

Безопасное обновление

Назначение шаблона

Шаблон предназначен для организации безопасного обновления системы и приложений через канал связи с удаленным сервером обновлений.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона: обеспечение целостности и аутентичности данных обновлений (бинарных образов, скриптов, конфигурационных данных обновлений и т.п.) в условиях доставки этих данных через каналы связи сетей общего доступа.

Предположения безопасности

Предположения безопасности отсутствуют.

Предположения и условия, при которых шаблон не может быть применен: наличие альтернативного канала доступа к хранилищу данных, который позволяет обходить установленные на основе реализации настоящего шаблона ограничения доступа.

Описание решения

Шаблон должен отвечать следующим требованиям:

- реализация шаблона должна обеспечивать аутентификацию сервера обновлений;
- реализация шаблона должна обеспечивать возможность отката обновления в случае, если оно неработоспособно;
- реализация шаблона должна обеспечивать проверку целостности, аутентичности и актуальности обновления;
- реализация шаблона должна обладать устойчивостью к атакам злоумышленника.

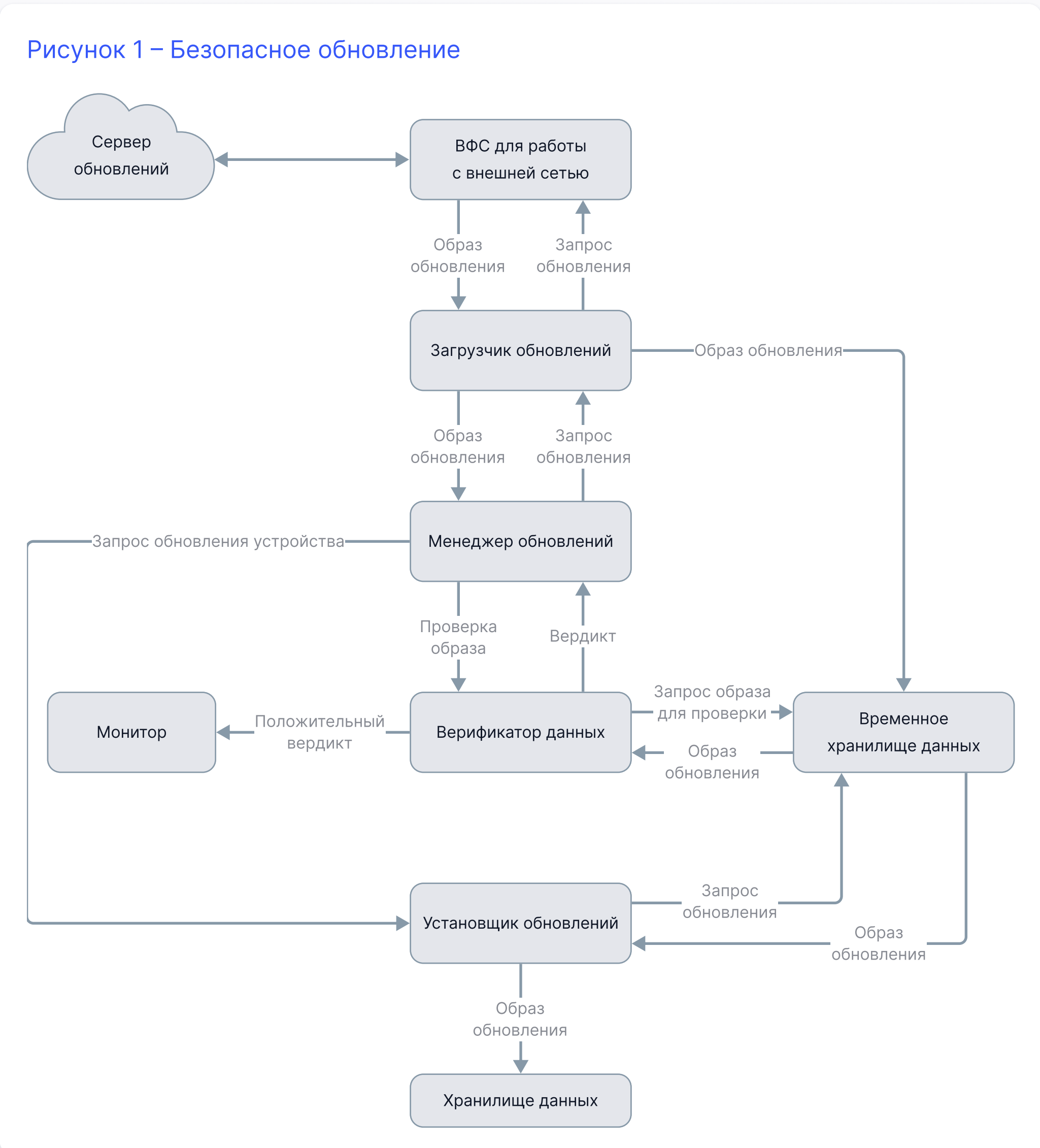
Элементы системы, реализующей шаблон:

