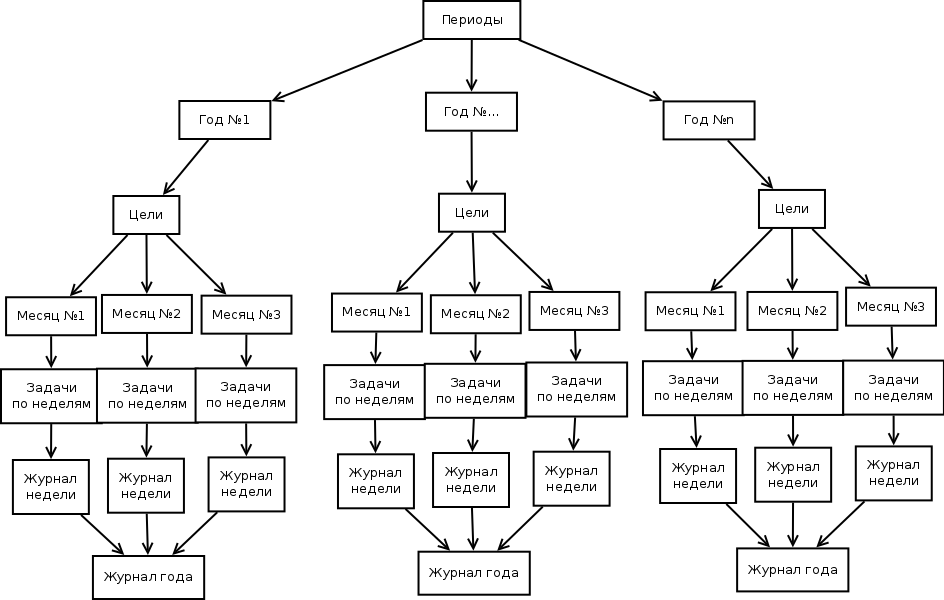
Описание:

Автоматизированная система по управлению задачами в режиме «12 недель в году». Основывается на одноименной методике управления целями.

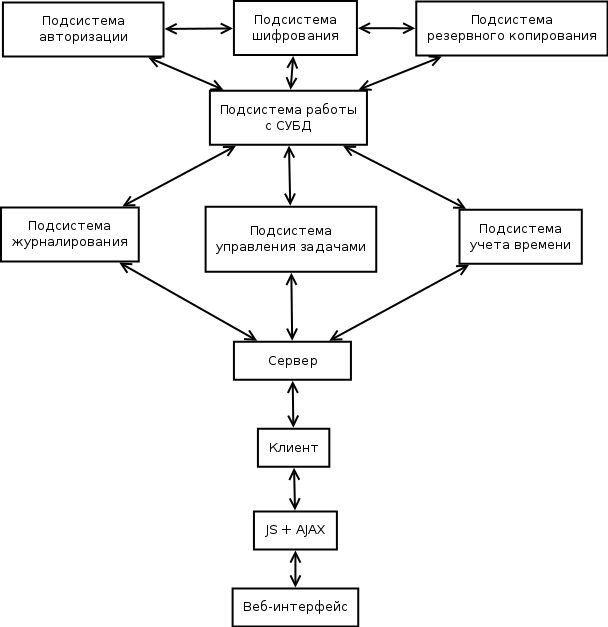
Автоматизированная система имеет клиент-серверную архитектуру и использует следующие технологии:

1. Протокол HTTP/HTTPS для обмена данными между клиентом и сервером
2. Клиентская часть под управлением браузера Mozilla Firefox/Google Chrome
3. Серверная часть под управлением веб-сервера Tomcat и java servlets.
4. Защита информации с помощью библиотек шифрования
5. Поддержание доступности информации за счет резервного копирования на текущий диск, а также на публичные дисковые пространства Yandex, Google, Microsoft
6. Поддержание целостности информации за счет аутентификации и авторизации действий с данными.

Схема работы по системе:



Логическая схема взаимодействия подсистем



Подсистема защиты состоит из трех основных компонентов:

1. Подсистема шифрования – для обеспечения конфиденциальности информации
2. Подсистема авторизации – для обеспечения целостности информации и защиты от незаконного искажения информации
3. Подсистема резервного копирования и восстановления – для обеспечения доступности информации.

