

uniteller

self @ online & onlife

Технический порядок. Интернет-эквайринг

Всего листов: 77

Версия 1.20 rev. 5
Дата изменения: 2013-03-12

Москва, 2013

Содержание:

Термины и определения	4
Введение	6
1. Функциональные возможности, предоставляемые в рамках услуги «Интернет-эквайринг»	6
2. Подключение точки продажи.....	6
2.1. Подключение магазина.....	6
2.2. Отключение магазина	7
3. Тестовое подключение	7
3.1. Назначение тестового подключения и подготовка магазина.....	7
3.2. Параметры тестового подключения	8
3.3. План проведения тестирования	9
3.3.1. Варианты тестирования.....	9
3.3.2. Тест успешной оплаты	9
3.3.3. Тест неуспешной оплаты	10
4. Порядок выполнения основных операций.....	11
4.1. Операция продажи	11
4.1.1. Общая последовательность операции продажи.....	11
4.1.2. Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры.....	14
4.1.3. Способы вывода страницы оплаты. Интеграция страницы оплаты на сайт интернет-магазина	19
4.1.4. Страница оплаты на сайте Uniteller в зависимости от переданных значений параметров MeanType и EMoneyType	20
4.1.5. Платёж в фоновом режиме	24
4.1.6. Платёж через внешнюю форму	27
4.2. Преавторизация платежа.....	28
4.2.1. Общее описание	28
4.2.2. Проведение преавторизации платежа.....	28
4.2.3. Подтверждение платежа, проведённого с преавторизацией.....	29
4.3. Рекуррентные платежи	31
4.3.1. Общее описание	31
4.3.2. Особенности рекуррентных платежей и принципы их проведения в системе Uniteller	31
4.3.3. Проведение рекуррентных платежей	32
4.4. Регистрация банковских карт для повторных платежей.....	34
4.4.1. Общая информация о регистрации банковских карт	34
4.4.2. Для чего нужна регистрация карт и типичные механизмы привязки	34
4.4.3. Безопасность и разделение ответственности.....	35
4.4.3.1. Данные карты, «маска» и её статусы.....	35
4.4.3.2. Уникальный идентификатор покупателя Customer_IDP	35
4.4.4. Типичные сценарии использования	35
4.4.4.1. Оплата картой без авторизации в интернет-магазине.....	35
4.4.4.2. Первая оплата картой после авторизации в интернет-магазине	36
4.4.4.3. Последующие оплаты зарегистрированной картой	36
4.4.4.4. Выбор зарегистрированной карты на стороне Uniteller при оплате.....	37
4.4.4.5. Регистрация карты по случайной сумме	38
4.4.4.6. Выбор зарегистрированной карты на стороне интернет-магазина при оплате.....	40
4.4.4.7. Удаление регистрации карты	40
4.4.4.8. Блокировка зарегистрированной карты.....	40
4.4.4.9. Разблокировка зарегистрированной карты	40
4.4.4.10. Изменение статуса регистрации карты	40
4.4.4.11. Получение списка зарегистрированных карт.....	42
4.4.4.12. Привязка карт по реестру	44
4.5. Отмена платежа и возврат средств.....	45
4.5.1. Суть терминов «отмена платежа» и «возврат средств». Особенности реализации отмен у разных банков-эквайеров	45
4.5.2. Запрос отмены платежа и возможные форматы ответа.....	46
4.5.2.1. Общий вид запроса отмены платежа	46
4.5.2.2. Особенности отмены платежа для эквайера ЗАО «КОКК».....	48

4.5.2.3. Особенности отмены платежа электронной валютой Яндекс.Деньги	48
4.5.3. Отмена платежа с преавторизацией	49
4.5.4. Возврат средств	49
4.6. Получение результатов авторизации	49
4.6.1. Уведомление сервера интернет-магазина о статусе оплаты	49
4.6.2. Запрос результата авторизации	51
4.6.2.1. Общий вид запроса результата авторизации	51
4.6.2.2. Особенности запроса результата авторизации платежа электронной валютой	54
4.6.2.3. Особенности запроса результатов авторизации платежа для оплат авиабилетов через ГДС	55
4.6.3. Ограничения при осуществлении запроса результатов авторизации	55
4.7. Автоматический контроль статусов заказов	55
4.7.1. Общая информация об автоматическом контроле статуса заказов	55
4.7.2. Протокол запроса статуса заказа с сервера мерчанта	58
5. Порядок работы в Личном кабинете	58
5.1. Просмотр списка операций	58
5.2. Возврат средств из Личного кабинета	58
6. Техническая поддержка пользователей	59
7. Справочная информация	60
7.1. Возможные поля параметра S_FIELDS	60
7.2. Значения поля response_code	61
7.3. Форматы ответов	62
7.3.1. Запрос состояния транзакции	62
7.3.1.1. Формат сообщения об ошибке	62
7.3.1.2. CSV	62
7.3.1.3. “В скобках”	62
7.3.1.4. WDDX	63
7.3.1.5. XML	64
7.3.1.6. SOAP	66
7.3.2. Запрос отмены платежа	67
7.3.2.1. CSV	67
7.3.2.2. WDDX	67
7.3.2.3. XML	68
7.3.2.4. SOAP	69
7.3.3. Запрос рекуррентного платежа	71
7.3.3.1. CSV	71
7.4. Примеры кода на PHP	72
7.4.1. Получение отчёта о выполненной транзакции через SOAP	72
7.4.2. Пример PHP-кода на странице оплаты мерчанта	73
7.4.3. Пример PHP-кода запроса результата авторизации на сервере Uniteller	74
7.4.4. Пример PHP-кода отмены платежа по RRN	75
7.5. Необходимость подписания формы оплаты	77
Приложение 1. Дополнительные функции для оплаты авиаперевозок	
Приложение 2. Регистрация банковских карт для повторных платежей. Передача Банком-эмитентом реестра выпущенных карт при регистрации карт «по реестру»	

Термины и определения

Термин	Определение
CVV2 (CVC2)	CVV2 (Card Verification Value 2) — трёхзначный или четырёхзначный код проверки подлинности карты платёжной системы Visa. Аналогичный защитный код для карт MasterCard носит название Card Validation Code 2 (CVC2).
GDS	см. ГДС
HTTP	Протокол передачи гипертекста (Hypertext transfer protocol). Открытый протокол для передачи данных в сети Интернет.
ID	Идентификатор (identity).
IP-адрес	Сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
PAN	Номер платёжной карты (Primary Account Number), кредитной или дебетовой, которая идентифицирует платёжную систему и персональный счёт держателя карты.
PCI DSS	Payment Card Industry Data Security Standard (Стандарт защиты информации в индустрии платёжных карт), набор требований к безопасности данных держателей карт, разработанный международными платёжными системами VISA, MasterCard, American Express, JCB, Discover.
Uniteller	ЗАО «Предпроцессинговый расчетный центр».
Авторизация	(При доступе в Личный кабинет Uniteller) — процесс предоставления пользователю, программе или процессу прав доступа или других полномочий на выполнение некоторых действий. (При платеже по банковской карте) — процедура получения разрешения эмитента на совершение операции оплаты по карте (часто термином «авторизация» обозначается операция блокировки средств на карте Покупателя).
ГДС	Глобальная дистрибьюторская система (Global Distribution System, GDS) — информационная система, предоставляющая информацию о рейсах авиакомпаний и возможность бронирования авиабилетов. Мёрчанты (Агентства), работающие на рынке услуг по бронированию авиабилетов, обычно интегрированы с одной или несколькими ГДС.
Держатель карты или Покупатель	Посетитель электронного магазина Мёрчанта с целью ознакомления с ассортиментом (услугами) и осуществления покупки.
Заказ	Заказ в системе Uniteller является сущностью, соответствующей заказу в интернет-магазине Мёрчанта. Ключевыми параметрами заказа являются принадлежность к интернет-магазину Мёрчанта, номер заказа, сумма, статус.
Магазин; интернет-магазин	Сайт интернет-магазина Мёрчанта, на котором производится приём платежей от Покупателей и через программное обеспечение которого идёт обмен данными с системой Uniteller.
Мёрчант	Организация, заключившая с Uniteller договор об оказании услуг по информационно-технологическому сопровождению приёма банковских карт.

Термин	Определение
Операция	Операция в системе Uniteller является сущностью, соответствующей попытке оплаты заказа выбранным способом (оплата банковской картой или оплата с помощью электронной платёжной системы).
Пароль	Секретная строка символов, которая служит для аутентификации Покупателя.
Протокол	Согласованный метод обмена данными, используемый в сетях.
Рекуррентный платёж	Платёж, осуществляемый в автоматическом режиме без участия Держателя карты с его согласия и по заранее утверждённому расписанию.
Сервер	Компьютер, предоставляющий сервисы другим компьютерам сети.

Введение

Этот документ является техническим порядком, содержащим необходимую и достаточную информацию для подключения и последующего бесперебойного получения услуги «Интернет-эквайринг», предоставляемой компанией Uniteller.

Документ предназначен техническим специалистам, обеспечивающим подключение на интернет-ресурсах клиентов услуги «Интернет-эквайринг».

1. Функциональные возможности, предоставляемые в рамках услуги «Интернет-эквайринг»

Интернет-эквайринг — это приём к оплате платёжных карт через Интернет с использованием специально разработанного web-интерфейса, позволяющего провести расчёты в интернет-магазинах.

В рамках услуги «Интернет-эквайринг» процессинговый центр Uniteller предоставляет своим клиентам следующие возможности:

- Обеспечение на сайте интернет-магазина клиента возможности следующих видов оплат:
 - банковскими картами всех основных международных платёжных систем (VISA, MasterCard, JCB, Diners Club, ChinaUnionPay);
 - через популярные электронные платёжные системы: PayPal, QIWI Кошелек, WebMoney WMR, Деньги@Mail.Ru, Евросеть, Яндекс.Деньги;
 - со счёта мобильного телефона (Мобильный платёж (Билайн, Мегафон, МТС)).
- Возможность глубокой кастомизации страницы оплаты, демонстрируемой Покупателю.
- Проведение платежей с преавторизацией.
- Поддержка рекуррентных платежей.
- Регистрация банковских карт для упрощения последующих платежей.
- Автоматический контроль статусов заказов.
- Интеграция с основными системами бронирования и продажи авиабилетов.
- Личный кабинет системы Uniteller с широкими возможностями мониторинга и администрирования платежей.

2. Подключение точки продажи

2.1. Подключение магазина

Точка продажи Мёрчанта может быть подключена только при условии подключения Мёрчанта к системе Uniteller.

Мёрчант считается подключенным к системе Uniteller при выполнении следующих условий:

- С Uniteller заключён договор об оказании услуг по информационно-технологическому сопровождению приёма банковских карт.
- С Банком-эквайером заключён договор об обслуживании держателей банковских карт.
- От Uniteller получен идентификатор **MERCHANT_ID**.

Если данные о точке продажи, указанные в заявлении, соответствуют правилам Uniteller, Банка-Эквайера и Международных платёжных систем, Uniteller переходит к подключению точки продажи, регистрируя точку продажи на сервере Uniteller с присвоением идентификатора **TERMINAL_ID**.

Для подключения точки продажи к системе Uniteller выполняются следующие действия:

- Ответственный менеджер отдела продаж Uniteller добавляет в систему Uniteller следующую информацию:
 - Запись с параметрами заключённого договора об оказании услуг по информационно-технологическому сопровождению приёма банковских карт.
 - Записи о торговых точках (интернет-магазинах), подключаемых в рамках данного договора, с присвоением идентификатора **TERMINAL_ID**. При подключении каждой торговой точки Мёрчанту передаётся её идентификатор **Shop_IDP**¹.
- Для подключения возможности оплат товаров и/или услуг валютами электронных платёжных систем заключается дополнительный договор на обслуживание электронных валют и информация о нём добавляется в систему Uniteller по представлению менеджера отдела продаж Uniteller.

2.2. Отключение магазина

Под отключением магазина подразумевается прекращение предоставления услуг сервиса Uniteller, в том числе предоставления информации в Личном кабинете о данной торговой точке (магазине) Мёрчанта.

Uniteller может осуществить блокировку или отключение точки продажи по письменному заявлению Мёрчанта.

3. Тестовое подключение

3.1. Назначение тестового подключения и подготовка магазина

Тестовое подключение интернет-магазина Мёрчанта к системе Uniteller является обязательным этапом предоставления услуги «Интернет-эквайринг» и имеет следующее назначение:

- Начальная регистрация торговой точки Мёрчанта в системе Uniteller. (Номер магазина присваивается Uniteller каждому интернет-магазину Мёрчанта в момент подключения точки продажи).
- Реализация в программном обеспечении сайта интернет-магазина алгоритмов обмена данными с сайтом Uniteller и проверка правильности их работы.
- Знакомство персонала Мёрчанта с функциональными возможностями Личного кабинета системы Uniteller.
- Организационная подготовка персонала Мёрчанта к обеспечению процесса приёма оплат по банковским картам.

Тестовое подключение осуществляется только на тестовом сервере Uniteller.

