# Динамическое ограничение доступа к данным

## Назначение шаблона

Шаблон предназначен для организации динамического ограничения доступа к данным (обеспечение невозможности одновременного доступа к доверенному и недоверенному хранилищу данных). Шаблон может быть применен для организации однократного доступа к доверенным данным в одном сеансе работы системы (между перезагрузками).

## Типовые цели безопасности

**Типовые цели безопасности при применении шаблона включают:**

- уменьшение поверхности атаки на данные (как правило, служебные и (или) конфигурационные) для которых действуют требования по их конфиденциальности и (или) целостности;
- обеспечение определенного режима доступа к данным.

## Предположения безопасности

Предположения безопасности включают доверие ядру безопасности, реализующему применение политики контроля доступа.

Предположения и условия, при которых шаблон не может быть применен: существует альтернативный канал доступа к данным, который позволяет обходить установленные на основе реализации шаблона ограничения доступа.

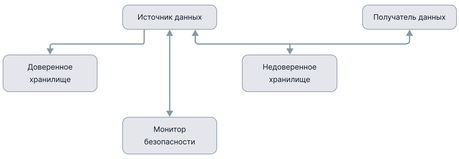
## Описание решения

**Элементы системы, реализующей шаблон:**

- источник данных;
- получатель данных;
- доверенное хранилище;
- недоверенное хранилище;
- монитор безопасности.

Взаимодействие элементов шаблона представлено на рисунке 1.

Рисунок 1 – Динамическое ограничение доступа к данным




**Алгоритм динамического ограничения доступа к данным на основе шаблона требует создания конечного автомата, который позволяет системе находиться в одном из двух состояний:**

1. Защищенном, когда источник данных имеет доступ только к доверенному хранилищу и не имеет доступ к внешней сети и другим компонентам системы;
2. Рабочем, когда ни один компонент не имеет доступа к доверенному хранилищу данныых.

**Алгоритм представляет собой следующую последовательность шагов:**

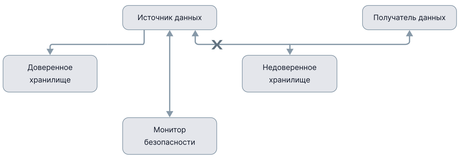
Шаг 1 — Система находится в защищенном состоянии. Источник данных имеет доступ к доверенному хранилищу и получает необходимые для работы конфигурации;

Шаг 2 — Источник совершает попытку обращения к недоверенному хранилищу;

Шаг 3 — Срабатывает политика, переводящая систему в рабочее состояние. Доступ к доверенному хранилищу запрещен для всех компонентов системы.

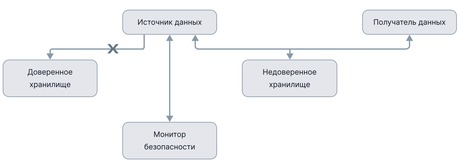
Система в защищенном состоянии представлена на рисунке 2.

Рисунок 2 – «Динамическое ограничение доступа к данным», система в защищенном состоянии




Система в рабочем состоянии представлена на рисунке 3.

Рисунок 3 – «Динамическое ограничение доступа к данным», система в рабочем состоянии




## Требования к технологии разработки элементов системы

Поскольку шаблон использует шаблон «Монитор», применяются требования к технологии, определенные для базового шаблона.

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

## Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона и шаблона «Монитор».

## Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

**Ключевые слова:**

- методология разработки;
- система;
- программное обеспечение;
- конструктивная информационная безопасность;
- требования безопасности информации;
- архитектура программного обеспечения;
- доверенная система;