Подсистема шифрования состоит из двух частей – шифрование канала связи между сервером и клиентом, и шифрование архивных данных на сервере СУБД. Методы шифрования канала обеспечиваются библиотекой SSL. Методы архивного шифрования обеспечиваются библиотекой JCA и собственными разработками.

Подсистема авторизации состоит из двух частей: уровень управления доступом и уровень аутентификации пользователя. Аутентификация осуществляется путем двухфакторной авторизации – с помощью пароля и с помощью сертификата открытого ключа. Аутентификация пользователя обеспечивает доступ к разрешенным данным, а также гарантирует, что данные останутся неизменными (для каждого блока данных создается электронная подпись, в случае неавторизованного изменения данных генерируется событие нарушения целостности и проводится резерное восстановление данных)

Подсистема резервного копирования предоставляет функции по созданию зашифрованных архивов и размещению их в публичные и частные хранилища (облачные, отдельный сервер, используемый диск). Рекомендуется использовать не менее трех различных источников данных. Каждый архив оснащается электронной подписью для гарантирования защищенности архивной информации от искажения.

Требования к подсистеме шифрования:

1. Шифрование канала осуществляется с помощью протокола SSL (настраивается непосредственно на Tomcat)
2. Сертификат SSL является самоподписанным и устанавливается на каждом клиенте перед использованием вручную.
3. Архивное шифрование является двуслойным и реализуется с помощью алгоритмов AES-256 и ГОСТ Р 34.13-2015. Реализация с помощью алгоритма ГОСТ является внутренней, внешне данные выглядят как зашифрованные с помощью AES-256
4. Ключи шифрования располагаются в базе данных в зашифрованном виде. Шифрование обеспечивается библиотекой pg\_crypto и базируются на алгоритме BlowFish
5. Архивное шифрование применяется к строковым данным БД, кроме системной информации, а также данных подсистемы авторизации. К ним используются методы хеширования по алгоритму ГОСТ Р серии 34 2012 года

Требования к подсистеме авторизации:

1. Аутентификация осуществляется с помощью пароля, подписанного с помощью закрытого ключа абонента.
2. Используется алгоритм подписи ГОСТ Р 34.10 2012 года.
3. Сертификат открытого ключа генерируется системой при первой регистрации и устанавливается на клиенте пользователя. Подписывается с помощью сертификата сервера, что обеспечивает дополнительную защиту от подмены сервера.
4. Электронная подпись применяется для аутентификации данных. Для этих целей на каждую строку в таблице SQL создается дополнительное поле, содержащее ЭЦП для всех полей таблицы. ЭЦП формируется с помощью ключа подписи абонента, который хранится в зашифрованном паролем контейнере, который хранится в таком виде на сервере. Формирование ЭЦП также происходит на сервере, но для подписания пользователь должен ввести пароль от контейнера.
5. Создание контейнера ключа ЭЦП осуществляется или с помощью апплета, который запускается на сервере, или с помощью отдельного ПО, который можно скачать с сервера. После генерации закрытого ключа и помещения его в архив он шифруется, копируется на сервер, а затем для него создается подписанный сертификат ЭЦП. Этот сертификат отправляется пользователю для сохранения на компьютере, а также сохраняется на сервере. Этот сертификат используется для проверки ЭЦП пользователя, а также для подтверждения подлинности самого сервера при дальнейшей эксплуатации.

Требования к подсистеме резервного копирования:

1. Резервное копирование реализуется с помощью средств языка Java. Резервная копия осуществляется для данных КАЖДОГО абонента в отдельности. В случае нарушения данных одного пользователя не возникает потребности откатывать данные всех пользователей, что минимизирует затраты. Резервные копии хранятся на жестком диске сервера, а также минимум в двух других различных источниках: на рабочей машине клиента, в одном из облачных хранилищ. Резервные копии защищаются с помощью средств шифрования данных.
2. Каждая резервная копия имеет параметры создания, а также ЭЦП для гарантии неизменности.
3. Восстановление данных осуществляется только для вызвавшего восстановление абонента. Сначала происходит проверка наличия всех копий на различных хранилищах, которые сравниваются путем сравнения ЭЦП для них. Выбирается та версия, которая имеет минимум 2 источника. В случае, если все версии различны, содержимое архивов распаковывается и предоставляется клиенту для выбора какой архив восстановить.