Оглавление

[Таблицы 2](#_Toc431731390)

[USERS 2](#_Toc431731391)

[SESSIONS 3](#_Toc431731392)

[ACCESS\_LIST 3](#_Toc431731393)

[MESSAGES 3](#_Toc431731394)

[CLIENT\_PAGE\_MAIN 4](#_Toc431731395)

[CLIENT\_PAGES 4](#_Toc431731396)

[DOCTOR\_PAGE\_MAIN 5](#_Toc431731397)

[DOCTOR\_NOTES 5](#_Toc431731398)

[PRESCRIPTIONS\_PAGES 6](#_Toc431731399)

[PRESCRIPTIONS\_REGISTRY 6](#_Toc431731400)

[SЕТS\_REGISTRY 7](#_Toc431731401)

[SЕТS\_ELEMENTS 7](#_Toc431731402)

[CALLBACK\_MSG 8](#_Toc431731403)

[REF\_DOCTOR\_SPECIALITIES 8](#_Toc431731404)

[REF\_MESSAGES\_TYPES 8](#_Toc431731405)

[REF\_PRESCRIPTIONS\_TYPES 9](#_Toc431731406)

[Диалоговые формы 9](#_Toc431731407)

[Регистрация пользователя 9](#_Toc431731408)

[Авторизация пользователя 9](#_Toc431731409)

[Карточка пациента 10](#_Toc431731410)

[Дополнительный раздел пациента 11](#_Toc431731411)

[Предоставление доступа к данным клиента 13](#_Toc431731412)

[Краткая карточка врача 14](#_Toc431731413)

[Используемые компоненты 14](#_Toc431731414)

# Таблицы

Таблицы модели данных:

ACCESS\_LIST реестр управления доступом и ключами

CLIENT\_PAGE\_MAIN главная страница данных клиента

CLIENT\_PAGES дополнительные страницы данных клиента

CALLBACK\_MSG сообщения обратной связи от пользователей

DOCTOR\_NOTES заметки врача по пациенту

DOCTOR\_PAGE\_MAIN главная страница данных врача

MESSAGES сообщения участникам

PRESCRIPTIONS\_PAGES состав назначений пациентам

PRESCRIPTIONS\_REGISTRY общий реестр назначений

SESSIONS список активных сессий пользователей

SETS\_ELEMENTS список элементов в составе комплексов назначений

SETS\_REGISTRY список комплексов назначений

USERS список логинов пользователей

Справочники:

REF\_DOCTOR\_SPECIALITIES перечень возможных специальностей врача

REF\_MESSAGES\_TYPES перечень возможных типов сообщений

REF\_PRESCRIPTIONS\_TYPES перечень категорий назначений

## USERS

Таблица логинов пользователей

|  |  |
| --- | --- |
| ID |  |
| LOGIN | Логин пользователя |
| PASSWORD | Первые 4 символа MD5-хэша пароля пользователя |
| EMAIL | E-mail пользователя |
| SIGN\_P\_KEY | Публичный ключ подписи |
| SIGN\_S\_KEY | Секретный ключ подписи |
| MSG\_KEY | Ключ шифрования копий исходящих сообщений |
| OPTIONS | Специальные права доступа |

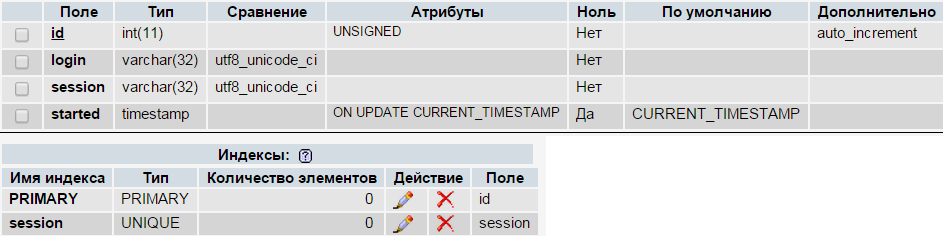


Специальные права доступа:

## SESSIONS

Список активных сессий пользователей

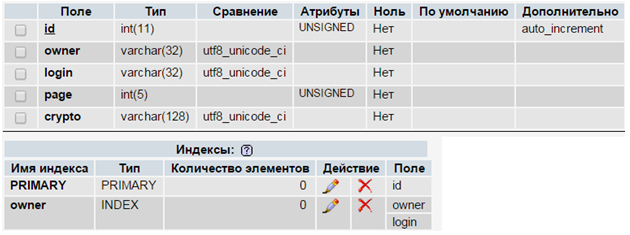
|  |  |
| --- | --- |
| ID |  |
| LOGIN | Логин пользователя → USERS.LOGIN |
| SESSION | Идентификатор сессии |
| STARTED | Дата/время регистрации сессии |