¹ **Примечание:** Идентификатор точки продажи в Личном кабинете называется **Uniteller Point ID**. Следовательно, значение **Shop_IDP** в Личном кабинете указано на странице «Точки продажи компании» (пункт меню «Точки продажи») в столбце **Uniteller Point ID**. При возникновении проблем просим обращаться в Службу технической поддержки Uniteller.

Для проведения тестового подключения Uniteller передает Мёрчанту следующую информацию:

- Данные о тестовых картах с сопутствующей информацией, необходимой для проведения тестирования (см. п. 3.3.2 «Тест успешной оплаты» на стр. 9 и п. 3.3.3 «Тест неуспешной оплаты» на стр. 10).
- Идентификатор (номер) тестового магазина.
- Ключевые адреса на тестовом сервере Uniteller (см. п. 3.2 «Параметры тестового подключения» ниже).
- Логин и пароль для доступа в Личный кабинет тестового сервера Uniteller.
- Авторизационные данные (логин и пароль), используемые в запросе результатов авторизации (эти данные указаны в Личном кабинете тестового сервера Uniteller в разделе «**Параметры авторизации**»).
- План проведения тестирования (см. п. 3.3 «План проведения тестирования» на стр. 9).

Обращаем ваше внимание на то, что для тестирования необходимо использовать только данные тестовых пластиковых карт Uniteller. Использование данных реальных пластиковых карт для тестирования запрещено.

Для осуществления тестового подключения точки продажи Мёрчанта к системе Uniteller необходимо ознакомиться с общей последовательностью проведения операции продажи (см. п. 4.1.1 «Общая последовательность операции продажи» на стр. 11) и разместить на странице сайта интернет-магазина форму оплаты (см. п. 4.1.2 «Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры» на стр. 14).

При подготовке к текстовому подключению и проведению тестирования рекомендуется поддерживать контакт со Службой технической поддержки Uniteller для согласования действий и решения текущих вопросов (координаты Службы технической поддержки указаны в п. 6 «Техническая поддержка пользователей» на стр. 59).

3.2. Параметры тестового подключения

Для проведения тестирования необходимо использовать следующие адреса серверов:

- В качестве адреса формы оплаты платёжного шлюза (URL-адрес, который указывается в HTML-форме оплаты на сайте интернет-магазина): <https://test.wpay.uniteller.ru/pay/>
- Для получения результатов авторизации: <https://test.wpay.uniteller.ru/results/>
- Для получения WSDL-файла: <https://test.wpay.uniteller.ru/results/wsdl/>
- Адрес Личного кабинета тестового сервера Uniteller: <https://test.lk.uniteller.ru/>

Обращаем ваше внимание на то, что тестовый сервер Uniteller, по сравнению с «боевым», обладает ограниченной функциональностью и предоставляет только базовые функции платёжного сервиса Uniteller, достаточные для тестирования интеграции.

Тестовый сервер Uniteller предоставляет следующие базовые функции:

- Проведение авторизации платежа (блокировка средств на платёжной карте).
- Проведение отмены авторизации платежа.
- Обработка запроса статуса авторизации платежа.
- Регистрация карты в системе Uniteller по успешному платежу.
- Проведение платежа по карте, предварительно зарегистрированной в системе Uniteller.

Все остальные функциональные возможности, доступные на «боевом» сервере Uniteller (например, преавторизация платежа, оплата электронными валютами, проведение списания средств), на тестовом сервере не поддерживаются.

Так как при проведении тестирования работа с электронными валютами не поддерживается, в тестовом запросе на оплату параметры **MeanType** и **EMoneyType** не должны передаваться или должны иметь пустые значения (в соответствии с алгоритмом вычисления обязательного параметра **Signature**, приведённым в табл. 1 на стр. 15, вместо значений параметров **MeanType** и **EMoneyType** подставляется значение хэш-функции md5 от пустой строки).

3.3. План проведения тестирования

3.3.1. Варианты тестирования

Uniteller предоставляет Мёрчанту два теста:

1. **Тест успешной оплаты** — оплата тестовой картой № 1 с корректными параметрами. Этот тест позволяет проверить случай, при котором Покупатель на сайте Мёрчанта производит оплату картой с корректными параметрами — оплата на сайте принимается, сайт реагирует правильным образом (выдаёт товар или предоставляет услугу, показывает Покупателю страницу успешной оплаты и т. д.).
2. **Тест неуспешной оплаты** — оплата тестовой картой № 2 с некорректными параметрами (неправильный номер карты, недостаточно средств на карте и т. д.). Этот тест позволяет проверить случай, при котором Покупатель на сайте Мёрчанта производит оплату картой с некорректными параметрами — сайт, соответственно, не принимает оплату и также реагирует правильным образом (показывает Покупателю сообщение об ошибке, не выдаёт товар или не предоставляет услугу).

3.3.2. Тест успешной оплаты

Все поля в форме оплаты банковской картой являются обязательными для заполнения.

Параметры тестовой карты № 1:

- Имя Держателя карты.
- Страна.
- Город.
- Почтовый адрес.
- Номер телефона.
- Электронная почта.
- Тип карты — VISA.
- Номер карты — 4405050300000000.
- Срок действия — 12/2015.
- CVV2— 123.
- Название банка-эмитента — любой, например UCS.
- Телефон службы технической поддержки банка — любой номер телефона.

После успешно проведённой оплаты Покупателю будет показана страница с информацией о проведённой транзакции и кнопкой **[Вернуться в интернет магазин]**. После нажатия на эту кнопку браузер Покупателя должен быть направлен на сайт Мёрчанта, на страницу с адресом, сохранённым в переменной **URL_RETURN_OK**, которая соответствует успешному проведению оплаты с помощью карты.

Также тестовая среда имеет возможность генерации ошибки платёжной системы при проведении покупки с помощью этой карты.

Сумма платежа определяет результат оплаты следующим образом:

- Если сумма в пределах $0 \leq \text{сумма} \leq 1000.00$ (исключая диапазон 370.00–380.00, см. следующий пункт) или $5000.00 < \text{сумма}$, то происходит успешная оплата.
- Если сумма в пределах $370.00 \leq \text{сумма} < 380.00$, то выдаётся ошибка «Просроченная карта» (Your payment has been declined. Expired card).
- Если сумма в пределах $1000.00 < \text{сумма} \leq 2000.00$, то выдаётся ошибка «Недостаточно средств» (*Not sufficient funds*).
- Если сумма в пределах $2000.00 < \text{сумма} \leq 3000.00$, то выдаётся ошибка «Ваш платеж отклонен. Пожалуйста, проверьте правильность введенной информации по Вашей банковской карте и попробуйте еще раз».
- Если сумма находится в пределах $3000.00 < \text{сумма} \leq 5000.00$, то происходит успешная оплата, но время ответа сервера увеличивается до 110 секунд.

3.3.3. Тест неуспешной оплаты

Все поля на форме оплаты банковской картой являются обязательными для заполнения.

Параметры тестовой карты № 2:

- Имя Держателя карты.
- Страна.
- Город.
- Почтовый адрес.
- Номер телефона.
- Электронная почта.
- Тип карты — VISA.
- Номер карты — 4405050300000001.
- Срок действия — 12/2015.
- CVV2 — 123.
- Название банка-эмитента — любой, например UCS.
- Телефон службы технической поддержки банка — любой номер телефона.

Результатом проведения оплаты с использованием этой карты должен быть показ страницы оплаты с сообщением об ошибке. Если после этого Покупатель нажмёт кнопку [Вернуться без оплаты], то его браузер будет направлен на сайт Мёрчанта, на страницу с адресом, сохранённым в переменной URL_RETURN_NO, которая соответствует неуспешной оплате.

4. Порядок выполнения основных операций

4.1. Операция продажи

4.1.1. Общая последовательность операции продажи

В общем виде последовательность операции продажи изображена на рис. 1.

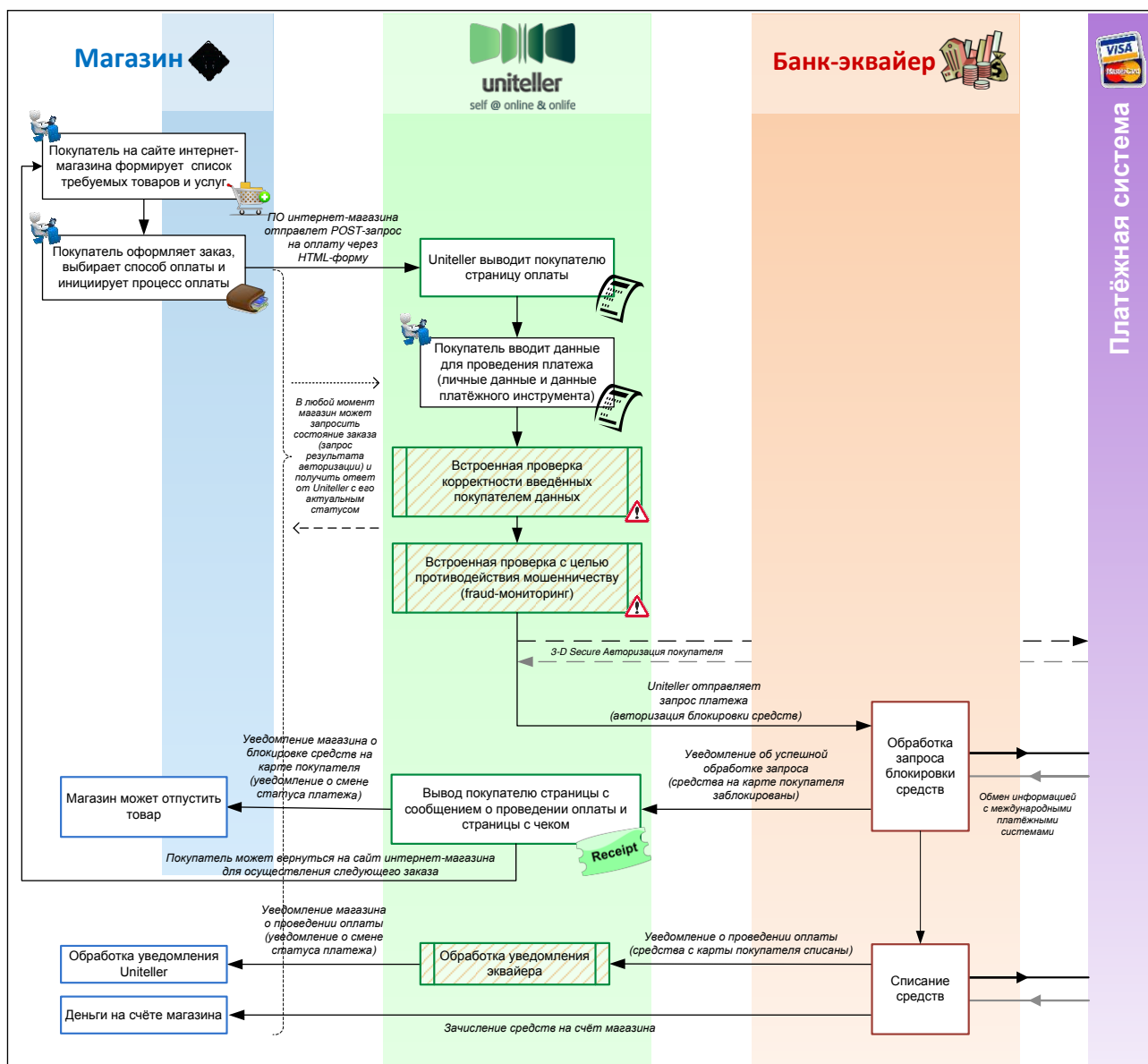


Рис. 1 — Общая последовательность операции продажи

1. Необходимость в оплате возникает при формировании Покупателем на сайте интернет-магазина заказа — набора товаров и/или услуг, требующего оплаты.
2. Операция продажи в системе Uniteller инициируется при получении с сайта интернет-магазина значений полей HTML-формы с параметрами необходимой оплаты. Эта форма может располагаться, например, на странице «**Корзина**», а её поля отсылаются при нажатии Покупателем на сайте интернет-магазина кнопки формы [**Оплатить**]. Пример шаблона HTML-формы приведён п. 4.1.2 «Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры» на стр. 14.
3. Существуют следующие способы оплаты:
 - банковской картой различных международных платёжных систем (VISA, MasterCard, DinersClub, JCB);
 - с помощью различных электронных платёжных систем (EasyPay, Moneybookers, MoneyMail, PayPal, Platezh.ru, QIWI Кошелёк, RBK Money, WebCredits, WebMoney WMR, Yota.money, ВКонтакте, Деньги@Mail.Ru, Евросеть, Мобильный платёж Билайн, Мобильный платёж Мегафон, Мобильный платёж МТС, ПлатФон, Яндекс.Деньги).

Использование того или иного способа оплаты может определяться как предварительно Мёрчантом путём фиксации передаваемых из формы значений параметров **MeanType** и **EMoneyType** (см. п. 4.1.4 «Страница оплаты на сайте Uniteller в зависимости от переданных значений параметров MeanType и EMoneyType» на стр. 20), так и, если это не определено Мёрчантом, выбираться самим Покупателем в ходе оплаты.

