: серверная инфраструктура с двумя серверами, где один сервер активно обслуживает клиентов, а второй готов вступить в действие при любом сбое.

2. Active-Active схема («двойная активность»).

Оба модуля функционируют одновременно, разделяя нагрузку между собой. Если один из них выходит из строя, оставшийся модуль берет на себя всю рабочую нагрузку.

Пример реализации: базы данных, хранящиеся на нескольких независимых серверах, работающих параллельно и осуществляющих взаиморезервирование.

Практические аспекты проектирования модели дублирования.

При проектировании модели дублирования стоит учитывать следующие моменты:

– технические характеристики оборудования и совместимость компонентов;

– время переключения на резервный модуль и возможная потеря данных;

– уровень автоматизации процесса переключения и необходимость вмешательства человека.

– стоимость приобретения и поддержки резервных элементов.

Таблица 1

Плюсы и минусы использования модели дублирования

Преимущества	Недостатки
Высокая надежность и стабильность работы системы	Дополнительные расходы на приобретение и эксплуатацию оборудования
Незначительные перерывы в обслуживании при отказах оборудования	Требуется грамотное проектирование и настройка механизма переключения
Повышенный уровень защиты от угроз и кибератак	Ограниченные возможности масштабирования при увеличении числа элементов

Модели дублирования подсистем являются важным инструментом повышения надежности и безопасности информационных систем. Их применение оправдано там, где необходима высокая степень бесперебойности и устойчивости к внешним воздействиям. Грамотное проектирование и правильная реализация обеспечивают значительную выгоду для организаций любого масштаба.

Список использованных источников:

1. Исмагилова А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 8 (116). С. 273–281.

2. Давлетова Д.Р. Дублирование в защите информации / Д.Р. Давлетова, И.А. Шагапов // Естественные и технические науки. 2024. № 12 (199). С. 266–304.

3. Шагапов И.А. Рекомпозиционный подход в защите информации / И.А. Шагапов, А.С. Исмагилова, И.В. Салов // Международный форум KAZAN DIGITAL WEEK – 2021: сборник материалов, Казань, 21–24 сентября 2021 г. Том Часть 1. Казань: ГБУ «НЦБЖД», 2021. С. 275–282.

4. Шагапов И.А. К механизму переключения состояний системы защиты информации при использовании рекомпозиционного подхода / И.А. Шагапов // Естественные и технические науки. 2023. № 12 (187). С. 300–304.

Davletova D.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A
Ufa University of Science and Technology, Ufa

BUILDING A MODEL OF SUBSYSTEM DUPLICATION IN INFORMATION SECURITY

Abstract. Information protection is a critically important task in many areas of human activity, from business to public administration. One of the ways to increase the reliability of information security is the duplication of subsystems that ensure the security of information resources. This work is devoted to the construction of a model of duplication of subsystems in information security.

Keywords: information protection, subsystem duplication, model construction.