## ACCESS\_LIST

Реестр управления доступом и ключами

|  |  |
| --- | --- |
| ID |  |
| OWNER | Владелец страницы → USERS.LOGIN |
| LOGIN | Логин пользователя → USERS.LOGIN |
| PAGE | Номер страницы: 0 – главная страница |
| CRYPTO | Ключ шифрования страницы, зашифрованный на пароле LOGIN-пользователя |



## MESSAGES

Сообщения участникам

|  |  |
| --- | --- |
| ID |  |
| RECEIVER | Получатель → USERS.LOGIN |
| SENDER | Отправитель → USERS.LOGIN |
| SENT | Тайм-штамп отправки |
| TYPE | Тип сообщения → REF\_MESSAGES\_TYPES |
| TEXT | Текст сообщения |
| COPY | Копия текста сообщения (шифруется на ключе MSG\_KEY отправителя) |
| DETAILS | Прилагаемая техническая спецификация |
| READ | Метка прочтения |

## 

## CLIENT\_PAGE\_MAIN

Главная страница данных клиента

|  |  |
| --- | --- |
| ID |  |
| OWNER | Владелец страницы → USERS.LOGIN |
| CHECK | Контрольная строка проверки шифрования |
| NAME\_F | Фамилия |
| NAME\_I | Имя |
| NAME\_O | Отчество |
| REMARK | Примечание |



## CLIENT\_PAGES

Дополнительные страницы данных клиента

|  |  |
| --- | --- |
| ID |  |
| OWNER | Владелец страницы → USERS.LOGIN |
| PAGE | Номер страницы |
| TYPE | Тип страницы: client, prescription |
| CREATOR | Создатель страницы → USERS.LOGIN |
| CHECK | Контрольная строка проверки шифрования |
| TITLE | Заголовок страницы |
| REMARK | Примечание |
| PUBLISHED | Метка опубликования страницы |



## DOCTOR\_PAGE\_MAIN

Главная страница данных врача

|  |  |
| --- | --- |
| ID |  |
| OWNER | Владелец страницы → USERS.LOGIN |
| NAME\_F | Фамилия |
| NAME\_I | Имя |
| NAME\_O | Отчество |
| SPECIALITY | Специальность (список кодов) → REF\_DOCTOR\_SPECIALITIES |
| REMARK | Примечание |



## DOCTOR\_NOTES

Заметки врача по пациенту

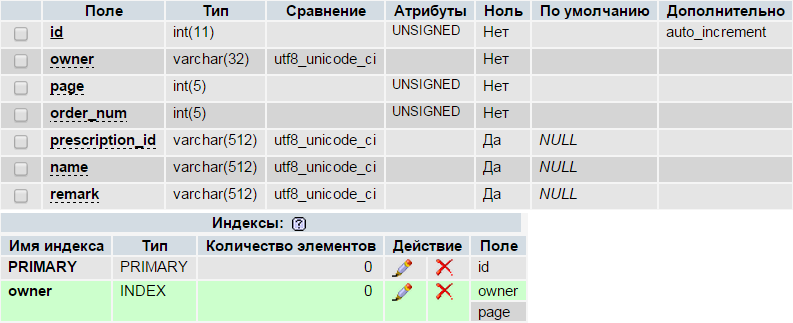
|  |  |
| --- | --- |
| ID |  |
| OWNER | Владелец страницы → USERS.LOGIN |
| CLIENT | Пациент → USERS.LOGIN |
| CHECK | Контрольная строка проверки шифрования |
| CATEGORY | Категория |
| REMARK | Примечание |

## 

## PRESCRIPTIONS\_PAGES

Состав назначений пациентам

|  |  |
| --- | --- |
| ID |  |
| OWNER | Пациент-владелец → USERS.LOGIN |
| PAGE | Номер страницы |
| ORDER\_NUM | Порядковый номер в списке |
| PRESCRIPTION\_ID | Идентификатор назначения → PRESCRIPTIONS\_REGISTRY |
| NAME | Название назначения |
| REMARK | Примечание |