4. В результате отправки параметров вышеуказанной формы Покупателю выводится страница оплаты. Вид страницы оплаты зависит от того, выбран ли предварительно способ оплаты, или его только предстоит выбрать (см. п. 4.1.4 «Страница оплаты на сайте Uniteller в зависимости от переданных значений параметров MeanType и EMoneyType» на стр. 20), а также от выбранного шаблона страницы оплаты и его настроек (см. п. 4.1.3 «Способы вывода страницы оплаты. Интеграция страницы оплаты на сайт интернет-магазина» на стр. 19). Если способ оплаты предварительно не определён, то будет показана страница выбора способа оплаты, в противном случае сразу будет показана страница оплаты выбранным способом.
5. На странице оплаты выбранным способом Покупатель вводит данные, требуемые для проведения платежа (например, данные банковской карты), и нажимает [**Оплатить**]. При этом в системе Uniteller создаётся заказ и операция по карте или электронной валюте (для оплаты по банковской карте и электронной валютой, соответственно).
6. Система Uniteller проводит ряд проверок на корректность введённых данных и для противодействия мошенничеству, а также, в случае проведения платежа с 3-D Secure-авторизацией, Покупатель проходит 3-D Secure-авторизацию на сервере платёжной системы.
7. При успешном прохождении внутренних проверок Uniteller и 3-D Secure-авторизации система Uniteller направляет запрос блокировки средств (авторизации) в банк-эквайер.
8. Банк-эквайер проводит свои проверки данных, присланных в запросе платежа, и, при их успешном прохождении, блокирует на счёте Покупателя требуемую сумму и уведомляет Uniteller о завершении авторизации блокировки средств (см. п. 4.6.1 «Уведомление сервера интернет-магазина о статусе оплаты» на стр. 49).
9. Система Uniteller выводит Покупателю страницу успешной оплаты, на которой перечислена вся основная информация по платежу (см. ниже в этом пункте перечень обязательных данных).
Одновременно система Uniteller посылает уведомление на сайт интернет-магазина о

блокировке средств по оплачиваемому заказу. На основании этого сообщения магазин может отпустить товар по заказу².

10. На основании произведённого запроса авторизации блокировки средств в банк-эквайер продолжает обработку платежа, пока сумма платежа не будет зачислена со счёта Покупателя на счёт магазина. При списании средств со счёта Покупателя банк-эквайер информирует об этом систему Uniteller, а Uniteller, в свою очередь, информирует об этом магазин (см. п. 4.6.1 «Уведомление сервера интернет-магазина о статусе оплаты» на стр. 49).

В зависимости от выбранного способа оплата проводится по одной из следующих схем:

- **в фоновом режиме** — Покупатель остаётся на сайте Uniteller и вводит, при необходимости, требуемую дополнительную информацию, в результате оплаты происходит отображение страницы результата оплаты или выставления счёта (см. п. 4.1.5 «Платёж в фоновом режиме» на стр. 24);
- **через внешнюю форму** — Покупатель перенаправляется на сайт выбранной электронной платёжной системы для продолжения операции оплаты без участия Uniteller (см. п. 4.1.6 «Платёж через внешнюю форму» на стр. 27). При этом система Uniteller отслеживает статус этой оплаты.

В случае оплаты через электронную платёжную систему создаётся счёт, который Покупатель должен оплатить впоследствии.

Со страницы оплаты Покупатель может вернуться на сайт интернет-магазина, нажав [**Вернуться в интернет-магазин**]. Покупатель будет перенаправлен на адрес, сохранённый в параметре **URL_RETURN_OK** (если он задан) или **URL_RETURN** (если задан только он), с GET-параметром **Order_ID**, равным **Order_IDP**. Если в URL-адресе уже присутствует **GET**-параметр **Order_ID**, его значение будет заменено.

Пример:

```
URL_RETURN_OK=http://example.com/pay/ok/?param1=value1&param2=value2
```

Перенаправление после оплаты произойдет на адрес:

```
http://example.com/pay/ok/?param1=value1&param2=value2&Order_ID=1234
```

Код страницы сайта Мёрчанта в любом случае должен выполнить запрос, описанный в п. 4.6 «Получение результатов авторизации» (см. стр. 49), к серверу `wrap.uniteller.ru`, используя **Order_ID**, и убедиться в том, что заказ с этим **Order_ID** действительно существует, имеет правильный статус и сумму.

В случае ошибки браузер Покупателя будет перенаправлен на другую (или на ту же самую) страницу на сайте Мёрчанта, которая должна сообщить Покупателю о неуспешности платежа.

² **Примечание:** Критерием оплаты заказа является ответ на запрос Мёрчанта о подтверждения блокировки средств со статусом платежа **authorized** (или **paid**) (см. п. 4.6.2 «Запрос результата авторизации» на стр. 48). О необходимости реализации и использования на сайте магазина механизма запросов результатов авторизации говорится ниже в этом пункте.

Не исключена ситуация, когда перенаправление на страницу успешной оплаты на сайте Мёрчанта не происходит (например, по причине сбоя браузера на стороне Покупателя).

По этой причине рекомендуется:

- использовать механизм уведомлений, описанный в п. «Уведомление сервера интернет-магазина о статусе оплаты» (см. стр. 49), а также
- проверять статус оплаты (см. п. 4.6 «Получение результатов авторизации» на стр. 49) при любой активности на сайте со стороны Покупателя в случае, когда оплата не подтверждена соответствующим обращением на страницу успешной оплаты (**URL_RETURN_OK**), неуспешной оплаты (**URL_RETURN_NO**) или страницы подтверждения факта оплаты (**URL_RETURN**).

Механизм уведомления интернет-магазина о статусе оплаты является средством информирования, которое в определённых условиях подвержено сбоям и задержкам. Для Мёрчанта критерием оплаты заказа должен являться только ответ на его запрос получения результата авторизации (см. п. 4.6.2 «Запрос результата авторизации» на стр. 51) по требуемому заказу и статус заказа в полученном ответе — **Authorized** или **Paid**.

При успешном выполнении оплаты Мёрчант обязан вывести Держателю карты страницу, содержащую следующие данные:

- Торговое наименование Мёрчанта ("Doing business as" name).
- Латинское наименование точки приёма, присвоенное Uniteller (сообщается Мёрчанту вместе с идентификатором точки MERCHANT_ID).
- URL электронного магазина.
- Контактный адрес электронной почты предприятия и контактный телефон.
- Маскированный номер платёжной карты (от 0 до 6 первых цифр и последние 4 цифры номера карты (PAN), соединённые звёздочками).
- Сумма операции в валюте, установленной Uniteller в договоре.
- Дата операции.
- Уникальный идентификатор транзакции (RRN).
- Имя Держателя карты.
- Код авторизации платежа (Authorization code).
- Тип операции (продажа).
- Наименование товара/описание услуг.
- Условия возмещения/возврата (если установлены).
- Точная дата окончания демонстрационного периода (если имеет место).

Полный номер карты **НЕ ДОЛЖЕН** присутствовать на странице успешной оплаты.

Далее будут описаны требуемые параметры и условия проведения операции оплаты и рассмотрены частные случаи её проведения.

4.1.2. Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры

Мёрчанту необходимо разместить на странице сайта интернет-магазина, с которой совершается оплата, HTML-форму, определяющую параметры предстоящей оплаты.

HTML-форма должна передавать следующие обязательные (см. табл. 1) и необязательные (см. табл. 2) параметры на адрес: <https://wpay.uniteller.ru/pay/>.

Табл. 1 — Обязательные параметры формы оплаты на сайте Мёрчанта

№	Параметр	Описание
1	Shop_IDP	Идентификатор точки продажи в системе Uniteller. В Личном кабинете этот параметр называется Uniteller Point ID и его значение доступно на странице « Точки продажи компании » (пункт меню « Точки продажи ») в столбце Uniteller Point ID . Формат: текст, содержащий либо латинские буквы и цифры в количестве от 1 до 64, либо две группы латинских букв и цифр, разделенных «-» (первая группа от 1 до 15 символов, вторая группа от 1 до 11 символов), к регистру нечувствителен.
2	Order_IDP	Номер заказа в системе расчётов интернет-магазина, соответствующий данному платежу. Может быть любой непустой строкой максимальной длиной 127 символов, не может содержать только пробелы. Значение Order_IDP должно быть уникальным для всех оплаченных заказов (заказов, по которым успешно прошла блокировка средств) в рамках одного магазина. Пока по заказу не проведена блокировка средств (авторизация), допускается несколько запросов с одинаковым Order_IDP (например, несколько попыток оплаты одного и того же заказа).
3	Subtotal_P	Сумма покупки в валюте, оговоренной в договоре с банком-эквайером. В качестве десятичного разделителя используется точка, не более 2 знаков после разделителя. Например, 12.34.
4	Signature	Подпись, гарантирующая неизменность критичных данных оплаты (суммы, Order_IDP). (см. п. 7.5 «Необходимость подписания формы оплаты» на стр. 77) Signature вычисляется по следующему алгоритму: <pre>Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Subtotal_P) + & + md5(MeanType) +& + md5(EMoneyType) + & + md5(Lifetime) + & + md5(Customer_IDP) + & + md5(Card_IDP) + & + md5(IData) +& + md5(PT_Code) + & + md5(password)))</pre> где: <ul style="list-style-type: none"> • password — пароль из раздела «Параметры Авторизации» Личного кабинета системы Uniteller. • '+' — операция конкатенации текстовых строк (все строки преобразуются в байты в кодировке ASCII). • '&' — символ «разделитель полей». Если необязательный параметр не передаётся в форме, соответствующий этому полю (следующий за ним) знак '&' сохраняется в строке для вычисления Signature. • md5 — криптографическая хеш-функция (символы в нижнем регистре).

№	Параметр	Описание
		<ul style="list-style-type: none"> • uppercase — функция приведения к верхнему регистру. • MeanType — платёжная система банковской карты. Если MeanType не передаётся в форме, то следует его принять пустой строкой ³. • EMoneyType — тип электронной валюты. Если EMoneyType не передаётся в форме, то следует его принять пустой строкой ³. • Lifetime — время жизни формы оплаты в секундах. Если Lifetime не передаётся в форме, то следует его принять пустой строкой ³. • Customer_IDP — идентификатор покупателя, используемый некоторыми интернет-магазинами. Если Customer_IDP не передаётся в форме, то следует его принять пустой строкой ³. • Card_IDP — идентификатор зарегистрированной карты. Если Card_IDP не передаётся в форме, то следует его принять пустой строкой ³. • IData — «длинная запись». Если IData не передаётся в форме, то следует его принять пустой строкой ³. • PT_Code — тип платежа. Если PT_Code не передается в форме, то следует его принять пустой строкой ³.
5	Параметр URL_RETURN или два параметра: URL_RETURN_OK , URL_RETURN_NO	<p>URL_RETURN ⁴ — URL страницы, на которую должен вернуться Покупатель после осуществления платежа в системе Uniteller. Длина до 255 символов.</p> <p>URL_RETURN_OK ⁴ — URL страницы, на которую должен вернуться Покупатель после успешного осуществления платежа в системе Uniteller. Если этот параметр задан, то он является более приоритетным, чем параметр URL_RETURN. Длина до 255 символов.</p> <p>URL_RETURN_NO ⁴ — URL страницы, на которую должен вернуться Покупатель после неуспешного осуществления платежа в системе Uniteller. Если этот параметр задан, то он является более приоритетным, чем параметр URL_RETURN. Длина (до 255 символов).</p>

³ В этом случае в последовательность подставляется значение md5 от пустой строки, равное **d41d8cd98f00b204e9800998ecf8427e**

⁴ **Примечание:** Не допускается частичное кодирование спецсимволов в тексте URL. Адрес должен задаваться или полностью в некодированном виде (например, <https://domen.ru/account/shopnumber/>), или полностью в кодированном виде (<http%3A%2F%2Fdomen.ru%2Faccount%2Fshopnumber%2F>)

Табл. 2 — Необязательные параметры формы оплаты на сайте Мёрчанта

№	Параметр	Описание
1	Lifetime	Время жизни формы оплаты в секундах, начиная с момента её показа. Должно быть целым положительным числом. Если Покупатель использует форму дольше указанного времени, то форма оплаты будет считаться устаревшей, и платёж не будет принят. Покупателю в этом случае будет предложено вернуться на сайт Мёрчанта для повторного выполнения заказа.
2	Customer_IDP (64 символа)	Идентификатор Покупателя, используемый некоторыми интернет-магазинами.
3	Card_IDP (до 128 символов)	Идентификатор зарегистрированной карты
4	PT_Code	Тип платежа. Произвольная строка длиной до десяти символов включительно. В подавляющем большинстве схем подключения интернет-магазинов этот параметр не используется.
5	MeanType	Платёжная система кредитной карты. Может принимать значения: 0 — любая, 1 — VISA, 2 — MasterCard, 3 — Diners Club, 4 — JCB, 5 — AMEX (пока не поддерживается).
6	EMoneyType	Тип электронной валюты. Возможные значения перечислены в табл. 3 (см. стр. 18).
7	BillLifetime	Срок жизни заказа оплаты в электронной платёжной системе в часах (от 1 до 1080 часов). Значение параметра BillLifetime учитывается только для QIWI-платежей. Если BillLifetime не передаётся, то для QIWI-платежа срок жизни заказа на оплату устанавливается по умолчанию — 72 часа.
8	Preauth	Признак преавторизации платежа. Может принимать значение "1".
9	Language (2 символа)	Код языка интерфейса платёжной страницы. Может быть en или ru .
10	Comment (до 1024 символов)	Комментарий к платежу.
11	FirstName (64 символа)	Имя
12	LastName (64 символа)	Фамилия
13	MiddleName (64 символов)	Отчество
14	Email (64 символа)	Электронный адрес
15	Phone (64 символов)	Телефон
16	Address (128 символов)	Адрес (в стандартном шаблоне в настоящее время не используется)

№	Параметр	Описание
17	Country (64 символа)	Название страны Покупателя (в стандартном шаблоне в настоящее время не используется)
18	State (3 символа)	Код штата/региона
19	City (64 символа)	Город (в стандартном шаблоне в настоящее время не используется)
20	Zip (64 символа)	Почтовый индекс

Параметры **Email**, **Phone**, переданные в запросе к странице оплаты от сайта Мёрчанта, автоматически подставляются в соответствующие поля (скрытые) формы оплаты и не могут быть изменены Покупателем. Если эти поля от Мёрчанта не переданы, то соответствующие им поля видны на странице оплаты и доступны для редактирования.