- сервер обновлений - удаленный сервер, содержащий данные обновлений (бинарных образов, скриптов, конфигурационных данных обновлений и т.п.);
- элемент, реализующий обмен данными с внешней сетью (к примеру, реализующий ВФС для внешней сети);
- менеджер обновлений - элемент, управляющий процессом обновления и предоставляющий пользователю интерфейс управления обновлениями;
- загрузчик обновлений - элемент, обеспечивающий связь с сервером обновлений и загрузку обновления на устройство. Может выполнять проверку наличия обновлений при соответствующих настройках Менеджера обновлений;
- аутентификация сервера должна осуществляться по безопасному каналу связи, к примеру, организованного посредством реализации шаблона «Терминатор TLS»;
- временное хранилище обновления и связанных с ним метаданных (номер версии, ЭЦП, контрольная сумма), используется для изоляции обновления на время проверок;
- верификатор данных - элемент, осуществляющий проверку обновления в соответствии с заложенной логикой и обеспечивающий вынесение вердикта (положительный или отрицательный) по результатам проверки файла обновления и связанных с ним метаданных. Типовые проверки могут включать: целостность (проверка контрольной суммы), аутентичность (проверка цифровой подписи), номер версии;
- хранилище данных;
- монитор;
- установщик обновлений - компонент, осуществляющий запись в хранилище данных и должную установку обновления.

Разграничение доступа к Временному хранилищу данных и Хранилищу данных обеспечивается реализацией шаблона «Разделение потоков данных на уровне драйвера ресурсов».

Монитор реализуется на основе шаблона «Монитор».

Взаимодействие элементов шаблона представлено на рисунке 1.



Система может находиться в одном из трех состояний конечного автомата:

- 1 Хранилище доступно для записи файла обновления. В этом состоянии Временное хранилище данных доступно только для записи.
- 2 Хранилище запечатано. В этом состоянии Временное хранилище данных доступно только для чтения и только компонентом Верификатор данных. После верификации данные во Временном хранилище данных могут считаться доверенными (целостными, аутентичными, актуальными).
- 3 Хранилище верифицировано. В этом состоянии данные во Временном хранилище данных доступны только для чтения компонентом Установщик данных.

Алгоритм установки обновления, реализуемый на основе шаблона:

- | | | |
|-----|---|--|
| Шаг | 1 | Менеджер обновлений запрашивает проверку наличия обновлений у Загрузчика обновлений; |
| Шаг | 2 | Загрузчик обновлений проверяет наличие обновлений и при наличии актуальной версии скачивает обновление и сопутствующую мета-информацию во Временное хранилище данных; |
| Шаг | 3 | Загрузчик обновлений уведомляет Менеджера обновлений о загрузке файла обновления во Временное хранилище данных; |
| Шаг | 4 | После записи обновления во Временное хранилище данных система переходит в состояние запечатывания Временного хранилища данных; |
| Шаг | 5 | Менеджер обновлений запрашивает у Верификатора данных проверку файла обновления и метаданных; |
| Шаг | 6 | Верификатор данных читает данные из Временного хранилища данных, проводит проверку и в случае положительного вердикта передает данные в монитор; система переходит в состояние возможности передачи данных из Временного хранилища данных; |
| Шаг | 7 | В случае положительного вердикта Верификатор данных информирует Менеджера обновлений о том, что образ корректный; |
| Шаг | 8 | Менеджер обновлений передает в Установщик обновлений команду на обновление устройства; |
| Шаг | 9 | Установщик обновлений читает данные из Временного хранилища данных, выбирает один из разделов для записи обновлений, записывает файл обновлений и инициирует процедуру установки обновления. После передачи файла обновления Временное хранилище данных форматируется и переходит в стартовое состояние. |

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;

Необходимо реализовать подходы к обеспечению корректности верификации данных обновления, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода компонента, реализующего проверку целостности, аутентичности и актуальности данных обновления.

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.