## PRESCRIPTIONS\_REGISTRY

Общий реестр назначений

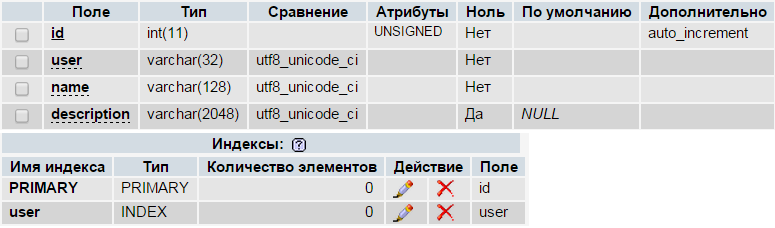
|  |  |
| --- | --- |
| ID |  |
| USER | Добавивший пользователь → USERS.LOGIN |
| TYPE | Тип назначения → REF\_PRESCRIPTIONS\_TYPES |
| NAME | Название |
| REFERENCE | Регистрационный индекс |
| DESCRIPTION | Основное описание |
| WWW\_LINK | Основная ссылка на внешнее описание |



## SЕТS\_REGISTRY

Список комплексов назначений

|  |  |
| --- | --- |
| ID |  |
| USER | Пользователь-владелец → USERS.LOGIN |
| NAME | Название |
| DESCRIPTION | Описание |



## SЕТS\_ELEMENTS

Реестр элементов в составе комплексов назначений

|  |  |
| --- | --- |
| ID |  |
| SET\_ID | Идентификатор набора→ SET\_REGISTRY |
| ORDER\_NUM | Порядковый номер |
| PRESCRIPTION\_ID | Идентификатор назначения → PRESCRIPTION\_REGISTRY |
| REMARK | Примечание |



## CALLBACK\_MSG

Сообщения обратной связи от пользователей

|  |  |
| --- | --- |
| ID |  |
| CREATED | Дата создания сообщения |
| SESSION | Сессия→ SESSIONS |
| CATEGORY | Категория сообщения |
| FORM | Имя диалоговой формы |
| MESSAGE | Текст сообщения |
| STATUS | Статус обработки сообщения |
| REMARK | Результат обработки сообщения |

## REF\_DOCTOR\_SPECIALITIES

Перечень возможных специальностей врача

|  |  |
| --- | --- |
| CODE | Код специальности |
| LANGUAGE | Язык описания специальности |
| NAME | Название специальности |



## REF\_MESSAGES\_TYPES

Перечень возможных типов сообщений

|  |  |
| --- | --- |
| CODE | Код типа сообщения |
| LANGUAGE | Язык описания типа сообщения |
| NAME | Название типа сообщения |

## REF\_PRESCRIPTIONS\_TYPES

Перечень возможных типов назначений

|  |  |
| --- | --- |
| CODE | Код типа назначения |
| LANGUAGE | Язык описания типа назначения |
| NAME | Название типа назначения |

# Диалоговые формы

## Регистрация пользователя

Файл - **registry.php**

При регистрации пользователя должны быть заданы следующие атрибуты:

* Логин
* Пароль
* Контактный e-mail
* Категория пользователя: Клиент, Врач или Тренер

На сервер передаются следующие данные:

* Логин
* Контактный e-mail
* Первые 4 символа MD5-хэша **пароля**
* **Ключ шифрования** главной страницы, зашифрованный на **пароле**
* Зашифрованная на **ключе шифрования** контрольная строка
* **Публичный ключ** электронной подписи
* **Секретный ключ** электронной подписи, зашифрованный на **пароле**

На сервере выполняются следующие действия:

* Проверка уникальности **логина**
* В таблице USERS создается запись о логине пользователя и его ключах электронной подписи
* В таблице ACCESS\_LIST создается запись об основном ключе шифрования пользователя
* Если при регистрации выбрано создание записи типа «Клиент»
* В таблице CLIENT\_PAGE\_MAIN создается запись о странице пользователя (без пользовательских данных)
* Если при регистрации выбрано создание записи типа «Врач»
* В таблице DOCTOR\_PAGE\_MAIN создается запись о странице пользователя (без пользовательских данных)

## Авторизация пользователя

Файл - **login.php**

При регистрации пользователя должны быть заданы следующие атрибуты:

* Логин
* Пароль

Перед отправкой данных на сервере **пароль** сохраняется на контексте окна.