Табл. 3 — Возможные значения параметра **EMoneyType**

Значение параметра	Расшифровка
0	Любая система электронных платежей
1	Яндекс.Деньги
2	RBK Money
3	MoneyMail
4	WebCreds
5	EasyPay
6	Platezh.ru
7	Деньги@Mail.Ru
8	Мобильный платёж Мегафон
9	Мобильный платёж МТС
10	Мобильный платёж Билайн
11	PayPal
12	ВКонтакте
13	Евросеть
14	Yota.money
15	QIWI Кошелек
16	ПлатФон
17	Moneybookers
29	WebMoney WMR

HTML-форма может располагаться, например, на странице «**Корзина**».

Кодировка символов (character encoding) на странице, на которой расположена форма, и самого содержимого полей формы должна быть **UTF-8**.

Пример шаблона HTML-формы показан ниже:

```
<form action="https://wpay.uniteller.ru/pay/" method="POST">
<input type="hidden" name="Shop_IDP" value="Ваш Shop_ID">
<input type="hidden" name="Order_IDP" value="Ваш Order_ID">
<input type="hidden" name="Subtotal_P" value="Сумма платежа">
<input type="hidden" name="Lifetime" value="Время жизни формы">
<input type="hidden" name="Signature" value="Подпись платежа">
<input type="submit" name="Submit" value="Оплатить">
<input type="hidden" name="URL_RETURN_OK" value="http://example.com/pay/ok/">
<input type="hidden" name="URL_RETURN_NO" value="http://example.com/pay/fail/">
</form>
```

4.1.3. Способы вывода страницы оплаты. Интеграция страницы оплаты на сайт интернет-магазина

Система Uniteller поддерживает 3 способа вывода страницы оплаты:

- на сайте Uniteller по адресу: <https://wpay.uniteller.ru/pay/> (шаблон страницы оплаты «**Стандартный**»);
- на сайте интернет-магазина через элемент `iframe` (шаблон «**Для iframe**»);
- на мобильном устройстве, если интернет-магазин имеет сайт, оптимизированный для вывода на мобильных устройствах (шаблон «**Для мобильных устройств**»).

Определение способа вывода страницы оплаты и настройка соответствующего шаблона осуществляются в Личном кабинете Uniteller в настройках магазина (см. документ «**Личный кабинет платёжной системы Uniteller. Руководство сотрудника мерчанта**»).

Если требуется вывод формы оплаты непосредственно на странице интернет-магазина через элемент `iframe`, выполните следующие действия:

1. В коде страницы в месте размещения элемента `iframe` добавьте следующий код:

```
<iframe width="630" height="332" name="pay_iframe"></iframe>
```

(в примере `pay_iframe` — id элемента `iframe`; **630** — ширина `iframe`; **332** — высота `iframe`; эти значения можно изменять в соответствии с дизайном страницы).

2. В форме оплаты (см. п. 4.1.2 «Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры» на стр. 14) для тега `form` укажите атрибут `target` со значением, совпадающим со значением атрибута `name` элемента `iframe`. Пример:

```
<form action="https://wpay.uniteller.ru/pay/" method="POST" target="pay_iframe">
```

Если требуется подстраивать высоту элемента `iframe` под высоту страницы оплаты Uniteller, необходимо выполнить следующие действия:

1. На странице, где будет размещена форма оплаты через `iframe`, подключите библиотеку jQuery (необходима для использования функции `animate()`), как описано по адресу: <http://api.jquery.com/animate/>.

Пример строки подключения:

```
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js" type="text/javascript"></script>
```

2. Добавьте на страницу с iframe следующий код:

```
<script type="text/javascript">
function listener(event) {
    if ( event.origin !== 'https://wpay.uniteller.ru' ) {
        return;
    }
    $('#pay_iframe').animate({height: event.data + 'px'}, 500);
}
if (window.addEventListener) {
    window.addEventListener('message', listener, false);
} else {
    window.attachEvent('onmessage', listener);
}
</script>
<iframe width="630" height="332" name="pay_iframe" id="pay_iframe"></iframe>
<script type="text/javascript">
    if ($.browser.msie && Number($.browser.version) < 9) {
        $('#pay_iframe').width(630 + 4);
        $('#pay_iframe').height(332 + 22);
    }
    if ($.browser.webkit) {
        // Chrome добавляет перед body отступ.
        $('#pay_iframe').height(332 + 10);
    }
</script>
```

где **pay_iframe** — id элемента **iframe**; **630** — ширина **iframe**; **332** — высота **iframe** (эти значения можно изменять в соответствии с дизайном страницы), **500** — типовой размер 3-D-Secure страницы банка (500x500 пикселей).

3. В форме оплаты (см. п. 4.1.2 «Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры» на стр. 14) должен быть указан атрибут **target** со значением, совпадающим со значением атрибута **name** элемента **iframe**. Пример:

```
<form action="https://wpay.uniteller.ru/pay/" method="POST" target="pay_iframe">
```

4.1.4. Страница оплаты на сайте Uniteller в зависимости от переданных значений параметров MeanType и EMoneyType


После того как Покупатель на сайте Мёрчанта в форме оплаты нажмёт кнопку [**Оплатить**], он будет переведён на одну из страниц сайта Uniteller в зависимости от переданных значений параметров **MeanType** и **EMoneyType**.

Покупатель может быть переведён на одну из следующих страниц сайта Uniteller:

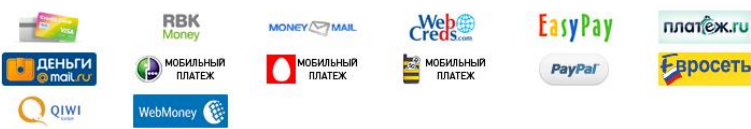
- **Форма выбора способа оплаты** (см. рис. 2) — форма, на которой, в общем случае, предоставляется выбор оплаты банковской картой одной из поддерживаемых платёжных систем или одной из числа поддерживаемых электронной валютой. Если на сервер Uniteller передаётся параметр **MeanType** или **EMoneyType**, соответствующий конкретному типу карты/электронной валюте, то выбор на форме по этому платёжному инструменту будет отсутствовать.


- **Форма оплаты банковской картой** (см. рис. 3) — форма, на которой, в общем случае, предоставляется выбор оплаты банковской картой одной из поддерживаемых международных платёжных систем. Если на сервер Uniteller передаётся параметр **MeanType**, соответствующий конкретному типу карты, то выбор будет отсутствовать.
- **Форма оплаты в конкретной электронной платёжной системе** (см. рис. 4) — форма, с помощью которой осуществляется оплата в электронной платёжной системе, соответствующей переданному параметру **EMoneyType**.
- **Страница с сообщением об ошибке** — см. табл. 5 на стр. 24.

Страница оплаты

 Вы оплачиваете заказ с сайта: **www.testshop.ru**
Номер заказа: **2012-01-17-793**
Сумма к оплате: **301.33 RUB**
Комментарий к оплате: **Тестовый платёж**

Пожалуйста, выберите способ оплаты



 Пожалуйста, введите данные для оплаты с помощью "Банковская карта"


Номер карты (от 12 до 19 символов)

Срок действия (ММ/ГГ)

Имя на карте

XXXX XXX
CVV2/CVC2

[Вернуться без оплаты](#)


Гарантии безопасности 

В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru

Рис. 2 — Форма выбора способа оплаты

Страница оплаты




Вы оплачиваете заказ с сайта: www.testshop.ru

Номер заказа: 2012-01-17-79490

Сумма к оплате: **301.34 RUB**

Комментарий к оплате: Тестовый платеж



Пожалуйста, введите данные для оплаты с помощью "Банковская карта"

Номер карты (от 12 до 19 символов)

Срок действия (ММ/ГГ)

Имя на карте





XXXX XXXX

CVV2/CVC2

[Вернуться без оплаты](#)

Оплатить

Гарантии безопасности







В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru

Рис. 3 — Пример формы оплаты банковской картой

Страница оплаты




Вы оплачиваете заказ с сайта: www.testshop.ru

Номер заказа: 2012-01-17-59222

Сумма к оплате: **301.35 RUB**

Комментарий к оплате: Тестовый платеж



Пожалуйста, введите данные для оплаты с помощью "Мобильный платеж Мегафон"

Мегафон™

Для выставления счета введите информацию и нажмите кнопку "Оплатить"





Номер мобильного телефона

Номер мобильного телефона, на который будет выставлен счет. Номер указывается в десятизначном формате. Например, 9123456780.

[Вернуться без оплаты](#)

Оплатить

Гарантии безопасности

В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru

Рис. 4 — Пример формы оплаты электронной валютой

В случае если выполняются следующие условия:

- в системе Uniteller есть договор на предоставление Мёрчанту услуги интернет-эквайринга;
- в системе Uniteller есть договор с Мёрчантом на обслуживание электронных валют, и договор имеет статус «Действует»;
- по условиям договора на обслуживание электронных валют разрешено обслуживание

магазина с требуемым идентификатором **Shop_IDP**;
Покупатель перейдёт на страницу в соответствии с табл. 4.

Табл. 4 — Зависимость страницы сайта Uniteller, на которую переходит пользователь со страницы оплаты сайта Мёрчанта, в зависимости от значений параметров MeanType и EMoneyType

№	Значение параметра MeanType (N — целочисленное значение в допустимом диапазоне)	Значение параметра EMoneyType (N — целочисленное значение в допустимом диапазоне)	Страница на сайте Uniteller
1	Не передаётся	Не передаётся	Форма выбора способа оплаты (см. рис. 2 на стр. 21).
2	0	Не передаётся	Форма оплаты картой (см. рис. 3 на стр. 22).
3	N	Не передаётся	Форма оплаты картой (см. рис. 3 на стр. 22).
4	Не передаётся	0	Форма выбора способа оплаты, но без информации о картах (см. рис. 2 на стр. 21).
5	Не передаётся	N	Форма оплаты в соответствующей электронной платёжной системе (см. рис. 4 на стр. 22).
6	0	0	Форма выбора способа оплаты (см. рис. 2 на стр. 21).
7	N	0	Форма выбора способа оплаты (см. рис. 2 на стр. 21).
8	0	N	Форма выбора способа оплаты (см. рис. 2 на стр. 21). На форме можно выбрать только карты или единственно указанную электронную платёжную систему.
9	N	N	Форма выбора способа оплаты (см. рис. 2 на стр. 21). На форме можно выбрать только карты или единственную указанную электронную платёжную систему.

Если передаётся параметр **MeanType** и выполняется одно из условий (магазину не разрешены оплаты электронными валютами):

- в системе Uniteller нет договора с Мёрчантом на обслуживание электронных валют или имеющийся договор не находится в статусе «Действует»;
- в системе Uniteller есть договор с Мёрчантом на обслуживание электронных валют в статусе «Действует», но по нему не разрешено обслуживание магазина с переданным идентификатором **Shop_IDP** или не разрешены платежи по электронной валюте с переданным **EMoneyType**;

то Покупатель перейдёт на страницу с формой оплаты картой (см. рис. 3 на стр. 22).

Если на этапе загрузки страницы оплаты возникла ошибка интеграции (например, Мёрчант передал параметры с ошибками), то будет загружена страница «**Ошибка загрузки страницы оплаты**» (см. рис. 5), на которой текст ошибки в явном виде не показывается.

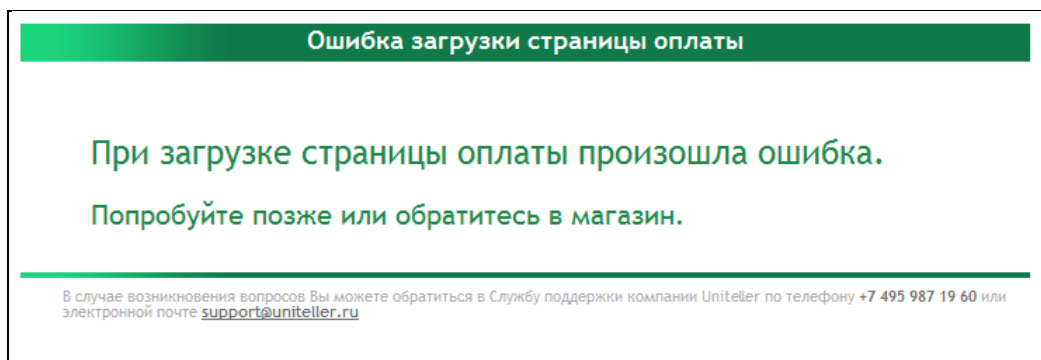


Рис. 5 — Страница «Ошибка загрузки страницы оплаты»

Для того чтобы прочесть текст ошибки (например, чтобы понять проблему интеграции при тестовом подключении) необходимо открыть исходный код страницы «**Ошибка загрузки страницы оплаты**» и прочитать описание ошибки в HTML-комментарии сразу после тега <body>.

Пример:

```
...
<body>
<!-- MERCHANT ERROR: Signature is not valid -->
<div id="page">
  <div id="header">Ошибка загрузки страницы оплаты</div>
...
```

Сообщение об ошибке возможно в ситуациях, перечисленных в табл. 5.

Табл. 5 — Возможные сообщения об ошибках, определяемые переданными значениями параметров MeanType и EMoneyType

№	Условие	Значение параметра MeanType	Значение параметра EMoneyType (N — целочисленное значение в допустимом диапазоне)	Сообщение об ошибке
1	В системе нет действующего договора на обслуживание электронных валют или по действующему договору не разрешено обслуживание магазина с требуемым Shop_IDP	Не передаётся	Передаётся	«К сожалению, вы не можете оплатить данный заказ. Установлено ограничение интернет-магазина.»
2	По действующему в системе договору на обслуживание электронных валют не разрешено обслуживание требуемой электронной валюты (EMoneyType=N)	Не передаётся	N	«К сожалению, вы не можете оплатить данный заказ. Установлено ограничение интернет-магазина.»

4.1.5. Платёж в фоновом режиме

Ряд платёжных инструментов (например, оплата банковской картой, Мобильный платёж (МТС, Билайн, Мегафон), Евросеть, QIWI) производят оплату в так называемом фоновом режиме, когда Покупатель для совершения оплаты не перенаправляется с сайта Uniteller на сайт платёжной


системы, а вводит всю необходимую информацию, а также получает страницу с результатами оплаты, непосредственно на сайте Uniteller.

В общем случае оплата в фоновом режиме имеет следующую последовательность:

1. Пользователь на сайте Uniteller (см. рис. 2 на стр. 21) выбирает способ оплаты, который проводится в фоновом режиме, или с формы оплаты Мёрчанта передаётся параметр, определяющий соответствующий способ оплаты.
2. Пользователь переходит на страницу с формой оплаты выбранным способом (см. рис. 3 на стр. 22, рис. 4 на стр. 22), на которой вводит, если требуется, информацию, необходимую для осуществления платежа.
3. Если проверка введённой Покупателем информации проходит успешно, то происходит отправка платежа. В случае некорректно введённой информации Покупателю показывается соответствующее сообщение об ошибке.
4. Если платёж отправлен успешно, то происходят следующие события:
 - В случае оплаты по банковской карте производится блокировка средств на карте (авторизационная транзакция) на сумму заказа (параметр **Subtotal_P**). В системе Uniteller создаётся заказ и операция по карте в статусе «Успешная авторизация».
 - Для платежа по банковской карте на странице с результатами оплаты указана следующая информация (см. рис. 6) (на адрес электронной почты Покупателя будет выслано письмо с этими же данными):
 - Номер заказа — номер, который был передан на форму оплаты в параметре **Order_IDP**.
 - Сумма операции.
 - Покупатель — имя владельца карты, введённое Покупателем на форме оплаты.
 - Номер карты — маскированный номер карты (показываются только первые 6 и последние 4 цифры номера, разделённые звёздочками).
 - Код авторизации — номер процессинга, который идентифицирует эту транзакцию в банке-эквайере.
 - Дата операции — дата и время выполнения операции.
 - Для платежа «Мобильный платёж» (МТС, Билайн, Мегафон) на мобильный телефон Покупателя будет отправлено СМС-сообщение, информирующее о выставлении счёта.
 - В случае оплаты через электронную валюту в системе Uniteller создаётся заказ и операция по электронной валюте со статусом «Ожидает оплаты», а Покупателю показывается страница с результатами выставления счёта⁵ (см. рис. 7).
Для платежа «Евросеть» форма результата оплаты будет содержать данные «**Получатель платежа**» («ДеньгиOnline») и «**Номер платежа в Евросети**», по которому Покупатель сможет оплатить заказ в торговой точке Евросети (см. рис. 8).
5. Если отправка платежа завершилась ошибкой, Покупателю показывается страница с сообщением об ошибке оплаты.

⁵ Если счёт при оплате электронной валютой выставлен, то повторно инициировать оплату этого же заказа нельзя. Если по каким-то причинам первоначально выставленный счёт оплачен не будет, а продать товар надо, то магазину следует сформировать новый заказ и инициировать его оплату.

Страница оплаты



Вы оплачиваете заказ с сайта: www.testshop.ru

Номер заказа: 2012-01-17-79490

Сумма к оплате: **301.34 RUB**

Комментарий к оплате: Тестовый платеж

Ваш платеж банковской картой совершен успешно.

Пожалуйста, сохраните указанную информацию о платеже

Вернуться в магазин

Номер платежа:
2012-01-17-79490

Сумма операции:
301.34 RUB

Покупатель:
Ivan Ivanov

Номер карты:
440505*****0000

Код авторизации:
F84A8A

2012-01-17 19:57:51

Гарантии безопасности

В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru











Рис. 6 — Страница с результатом оплаты банковской картой

Страница оплаты



Вы оплачиваете заказ с сайта: www.testshop.ru

Номер заказа: 2012-01-17-59222

Сумма к оплате: **301.35 RUB**

Комментарий к оплате: Тестовый платеж

Счет для оплаты в пользу предприятия e-коммерции Тестовый магазин [www.testshop.ru] выставлен успешно.

Вернуться в магазин

Сумма операции:
301.35 RUB

2012-01-17 19:58:45

Гарантии безопасности

В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru











Рис. 7 — Пример страницы с результатами выставления счёта на оплату электронной валютой

Страница оплаты



Вы оплачиваете заказ с сайта: **www.testshop.ru**

Номер заказа: **2012-01-17-793**

Сумма к оплате: **301.33 RUB**

Комментарий к оплате: **Тестовый платеж**

Счет для оплаты в пользу
предприятия e-коммерции
Тестовый магазин
[www.testshop.ru] выставлен
успешно.

Пожалуйста, сохраните указанную информацию
о платеже

Вернуться в магазин

Сумма операции:	301.33 RUB
Получатель платежа:	ДеньгиOnline
Номер платежа:	44151909
2012-01-17 20:00:03	

Гарантии безопасности

В системе Uniteller безопасность платежей и конфиденциальность введенной Вами информации обеспечивается использованием протокола SSL и другими специальными средствами. Ваши персональные данные хранятся исключительно нами и ни при каких обстоятельствах не будут предоставлены третьим лицам за исключением случаев, предусмотренных законодательством.

В случае возникновения вопросов Вы можете обратиться в Службу поддержки компании Uniteller по телефону +7 495 987 19 60 или электронной почте support@uniteller.ru




Рис. 8 — Страница с результатом выставления счёта при платеже «Евросеть»

4.1.6. Платёж через внешнюю форму

При оплате следующими платёжными инструментами: Яндекс.Деньги, RBK Money, MoneyMail, WebCredits, EasyPay, Platesh.ru, Деньги@Mail.Ru, PayPal, ВКонтакте, Yota.money, WebMoney WMR, оплата производится через внешнюю форму выбранной электронной платёжной системы с переходом Покупателя на сайт этой платёжной системы.

В общем случае оплата через внешнюю форму имеет следующую последовательность:

1. Пользователь на сайте Uniteller (см. рис. 2 на стр. 21) выбирает способ оплаты, который проводится через внешнюю форму, или с формы оплаты Мёрчанта передаётся параметр, определяющий соответствующий способ оплаты.
2. Пользователь переходит на страницу оплаты выбранной электронной валютой (см. рис. 4 на стр. 22), на которой вводит, если требуется, информацию, необходимую для осуществления платежа.
3. Если проверка введённой Покупателем информации проходит успешно, или ввод дополнительной информации не требуется, Пользователь перенаправляется на сайт соответствующей электронной платёжной системы. При этом в системе Uniteller создаётся заказ и операция по электронной валюте в статусе «Ожидание оплаты». В случае некорректно введённой информации Покупателю показывается соответствующее сообщение об ошибке.
4. Открывается страница на сайте соответствующей электронной платёжной системы. Пользователь оплачивает заказ в соответствии с инструкциями на этой странице. Возможны следующие особенности:
 - В различных платёжных системах возможны варианты как on-line оплаты счёта, так и разнесённого во времени выставления счёта и его оплаты.

- Объем информации о первоначальном заказе Покупателя в интернет-магазине Мёрчанта на странице оплаты платёжной системы варьируется и зависит от дизайна страницы и процесса оплаты соответствующей платёжной системы.
- Не у всех платёжных систем на страницах оплат имеется возможность (кнопка, ссылка и т. д.) возврата в интернет-магазин Мёрчанта, в котором сделан первоначальный заказ.

4.2. Преавторизация платежа

4.2.1. Общее описание

Платёжная система Uniteller позволяет выполнять платежи с преавторизацией.

Преавторизация — это возможность блокирования средств на карте пользователя без направления представления (settlement) в платёжную систему.

Для того чтобы средства были списаны с карты и перечислены Эквайнером на расчётный счёт Мёрчанта, последнему необходимо по каждой преавторизации отправить команду подтверждения платежа (см. п. 4.2.3 «Подтверждение платежа, проведённого с преавторизацией», стр. 29).

Уведомление о необходимости финансового списания (в виде POST- или GET-запроса) может быть направлено в систему Uniteller в течение 7 календарных дней после проведения успешной преавторизации. По истечении указанного срока запросы будут обработаны, но с большой долей вероятности такие операции будут успешно опротестованы Эмитентом, а средства по ним будут впоследствии списаны со счёта Мёрчанта в банке-эквайере.

Мёрчант в любой момент может отменить преавторизацию либо вернуть средства по завершённому платежу, выполнив операцию «Отмена платежа».

4.2.2. Проведение преавторизации платежа

Мёрчант для каждого своего магазина и каждого сформированного заказа может определить необходимость проводить оплату в обычном режиме (пользователь провел успешный платёж, больше ничего не требуется) или проводить оплату только после отправки дополнительного подтверждения операции (платёж с преавторизацией).

Для выполнения преавторизации платежа Мёрчант должен передать необязательный параметр **Preauth**. В случае если этот параметр передан и равен **“1”**, то считается, что проводится преавторизация, требующая дополнительного подтверждения прежде, чем будет отправлена команда завершения платежа. Проведение оплаты для Покупателя магазина не отличается от последовательности, описанной в п. 4.1 «Операция продажи» (см. стр. 11).

Также ПО Мёрчанта может обратиться по определенным адресам на сервере WPay, чтобы получить результаты авторизации.

Если для магазина Мёрчанта задан параметр **«URL-адрес уведомления магазина»**, то на этот адрес приходит HTTP POST запрос с параметрами:

- **Order_ID** — номер заказа;
- **Status** — статус (authorized, paid, canceled);
- **Signature** — цифровая подпись (uppercase(md5(Order_ID + Status + password))).

Статус **authorized** будет отправлен после проведения успешной преавторизации, **paid** — после успешной отправки команды **Complete** (после получения соответствующей информации от банка-эквайера), **canceled** — после успешной отмены преавторизации либо успешной отправки команды **REFUND**.

4.2.3. Подтверждение платежа, проведённого с преавторизацией

Для отправки подтверждения по проведённой ранее преавторизации необходимо выполнить POST- или GET-запрос на адрес <https://wpay.uniteller.ru/confirm/> с параметрами, указанными в табл. 6 и табл. 7. В ответ вернутся значения, перечисленные в параметре **S_FIELDS** (см. п. 7.1 «Возможные поля параметра S_FIELDS» на стр. 60).

Формат ответа будет зависеть от переданного параметра **Format**:

- 1 – Ответ в формате CSV. В качестве разделителя используется точка с запятой «;».
- 2 – Ответ в формате WDDX.
- 3 – Ответ в формате XML.

Если параметр **Format** не указан, ответ будет в формате CSV.

Табл. 6 — Обязательные параметры запроса подтверждения платежа, проведённого с преавторизацией

№	Параметр	Тип	Описание
1	Billnumber	12 цифр	Номер платежа в системе Uniteller (RRN)
2	Shop_ID	Строка длиной до 64 символов	Идентификатор точки продажи в системе Uniteller. Доступен Мёрчанту в Личном кабинете на странице «Точки продажи компании» (пункт меню «Точки продажи») в столбце Uniteller Point ID.
3	Login	Строка до 64 символов	Логин, выданный Мёрчанту при создании учётной записи в системе Uniteller
4	Password	80 символов	Пароль, выданный Мёрчанту при создании учётной записи в системе Uniteller.