На сервер передаются следующие данные:

* Логин
* Первые 4 символа MD5-хэша **пароля**

На сервере выполняются следующие действия:

* Проверка соответствия пароля-логина по таблице USERS
* Генерация **идентификатора сессии**
* В таблице SESSIONS создается запись о сеансе пользователя

На клиента передаются:

* Идентификатор сессии

**Идентификатор сессии** сохраняется на контексте окна.

## Карточка пациента

Файл – **client\_card.php**

Процедура обработки формы имеет две ветви исполнения:

* Отображение данных
* Сохранение данных

**Отображение данных** производится при первичном открытии формы (не задан POST-параметр **Check)** или при открытии формы пользователем – не владельцем данных (задан GET-параметр **Owner**). При этом выполняется следующая последовательность действий:

* По таблице SESSIONS идентифицируется сессия и ее владелец
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, устанавливается режим отображения **Read-only**.
* Из таблицы ACCESS\_LIST извлекается ключ шифрования карточки пациента и сохраняется на JavaScript-контексте формы
* Из таблицы CLIENT\_PAGE\_MAIN извлекаются данные полей формы, а также скрытое поле **Check**.
* Если не установлен режима **Read-only -** из таблиц ACCESS\_LIST и CLIENT\_PAGES извлекаются ключи и заголовки дополнительных страниц пациента и из них формируется список ссылок на дополнительные страницы пациента. По результатам выборки также определяется номер следующей дополнительной страницы, который сохраняется на JavaScript-контексте и используется при формировании ссылки «Создать новый раздел».
* Для режима **Read-only** добавляется вызов JavaScript-процедуры, которая отключает все активные кнопки и ссылки на странице.
* **На форме** производится:
* расшифровка данных в полях
* формирование ссылки «Создать новый раздел».

**Сохранение данных** производится при клике по кнопке «Сохранить» (задан POST-параметр **Check)**. При этом выполняется следующая последовательность действий:

* **На форме** производится шифрование данных в видимых полях.
* По таблице SESSIONS идентифицируется сессия и ее владелец
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, используется ветвь **«Отображение данных»** с режимом отображения **Read-only**.
* Из таблицы ACCESS\_LIST извлекается ключ шифрования карточки пациента и сохраняется на JavaScript-контексте формы
* Данные из полей формы сохраняются в таблицу CLIENT\_PAGE\_MAIN, они же возвращаются обратно - на форму.
* Из таблиц ACCESS\_LIST и CLIENT\_PAGES извлекаются ключи и заголовки дополнительных страниц пациента – из них формируется список ссылок на дополнительные страницы пациента. По результатам выборки также определяется номер следующей дополнительной страницы, который сохраняется на JavaScript-контексте и используется при формировании ссылки «Создать новый раздел».
* **На форме** (при возврате после сохранения) производится:
* расшифровка данных в полях
* формирование ссылки «Создать новый раздел».

## Дополнительный раздел пациента

Файл – **client\_page.php**

Процедура обработки формы имеет четыре ветви исполнения:

* Создание нового раздела
* Первое сохранение нового раздела
* Отображение данных
* Сохранение отредактированных данных

**Создание нового раздела** производится при клике по ссылке «Создать новый раздел» (задан GET-параметр **NewPage**, не задан POST-параметр **Check)**. При этом выполняется следующая последовательность действий:

* По таблице SESSIONS идентифицируется сессия и ее владелец
* Формируется форма с незаполненными полями.
* Для скрытого поля **Update** устанавливается значение «**Insert**»

**Первичное сохранение нового раздела** производится при первом клике по кнопке «Сохранить» для нового раздела (задан POST-параметр **Check,** POST-параметр **Update=**«**Insert**»). При этом выполняется следующая последовательность действий:

* **На форме**
* генерируется ключ шифрования
* генерируется значение поля **Check**
* производится шифрование значения поля **Check** и данных в видимых полях.
* По таблице SESSIONS идентифицируется сессия и ее владелец
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, используется ветвь **«Отображение данных»** с режимом отображения **Read-only**.
* В таблицу ACCESS\_LIST вставляется новая запись с ключом шифрования раздела данных
* В таблицу CLIENT\_PAGES вставляется новая запись со значениями из полей формы, они же возвращаются обратно - на форму.
* Из таблицы ACCESS\_LIST извлекается ключ шифрования раздела данных и сохраняется на JavaScript-контексте формы
* По результатам выборки из таблицы CLIENT\_PAGES определяется номер следующей дополнительной страницы, который сохраняется на JavaScript-контексте и используется при формировании ссылки «Создать новый раздел».
* Для скрытого поля **Update** устанавливается значение «**Update**»
* **На форме** (при возврате после сохранения) производится:
* расшифровка данных в полях
* формирование ссылки «Создать новый раздел».