Табл. 7 — Необязательные параметры запроса подтверждения платежа, проведённого с преавторизацией

№	Параметр	Тип	Значение по умолчанию	Описание
1	Subtotal_P	Число		Измененная сумма транзакции. Должна быть не более суммы исходного платежа. Передается только в случае необходимости изменения суммы платежа.
2	Currency	3-символа	Код валюты авторизации	Код валюты. Может быть использован только код валюты авторизации.
3	Language	2 символа	'ru'	Язык выдачи результатов
4	Format	1 (CSV), 2 (WDDX), 3 (XML), 4 (SOAP)	1	Формат выдачи результата. В формате 1 поля разделены точкой с запятой.

№	Параметр	Тип	Значение по умолчанию	Описание
5	S_FIELDS		пустое значение (или не передаётся) — все поля	Набор информационных полей, возвращаемых в ответе на запрос. Формат представления информации в ответе определяется параметром Format . (Подробно поддерживаемые поля параметра S_FIELDS описаны в п. 7.1 «Возможные поля параметра S_FIELDS» на стр. 60)

В случае возникновения ошибки будут возвращены 2 параметра: **firstcode** и **secondcode**, значения которых приведены в табл. 8.

Табл. 8 — Возможные сообщения об ошибках при запросе подтверждения платежа, проведённого с преавторизацией

Код (firstcode)	Сообщение (secondcode)	Расшифровка
1	Authentication error	Некорректные данные авторизации (Login, Password)
3	Mandatory parameter '%fieldName%' is not present in the request	Не указан обязательный параметр (%fieldName% - имя параметра)
4	Bill not found	Не найден платёж
5	Field %fieldName% has bad format	Неверный формат значения или значение не входит в область допустимых (%fieldName% - имя параметра)
10	S_FIELDS contains field '%name%' which is not allowed	В поле S_FIELDS присутствует неподдерживаемый параметр. %name% - код параметра
15	The operation failed	По некоторым причинам операция была прервана. Попробуйте в другой раз
18	Authorization confirm is not allowed	Невозможно выполнить подтверждение

Отправка запроса подтверждения не приводит к немедленной отправке команды завершения платежа по данному заказу. Отправка команд завершения платежа происходит автоматически для преавторизаций с полученным от Мёрчанта подтверждением перед закрытием операционного дня (в 20:30).

Если в течение определённого периода времени, зависящего от условий работы банка-эквайера, ПО Мёрчанта не отправило подтверждения по платежам с преавторизацией, эти платежи будут отклонены эквайером (никаких дополнительных действий для этого не требуется), и заблокированные ранее средства на счёте Покупателя по этим заказам станут доступны к использованию.

Если ПО Мёрчанта отправило подтверждение для заказа и получило успешный ответ, то любая следующая отправка подтверждения по данному заказу будет приводить к ответу, содержащему код и текст ошибки.

Если ПО Мёрчанта отправило подтверждение для заказа и получило код и текст ошибки, то Мёрчанту необходимо проанализировать эту ошибку и понять, что требуется изменить в запросе для получения успешного ответа по нему.

Если ПО Мёрчанта отправило подтверждение для заказа, который уже просрочен (отклонен), и получило успешный ответ, то при отправке команды завершения платежа по данному заказу от банка-эквайера будет получена ошибка.

4.3. Рекуррентные платежи

4.3.1. Общее описание

Платёжная система Uniteller позволяет выполнять рекуррентные платежи. Рекуррентные платежи — это платежи, осуществляемые без участия Держателя карты (в автоматическом режиме), с согласия Держателя карты и по заранее утверждённому расписанию (в том числе по наступлении определённых событий).

Примеры рекуррентных платежей:

- ежемесячное списание абонентской платы за Интернет;
- списание суммы по счёту за мобильный телефон согласно сделанным за месяц вызовам (при кредитной форме оплаты);
- автоматическое пополнение баланса мобильного телефона на 200 руб. при балансе меньше 100 руб.;
- списание суммы, исходя из условия — если остаток по счёту в онлайн-игре равен 10 руб., то платёж на 1000 руб., если 50 руб., то платёж на 500 рублей.

4.3.2. Особенности рекуррентных платежей и принципы их проведения в системе Uniteller

Можно выделить следующие особенности рекуррентных платежей:

- Инициирование рекуррентного платежа происходит без участия Держателя карты, поэтому отсутствует возможность получить CVV2(CVC2)-код банковской карты.
- Для проведения рекуррентного платежа необходимы данные его «родительского» платежа, осуществлённого с участием Держателя карты и служащего «шаблоном» для подобных ему последующих рекуррентных платежей.
- Рекуррентный платёж, по сути, не отличается от единичного платежа по банковской карте. Его особенностью является только то, что часть данных, необходимых для осуществления платежа, не заносится Покупателем, а берётся из «родительского» платежа.
- Так как при осуществлении рекуррентного платежа не участвует Держатель карты, то нет возможности обеспечить поддержку 3-D Secure-авторизации (при этом «родительский» платёж может быть проведён с поддержкой 3-D Secure-авторизации). Связанные с этим риски несёт Мёрчант.

При обеспечении рекуррентных платежей Uniteller руководствуется следующими принципами:

- Всё общение с Покупателем (Держателем карты) осуществляет Мёрчант. Uniteller имеет отношения только с Мёрчантом.
- Все действия по юридическому обеспечению отношений с Покупателем, а также по установке и поддержке требуемого расписания платежей осуществляет Мёрчант. Обращаем внимание на то, что для осуществления рекуррентных платежей Мёрчантом должно быть получено явное согласие Держателя карты. Это может быть отметка о согласии с Правилами списания на сайте Мёрчанта, подтверждение нажатием на кнопку **[OK]** во всплывающем окне и т. д. Подписание письменного документа не требуется. Периодичность списания задаётся либо Держателем карты самостоятельно, либо явно

задаётся Мёрчантом, чтобы избежать двояких толкований. Рекомендуется каким-либо образом протоколировать в электронном виде выбор Держателя карты для последующего возможного разбирательства спорных ситуаций.

- При проведении рекуррентных платежей функция Uniteller заключается в обработке запросов на платёжи, поступившие от Мёрчанта. Если от Мёрчанта поступил запрос на платёж, то Uniteller считает, что этот платёж легитимен и отвечает требованиям Покупателя и Мёрчанта.
- Сумма рекуррентного платежа может не совпадать с суммой его «родительского» платежа.
- Любой рекуррентный платёж может служить «родительским» платежом для последующих однотипных рекуррентных платежей.
- Включение поддержки рекуррентных платежей интернет-магазином Мёрчанта осуществляется только сотрудниками Uniteller.
- Интервал между рекуррентными платежами не может превышать 180 дней.

4.3.3. Проведение рекуррентных платежей

Для выполнения рекуррентного платежа необходимо выполнить POST- или GET-запрос на адрес: <https://wpay.uniteller.ru/recurrent/> с параметрами, указанными в табл. 9.

Табл. 9 — Обязательные параметры запроса выполнения рекуррентного платежа

№	Параметр	Описание
1	Shop_IDP	Идентификатор точки продажи в системе Uniteller. В Личном кабинете этот параметр называется Uniteller Point ID и его значение доступно на странице « Точки продажи компании » (пункт меню « Точки продажи ») в столбце Uniteller Point ID .
2	Order_IDP	Номер заказа в системе расчётов интернет-магазина, соответствующий данному платежу. Может быть любой непустой строкой максимальной длиной 127 символов, не может содержать только пробелы.
3	Subtotal_P	Сумма покупки в валюте, оговоренной в договоре с Эквайером. В качестве десятичного разделителя используется точка. Например, 12.34.
4	Parent_Order_IDP	Номер (Order_IDP) «родительского» платежа в системе расчётов интернет-магазина. Может быть любой непустой строкой максимальной длиной 127 символов, не может содержать только пробелы.

№	Параметр	Описание
5	Signature	<p>Подпись, гарантирующая неизменность критичных данных оплаты (суммы, Order_IDP) (см. п. 7.5 «Необходимость подписания формы оплаты» на стр. 77).</p> <p>Signature вычисляется по следующему алгоритму:</p> <pre>Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Subtotal_P) + & + md5(Parent_Order_IDP) + & + md5(password)))</pre> <p>где:</p> <ul style="list-style-type: none"> • password — пароль из раздела «Параметры Авторизации» Личного кабинета системы Uniteller. • '+' — операция конкатенации текстовых строк (все строки преобразуются в байты в кодировке ASCII). • '&' — символ «разделитель полей». • md5 — криптографическая хеш-функция. • uppercase — функция приведения к верхнему регистру.

Ответ на запрос будет передан в формате CSV (разделитель — точка с запятой).

Формат ответа подобен ответу при отмене платежа, но дополнен значением параметра **Signature**.

Формат ответа на запрос рекуррентного платежа указан в п. «Форматы ответов» в пп. «Запрос рекуррентного платежа» на стр. 71.

В случае возникновения ошибки будет возвращено 2 параметра: **ErrorCode** и **ErrorMessage**, значения которых приведены в Табл. 10.

Табл. 10 — Возможные сообщения об ошибках при запросе выполнения рекуррентного платежа

Код (ErrorCode)	Сообщение (ErrorMessage)	Расшифровка
2	Invalid signature	Неверная подпись в запросе
3	Mandatory parameter '%fieldName%' is not present in the request	Не указан обязательный параметр (%fieldName% — имя параметра)
5	Field %fieldName% has bad format	Неверный формат значения или значение не входит в область допустимых (%fieldname% — имя параметра)
15	The operation failed	По некоторым причинам операция была прервана. Попробуйте в другой раз.
22	Recurrent payment not allowed	Магазин не поддерживает рекуррентные платежи
23	Incorrect Parent_Order_IDP	Ссылка на «родительский» платёж отсутствует или указывает на неуспешный платёж.
24	Order_IDP already exists	Такой Order_IDP уже существует
25	Shop_IDP not found	Не найден Shop_IDP

4.4. Регистрация банковских карт для повторных платежей

4.4.1. Общая информация о регистрации банковских карт

Для облегчения Покупателям интернет-магазинов оплаты покупок по банковским картам платёжная система Uniteller позволяет регистрировать банковские карты с сохранением их основных данных для проведения по этим картам повторных платежей.

Для оплаты банковской картой, зарегистрированной ранее в платёжной системе Uniteller, держателю карты не нужно вводить все данные карты на форме оплаты — достаточно указать только CVV2/CVC2, и, возможно, пройти 3DSecure-авторизацию. При этом Покупатель может иметь несколько зарегистрированных банковских карт и выбирать непосредственно на платёжной форме Uniteller или на сайте интернет-магазина, какой именно картой он будет оплачивать свой заказ.

Использование механизма регистрации карт при осуществлении своих платежей находится полностью в ведении интернет-магазина.

4.4.2. Для чего нужна регистрация карт и типичные механизмы привязки

Возможны различные сценарии применения магазином механизмов привязки карт, например, наиболее распространёнными являются:

- Сохранение данных карты (за исключением CVV2/CVC2) при первой оплате по желанию Покупателя. При последующих оплатах в этом магазине Покупатель может выбрать зарегистрированную карту из списка и не вводить большое кол-во данных карты.
- Привязка карты выполняется не только для минимизации ввода данных пользователем, но также и для снижения риска мошеннических операций с нелегальным использованием банковских карт. Процесс привязки карты отделяется от последующих оплат. Оплата пользователем при таком режиме использования чаще всего в магазине производится только по зарегистрированной карте, при этом выбор конкретной зарегистрированной карты, привязанной к пользователю, может производиться на стороне магазина.
- Карты, выпускаемые банком, привязываются автоматически (без участия покупателя интернет-магазина) к указанному интернет-магазину и связываются с идентификаторами соответствующих покупателей данного магазина. Такой режим используется, например, в случае выпуска кобрендовых карт совместно банком и магазином, что позволяет владельцам таких карт, являющихся одновременно пользователями интернет-магазина, сразу получать возможность упрощённой оплаты в магазине по этим картам.

Существует три базовых механизма привязки карт:

- **Привязка по успешному платежу** — карта регистрируется, если при обычной оплате, вводя полные данные карты, покупатель подтверждает желание (ставит галочку) «**Сохранить данные карты**», и платёж завершается успехом (см. п. 4.4.4.2 «Первая оплата картой после авторизации в интернет-магазине» на стр. 36).
- **Привязка по случайной сумме** — карта регистрируется, если после авторизации случайной суммы покупатель её правильно подтверждает (см. п. 4.4.4.5 «Регистрация карты по случайной сумме» на стр. 38).
- **Привязка по реестру** — карта регистрируется на основе полученных от Банка-эмитента данных и активируется после указания связи этой карты с покупателем, информация о которой получена от интернет-магазина (см. п. 4.4.4.12 «Привязка карт по реестру» на стр. 44).
-

4.4.3. Безопасность и разделение ответственности

4.4.3.1. Данные карты, «маска» и её статусы

Зарегистрированная карта — это основные данные банковской карты (за исключением CVV2/CVC2), хранящиеся в процессинговом центре Uniteller. Данные карты никогда не передаются ни интернет-магазину, ни самому покупателю (через форму оплаты или как-либо иначе).