**Отображение данных** производится при первичном открытии формы (не задан POST-параметр **Check)** или при открытии формы пользователем – не владельцем данных (задан GET-параметр **Owner**). При этом выполняется следующая последовательность действий:

* По таблице SESSIONS идентифицируется сессия и ее владелец
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, устанавливается режим отображения **Read-only**.
* Из таблицы ACCESS\_LIST извлекается ключ шифрования раздела данных и сохраняется на JavaScript-контексте формы
* Если не установлен режима **Read-only -** по результатам выборки из таблицы CLIENT\_PAGES определяется номер следующей дополнительной страницы, который сохраняется на JavaScript-контексте и используется при формировании ссылки «Создать новый раздел».
* Из таблицы CLIENT\_PAGES извлекаются данные полей формы, а также скрытое поле **Check**.
* Для режима **Read-only** добавляется вызов JavaScript-процедуры, которая отключает все активные кнопки и ссылки на странице.
* Для скрытого поля **Update** устанавливается значение «**Update**»
* **На форме** производится:
* расшифровка данных в полях
* формирование ссылки «Создать новый раздел».

**Сохранение отредактированных данных** производится при клике по кнопке «Сохранить» (задан POST-параметр **Check**,POST-параметр **Update=**«**Update**»**)**. При этом выполняется следующая последовательность действий:

* **На форме** производится шифрование данных в видимых полях.
* По таблице SESSIONS идентифицируется сессия и ее владелец.
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, устанавливается режим отображения **Read-only**.
* Определяется соответствие владельца сессии и владельца данных, а в случае их различия, используется ветвь **«Отображение данных»** с режимом отображения **Read-only**.
* Данные из полей формы сохраняются в таблицу CLIENT\_PAGES, они же возвращаются обратно - на форму.
* Из таблицы ACCESS\_LIST извлекается ключ шифрования раздела данных и сохраняется на JavaScript-контексте формы
* По результатам выборки из таблицы CLIENT\_PAGES определяется номер следующей дополнительной страницы, который сохраняется на JavaScript-контексте и используется при формировании ссылки «Создать новый раздел».
* Для скрытого поля **Update** устанавливается значение «**Update**»
* **На форме** (при возврате после сохранения) производится:
* расшифровка данных в полях
* формирование ссылки «Создать новый раздел».

## Предоставление доступа к данным клиента

Файл – **pages\_access.php**

Процедура обработки формы имеет две ветви исполнения:

* Отображение данных
* Выполнение операции «Предоставить доступ»

**Отображение данных** производится при первичном открытии формы и после выполнения операции «Предоставить доступ». При этом выполняется следующая последовательность действий:

* По таблице SESSIONS идентифицируется сессия и ее владелец
* Из таблицы REF\_DOCTOR\_SPECIALITIES извлекается список специальностей врачей и сохраняется на JavaScript-контексте.
* Из таблицы DOCTOR\_PAGE\_MAIN извлекается список врачей и сохраняется на JavaScript-контексте.
* Из таблиц ACCESS\_LIST и USERS извлекаются ключ шифрования главной страницы и секретный ключ подписи пациента, соответственно, и сохраняется на JavaScript-контексте.
* Из таблиц CLIENT\_PAGES и ACCESS\_LIST извлекается список заголовков дополнительных страниц пациента и их ключей шифрованию и сохраняется на JavaScript-контексте.
* **На форме** производится:
* формирование списка страниц пользователя с расшифровкой заголовков
* формирование списка значений для поля «Специальность»
* формирование списка врачей

**Выполнение операции «Предоставить доступ»** производится при первом клике по кнопке «Предоставить доступ» (задан POST-параметр **Receiver**). При этом выполняется следующая последовательность действий:

* **На форме**
* составляется список номеров отмеченных для доступа страниц вместе с их расшифрованными ключами - формируется спецификация доступа
* с контекста формы «Краткая карточка врача» из фрейма «Details» извлекается открытый ключ подписи врача-получателя доступа
* спецификация доступа шифруется RSA на секретном ключе пациента и открытом ключе врача
* По таблице SESSIONS идентифицируется сессия и ее владелец
* В таблицу MESSAGES заносится новая запись с компонентами сообщения
* Далее обработка идет по ветви «Отображение данных»

## Краткая карточка врача

Файл – **doctor\_details.php**

Процедура обработки формы имеет единственную ветвь исполнения:

* Отображение данных

Выполняется следующая последовательность действий:

* По таблице SESSIONS идентифицируется сессия и ее владелец
* Из таблиц DOCTOR\_PAGE\_MAIN и USERS извлекаются реквизиты врача и открытый ключ подписи врача.
* Из таблицы REF\_DOCTOR\_SPECIALITIES извлекается список кодов специальностей, в соответствии с которым производится расшифровка специальностей врача
* Реквизиты врача выдаются в видимые поля формы, а логин врача и открытый ключ его подписи – в скрытые поля Login и Sign\_key, соответственно.

# Используемые компоненты

https://code.google.com/p/crypto-js/#DES,\_Triple\_DES