Каждая зарегистрированная карта принадлежит какому-либо зарегистрированному посетителю интернет-магазина. На одного посетителя может быть зарегистрировано несколько карт. Одна и та же карта может быть зарегистрирована на нескольких посетителей одного и того же или различных интернет-магазинов.

Каждая зарегистрированная карта имеет уникальный идентификатор **Card_IDP**, «маску» отображения и статус.

«Маска» отображения карты служит для того, чтобы предоставить посетителю интернет-магазина информацию о том, какие карты зарегистрированы на него, но в то же время не раскрыть данных карты в соответствии с требованиями безопасности. «Маска» карты состоит из первых 6 и последних 4 цифр номера карты, разделённых звёздочками (пример: 123456****1234). Иногда перед «маской» выводится тип карты словами (т.е. параметр **CardType**, пример: VISA 123456****1234). «Маска» карты показывается покупателю и может быть передана интернет-магазину.

Есть три статуса карты:

- **«Не подтверждена»** — посетитель начал процедуру регистрации карты, но еще не подтвердил указанием случайной суммы.
- **«Активна»** — совершать оплату зарегистрированной картой можно только, если она имеет статус «активна».
- **«Заблокирована»** — активная карта блокируется для того, чтобы по ней временно нельзя было совершать платежи.

4.4.3.2. Уникальный идентификатор покупателя **Customer_IDP**

Интернет-магазин должен присвоить уникальный идентификатор **Customer_IDP** каждому своему зарегистрированному посетителю. Таким идентификатором может служить имя пользователя в системе интернет-магазина (телефон, e-mail, логин и др.). Процессинговый центр отличает одного покупателя от другого только по параметру **Customer_IDP**, который получает от интернет-магазина при входе покупателя на платёжную страницу. Интернет-магазин должен предотвратить возможность использования **Customer_IDP** не тем посетителем, которому он был выдан. Ответственность за корректную аутентификацию и авторизацию покупателей несёт интернет-магазин.

Оплата картой, данные которой хранятся в процессинговом центре, возможна только при указании корректного CVV2/CVC2 карты. Если карта поддерживает 3DSecure-авторизацию, покупателю также придётся каждый раз при оплате её проходить.

4.4.4. Типичные сценарии использования

4.4.4.1. Оплата картой без авторизации в интернет-магазине

Последовательность действий при оплате банковской картой без авторизации в интернет-магазине имеет следующие основные шаги:

1. Покупатель интернет-магазина, не прошедший авторизацию на сайте магазина (также в случае, если покупатель прошёл регистрацию на сайте магазина, но магазин не передал на сайт Uniteller его идентификатор **Customer_IDP**), переходит на стандартную страницу оплаты картой на сайте Uniteller, на которой нужно указать все данные карты.
2. Покупатель указывает требуемые данные карты, которой совершает оплату.

3. В случае если все данные указаны верно, платёж совершается, данные карты не сохраняются.
4. При последующих оплатах покупателю придётся снова вводить все данные карты.

4.4.4.2. Первая оплата картой после авторизации в интернет-магазине

Последовательность действий при первой оплате банковской картой после авторизации в интернет-магазине имеет следующие основные шаги:

1. Посетитель интернет-магазина авторизуется на сайте магазина, магазин ставит ему в соответствие уникальный идентификатор **Customer_IDP**.
2. При вызове интернет-магазином формы оплаты заказа этого посетителя магазин указывает помимо прочих параметров идентификатор покупателя **Customer_IDP**.
3. При переходе на страницу оплаты картой на сайте Uniteller процессинговый центр определяет, что для данного покупателя нет ни одной зарегистрированной карты.
4. Покупателю отображается стандартная страница оплаты картой, на которой требуется указать все данные карты.
5. Также на стандартной странице оплаты отображается флажок «**Сохранить данные карты**» (по умолчанию флажок установлен), включающий регистрацию банковской карты.
6. Если покупатель снял флажок «**Сохранить данные карты**», дальнейшее поведение страницы оплаты и процессингового центра не отличается от сценария «Оплата картой без авторизации в интернет-магазине» (см. п. 4.4.4.1 на стр. 35).
7. Если галочка установлена, и попытка оплаты завершена успешно, карта регистрируется в процессинговом центре на этого покупателя этого интернет-магазина. Данным карты присваивается уникальный идентификатор **Card_IDP** и формируется соответствующая «маска» отображения. Карте присваивается статус «активна».
8. Интернет-магазину не сообщается никакой дополнительной информации о факте регистрации карты на этого покупателя.

4.4.4.3. Последующие оплаты зарегистрированной картой

Последовательность действий при последующей оплате зарегистрированной банковской картой имеет следующие основные шаги:

1. Посетитель интернет-магазина авторизуется на сайте магазина, магазин ставит ему в соответствие уникальный идентификатор **Customer_IDP**.
2. При вызове интернет-магазином формы оплаты заказа этого посетителя, магазин указывает помимо прочих параметров идентификатор покупателя **Customer_IDP**.
3. При переходе на страницу оплаты картой на сайте Uniteller процессинговый центр определяет, что у данного покупателя уже есть зарегистрированная карта.
4. Покупателю отображается упрощённая форма на странице оплаты картой, на которой присутствует текст, поясняющий ситуацию, и выводятся пиктограммы выбора карты для оплаты.
5. На пиктограмме зарегистрированной карты во всплывающей подсказке выводится её «маска». Также есть пиктограмма «**Банковская карта**» для оплаты «другой» (незарегистрированной) картой.
6. Покупатель имеет выбор — оплатить свой заказ при помощи указанной зарегистрированной картой, оплатить свой заказ другой картой или отменить регистрацию этой карты (удалить данные зарегистрированной карты).

7. В первом случае покупатель на странице оплаты вводит только CVV2/CVC2 карты и, возможно, проходит 3DSecure- авторизацию.
8. Во втором случае покупатель переходит к стандартной странице оплаты, на которой вводит все данные новой карты. Если данные новой карты в точности соответствуют данным уже зарегистрированной карты, регистрация новой карты не производится (такая карта уже зарегистрирована в системе). Если при этом галочка **«Сохранить данные карты»** установлена, то статус карты меняется на «активна» (например, если был статус «заблокирована»), если галочка не установлена, то статус не меняется.
9. В третьем случае процессинговый центр удаляет связь зарегистрированной карты и данного покупателя. Покупатель переходит к стандартной странице оплаты картой, на которой нужно указать все данные карты. См. также п. 4.4.4.7 «Удаление регистрации карты» на стр. 40.

4.4.4.4. Выбор зарегистрированной карты на стороне Uniteller при оплате

Последовательность действий при выборе на сайте Uniteller из списка зарегистрированных карт карты для осуществления оплаты имеет следующие основные шаги:

1. Посетитель интернет-магазина авторизуется на сайте магазина, магазин ставит ему в соответствие уникальный идентификатор **Customer_IDP**.
2. При вызове интернет-магазином формы оплаты заказа этого посетителя, магазин указывает помимо прочих параметров идентификатор покупателя **Customer_IDP**.
3. При переходе на страницу оплаты картой на сайте Uniteller процессинговый центр определяет, что у данного покупателя уже есть несколько зарегистрированных карт.
4. Покупателю отображается упрощенная форма на странице оплаты картой, на которой присутствует текст, поясняющий ситуацию, и выводится список выбора карты для оплаты.
5. В списке выбора карты для оплаты показаны «маски» отображения всех активных карт, зарегистрированных на этого покупателя этого интернет-магазина, и есть пункт **«Оплатить другой картой»**.
6. Покупатель может выбрать для оплаты любую карту из списка или выбрать пункт **«Оплатить другой картой»**.
7. В первом случае покупатель на странице оплаты вводит только CVV2/CVC2 карты и, возможно, проходит 3DSecure-авторизацию.
8. Во втором случае покупатель переходит к стандартной странице оплаты, на которой вводит все данные новой карты. Если данные новой карты в точности соответствуют данным какой-либо из уже зарегистрированных карт, регистрация новой карты не производится. Если при этом галочка **«Сохранить данные карты»** установлена, то статус карты меняется на «активна», если галочка не установлена, то статус не меняется.
9. Также покупатель имеет возможность удалить любую карту из списка зарегистрированных карт (см. также п. 4.4.4.7 «Удаление регистрации карты» на стр. 40).
10. Если покупатель удаляет последнюю зарегистрированную карту, он автоматически переходит на стандартную страницу оплаты, и дальнейшие действия не отличаются от сценария «Первая оплата картой после авторизации в интернет-магазине» (см. п. 4.4.4.2 на стр. 36). В том числе, покупатель может тут же зарегистрировать новую карту.

4.4.4.5. Регистрация карты по случайной сумме

Чтобы предоставить возможность регистрировать карты по случайной сумме интернет-магазину необходимо разместить на своём сайте соответствующую форму перехода к регистрации карты, пример шаблона которой показан ниже.

Пример HTML-шаблона формы перехода к регистрации по случайной сумме показан ниже:

```
<form action="https://wpay.uniteller.ru/pay/" method="POST">
<input type="hidden" name="Shop_IDP" value="Ваш Shop_ID">
<input type="hidden" name="Order_IDP" value="Ваш Order_ID">
<input type="hidden" name="Lifetime" value="Время жизни формы">
<input type="hidden" name="Customer_IDP" value="Идентификатор посетителя">
<input type="hidden" name="Signature" value="Подпись формы">
<INPUT TYPE="SUBMIT" NAME="Submit" value="Зарегистрировать">
<input type="hidden" name="Card_Registration" value="1">
<input type="hidden" name="URL_RETURN_OK" value="http://example.com/pay/ok/">
<input type="hidden" name="URL_RETURN_NO" value="http://example.com/pay/fail/">
</form>
```

где:

- **Shop_IDP** — идентификатор интернет-магазина. Доступен Мёрчанту в Личном кабинете на странице «Точки продажи компании» (пункт меню «Точки продажи») в столбце **Uniteller Point ID**.
- **Order_IDP** — номер заказа в системе расчётов интернет-магазина или любой уникальный идентификатор, по которому в дальнейшем интернет-магазин может запрашивать результат авторизации по заказу. Может быть любой строкой максимальной длиной 127 символов.
- **Lifetime** — время жизни формы в секундах, начиная с момента её показа. Должно быть целым положительным числом. Если Покупатель использует форму дольше указанного времени, то форма оплаты будет считаться устаревшей, и платёж не будет принят. Покупателю в этом случае будет предложено вернуться на сайт Мёрчанта для повторного выполнения заказа.
- **Customer_IDP** — уникальный идентификатор покупателя.
- **Card_Registration** — признак показа формы регистрации карты по случайной сумме. Для показа этой формы должен быть равен '1'. В случае отсутствия или любого другого значения на сайте Uniteller будет показана форма оплаты картой.
- **Signature** — подпись, гарантирующая неизменность критичных данных формы. **Signature** вычисляется по следующему алгоритму:

```
Signature = uppercase(md5(md5(Shop_IDP) + & + md5(Order_IDP) + & + md5(Lifetime) + & + md5(Customer_IDP) + & + md5(password)))
```

где:

- **password** — пароль из раздела «Параметры Авторизации» Личного кабинета системы Uniteller.
- '+' — операция конкатенации текстовых строк (все строки преобразуются в байты в кодировке ASCII).
- '&' — символ «разделитель полей». Если необязательный параметр не передаётся в форме, соответствующий этому полю (следующий за ним) знак '&' сохраняется в строке для вычисления **Signature**.
- **md5** — криптографическая хеш-функция (символы в нижнем регистре).
- **uppercase** — функция приведения к верхнему регистру.
- **Lifetime** — время жизни формы в секундах. Если **Lifetime** не передаётся в форме, то следует его принять пустой строкой (в последовательность подставляется значение md5 от пустой строки — d41d8cd98f00b204e9800998ecf8427e).

Последовательность действий при регистрации карты по случайной сумме имеет следующие основные шаги:

1. Посетитель интернет-магазина авторизуется на сайте магазина, магазин ставит ему в соответствие уникальный идентификатор **Customer_IDP**.
2. На сайте интернет-магазина посетителю предлагается зарегистрировать карту по случайной сумме. После подтверждения посетителем своего согласия на сайте интернет-магазина формируется форма перехода к регистрации по случайной сумме, в которой указываются идентификатор магазина **Shop_IDP**, идентификатор покупателя **Customer_IDP** и параметр **Card_Registration='1'** (пример формы см. выше). Запрос с параметрами формы передаётся на сайт Uniteller.
3. На сайте Uniteller, посетителю отображается страница регистрации карты, на которой требуется указать все данные карты. Сумма к оплате генерируется автоматически в размере от 0.01 до 9.99 руб., независимо от того, какое значение было передано в форме. Для всех эквайеров, поддерживающих преавторизацию платежа, платёж проводится с параметром **Preauth** (платёж с преавторизацией, см. п. 4.2 «Преавторизация платежа» на стр. 28), для остальных проводится обычная блокировка средств. В отличие от страницы оплаты, на странице регистрации сумма платежа не отображается покупателю и не присылается по электронной почте. На странице регистрации имеется поясняющий текст.
4. Если попытка оплаты завершена успешно, карта регистрируется в процессинговом центре на этого покупателя этого интернет-магазина. Данным карты присваивается уникальный идентификатор **Card_IDP** и формируется соответствующая «маска» отображения. Карте присваивается статус «не подтверждена».
5. Результатом успешной попытки оплаты является блокировка на карте покупателя суммы, случайно сгенерированной для регистрации карты. Покупателю требуется самостоятельно через инструменты, предоставленные банком-эмитентом (SMS-оповещение, личный кабинет на сайте банка, звонок в клиентскую службу и т. д.), узнать сумму, заблокированную на его карте в результате платежа. Покупателю отображается страница с текстом, поясняющим ситуацию.
6. Интернет-магазину не сообщается никакой дополнительной информации о факте регистрации карты на этого покупателя, но сообщается про статус попытки оплаты (см. п. 4.2.2 «Проведение преавторизации платежа» на стр. 28).
7. Если попытка оплаты завершена успешно, то интернет-магазин может получить при помощи запроса «Получение результатов авторизации» (см. п. 4.6 «Получение результатов авторизации» на стр. 49) информацию о финансовой операции с указанием суммы оплаты (**Subtotal_P**) и значения параметра **Card_IDP** — идентификатора зарегистрированной карты. Поле **Card_IDP** присутствует только для успешных операций регистрации по случайной сумме.
8. Покупатель интернет-магазина на сайте магазина вводит заблокированную сумму для подтверждения регистрации карты. Интернет-магазин сам проверяет правильность введённой суммы для соответствующей карты и сам ограничивает количество попыток (рекомендуется предоставлять не более 5 попыток).
9. Если покупатель успешно прошёл проверку, то интернет-магазин должен послать запрос на изменение статуса карты с «не подтверждена» на «активна» (см. п. 4.4.4.10 «Изменение статуса регистрации карты» на стр. 40).
10. Если покупатель не прошёл проверку (исчерпано количество попыток или истёк максимальный срок), то интернет-магазин должен послать запрос на удаление регистрации карты (см. п. 4.4.4.10 «Изменение статуса регистрации карты» на стр. 40).

11. После того как покупатель подтвердит или не подтвердит регистрацию карты или по истечении определённого срока (рекомендуется не более 6 часов) интернет-магазин должен отменить платёж (см. п. 4.5 «Отмена платежа и возврат средств» на стр. 45, п. 4.5.3 «Отмена платежа с преавторизацией» на стр. 49).

4.4.4.6. Выбор зарегистрированной карты на стороне интернет-магазина при оплате

Последовательность действий при выборе на сайте интернет-магазина из списка зарегистрированных карт карты для осуществления оплаты имеет следующие основные шаги:

1. Посетитель интернет-магазина авторизуется на сайте магазина, магазин ставит ему в соответствие уникальный идентификатор **Customer_IDP**.
2. Посетителю показывается список зарегистрированных активных карт, из которого он должен выбрать карту для осуществления оплаты. Карты в списке отображаются в виде «масок» отображения. На форме оплаты для этого покупателя интернет-магазин указывает идентификатор магазина **Shop_IDP**, идентификатор покупателя **Customer_IDP** и идентификатор **Card_IDP** карты, выбранной покупателем.
3. При переходе на сайт Uniteller покупателю отображается упрощённая форма на странице оплаты картой, выводятся поясняющий текст и «маска» ранее выбранной карты.
4. Покупатель на странице оплаты вводит только CVV2/CVC2 карты, и, возможно, проходит 3DSecure -авторизацию.

4.4.4.7. Удаление регистрации карты

При выборе покупателем действия по удалению ранее зарегистрированной карты интернет-магазин направляет в Uniteller соответствующий запрос с указанием **Card_IDP** карты, регистрацию которой требуется удалить (см. п. 4.4.4.10 «Изменение статуса регистрации карты» на стр. 40). Операция может завершиться успехом или неудачей.

4.4.4.8. Блокировка зарегистрированной карты

При выборе покупателем действия по блокировке ранее зарегистрированной карты интернет-магазин направляет в Uniteller соответствующий запрос с указанием **Card_IDP** карты, оплаты по которой требуется заблокировать (см. п. 4.4.4.10 «Изменение статуса регистрации карты» на стр. 40). В случае успеха статус карты меняется на «заблокирована». Заблокирована может быть только активная карта.

4.4.4.9. Разблокировка зарегистрированной карты

При выборе покупателем действия по разблокировке ранее зарегистрированной карты интернет-магазин направляет в Uniteller соответствующий запрос с указанием **Card_IDP** карты, оплаты по которой требуется разблокировать (см. п. 4.4.4.10 «Изменение статуса регистрации карты» на стр. 40). В случае успеха статус карты меняется на «активна».

4.4.4.10. Изменение статуса регистрации карты

Для того чтобы со стороны интернет-магазина удалить регистрацию карты или изменить её статус (подтвердить, заблокировать, разблокировать), нужно выполнить запрос на адрес: <https://wpay.uniteller.ru/card/> с GET- или POST-параметрами, указанными в табл. 11 и табл. 12.

Табл. 11 — Обязательные параметры запроса изменения статуса регистрации карты

№	Параметр	Тип	Описание
1	Shop_IDP	Строка до 64 символов	Идентификатор точки продажи в системе Uniteller.
2	Login	Строка до 64 символов	Логин, выданный Мёрчанту при создании учётной записи в системе Uniteller.
3	Password	Строка 80 символов	Пароль, выданный Мёрчанту при создании учётной записи в системе Uniteller
4	Card_IDP	Строка до 128 символов	Идентификатор зарегистрированной карты.
5	Customer_IDP	Может быть любой строкой максимальной длиной 64 символа.	Идентификатор пользователя, используемый некоторыми интернет-магазинами.
6	Action	Возможные значения: 1 – подтвердить регистрацию; 2 – удалить регистрацию; 3 – заблокировать карту; 4 – разблокировать карту.	Действие, которое нужно сделать с картой.

Табл. 12 — Необязательные параметры запроса изменения статуса регистрации карты

№	Параметр	Тип	Значение по умолчанию	Описание
1	Format	Возможные значения: 1 (CSV); 2 (WDDX); 3 (XML).	1	Формат выдачи результата. В формате 1 поля разделены точкой с запятой.

Ответ на запрос будет содержать поля, указанные в табл. 13.

Табл. 13 — Поля ответа на запрос изменения статуса регистрации карты

№	Поле	Тип	Значение
1	ErrorCode	Число (целое не отрицательное)	0, если запрос прошёл успешно, или номер ошибки в случае ошибки
2	ErrorMessage	Строка	Текстовое описание ошибки

В случае возникновения ошибки в ответе на запрос будут возвращены 2 параметра: **firstcode** и **secondcode**, значения которых приведены в табл. 14.

Табл. 14 — Возможные сообщения об ошибках при запросе изменения статуса регистрации карты

Код (firstcode)	Сообщение (secondcode)	Расшифровка
1	Authentication error	Некорректные данные авторизации (Login, Password)

Код (firstcode)	Сообщение (secondcode)	Расшифровка
3	Mandatory parameter '%fieldName%' is not present in the request	Не указан обязательный параметр (%fieldName% — имя параметра)
5	Field %fieldName% has bad format	Неверный формат значения или значение не входит в область допустимых (%fieldName% — имя параметра)
15	The operation failed	По некоторым причинам операция была прервана. Попробуйте в другой раз.
30	Card not found	Карта не найдена
31	Card can't be activated because it's blocked	Карта не может быть активирована, так как она заблокирована
32	Card can't be blocked because it's not confirmed	Карта не может быть заблокирована, так как она неактивна
33	Card can't be unblocked because it's not confirmed	Карта не может быть разблокирована, потому что она не активна
34	TempCard not found	Карта с таким TempCard_IDP (для заданного Shop_IDP) не найдена
35	Card is already registered	Карта уже зарегистрирована

4.4.4.11. Получение списка зарегистрированных карт

Для получения списка зарегистрированных карт конкретного покупателя (заданного **Customer_IDP**) интернет-магазин должен направить запрос на сайт Uniteller, в ответе на который будет передан список зарегистрированных карт (**Card_IDP**), для каждой из которых возвращается «маска» отображения карты (тип карты и маскированный номер), статус карты, идентификатор банка-эквайера (возможны названия на английском языке и ошибки, связанные с кодировкой символов), а также признак — является ли карта «своей» или «чужой» для объявленного банка-эквайера.

Запрос получения списка зарегистрированных карт выполняется на адрес: <https://wpay.uniteller.ru/card/> с GET- или POST-параметрами, указанными в табл. 15 и табл. 16.

Табл. 15 — Обязательные параметры запроса получения списка зарегистрированных карт

№	Параметр	Тип	Описание
1	Shop_IDP	Строка до 64 символов	Идентификатор точки продажи в системе Uniteller.
2	Login	Строка до 64 символов	Логин, выданный Мёрчанту при создании учётной записи в системе Uniteller.
3	Password	Строка 80 символов	Пароль, выданный Мёрчанту при создании учётной записи в системе Uniteller

№	Параметр	Тип	Описание
4	Customer_IDP	Может быть любой строкой максимальной длиной 64символа.	Идентификатор пользователя, используемый некоторыми интернет-магазинами.

Табл. 16 — Необязательные параметры запроса получения списка зарегистрированных карт

№	Параметр	Тип	Значение по умолчанию	Описание
1	Format	Возможные значения: 1 (CSV); 2 (WDDX); 3 (XML).	1	Формат выдачи результата. В формате 1 поля разделены точкой с запятой.

В случае успеха для каждой карты будет возвращена запись из 5 полей, указанных в табл. 17.

Табл. 17 — Поля ответа на запрос получения списка зарегистрированных карт в случае успеха

№	Поле	Тип	Значение
1	Card_IDP	Целое число до 128 цифр	Идентификатор зарегистрированной карты
2	CardType	Строка	Тип платёжной системы карты (visa, mastercard, dinnersclub, jcb)
3	CardNumber	Строка	Маскированный номер карты. Первые 6 цифр и последние 4 цифры номера карты (PAN), соединённые звёздочками
4	CardStatus	Число (целое неотрицательное)	Состояние привязки карты: (0 — не подтверждена, 1 — активна, 2 — заблокирована).
5	AcquirerID	Строка	Идентификатор банка-эквайера в системе Uniteller
6	IsOwnCard	Логический	Признак «своя»/«чужая» для предъявленной к оплате карты у выбранного эквайера. («0» — «чужая», «1» — «своя»)

При запросе списка зарегистрированных карт может быть передан необязательный параметр **Selected_Card**, в значении которого передаётся идентификатор карты, если требуется получить информацию только по ней (а не по всему списку карт). Если передан некорректный параметр **Selected_Card** (например, указанный идентификатор не существует), будет возвращён пустой список карт.

В случае возникновения ошибки в ответе будут поля, указанные в табл. 18.

Табл. 18 — Поля ответа на запрос получения списка зарегистрированных карт в случае ошибки

№	Поле	Тип	Значение
1	ErrorCode	Число (целое не отрицательное)	Номер ошибки
2	ErrorMessage	Строка	Текстовое описание ошибки

Возможные сообщения об ошибках соответствуют указанным в табл. 14 на стр. 41.

4.4.4.12. Привязка карт по реестру

В случае привязки карт «по реестру» карта регистрируется в системе Uniteller на основе данных, полученных от Банка-эмитента, и данных о сопоставлении карты и покупателя интернет-магазина, полученной от магазина.

Для того чтобы связать полученную от банка информацию о карте(ах) с конкретным пользователем интернет-магазина, магазин должен направить в Uniteller запрос, в котором передать идентификатор магазина **Shop_IDP**, а также пару значений параметров **Customer_IDP** и **TempCard_IDP** (то значение, которое было получено магазином от банка при выпуске карты). В результате обработки запроса все сохранённые в Uniteller карты с **TempCard_IDP** привязываются к данному **Customer_IDP** и получают статус «активна». На запрос магазин может получить либо положительный ответ, либо сообщение об ошибке. Сообщение об ошибке будет получено в случае, если ни одна карта не была привязана для заданных значений **Shop_IDP**, **Customer_IDP**, **TempCard_IDP**.

Для того чтобы связать полученные от банка карты с конкретным пользователем магазина, интернет-магазин должен выполнить запрос на адрес:

<https://wpay.uniteller.ru/card/> с GET- или POST-параметрами, указанными в табл. 19 и табл. 20.

Табл. 19 — Обязательные параметры запроса привязки карт «по реестру»

№	Параметр	Тип	Описание
1	Shop_IDP	2 числа, разделённые дефисом: Первое от 10 до 15 разрядов; Второе от 1 до 11 разрядов.	Идентификатор точки продажи в системе Uniteller.
2	Login	Строка до 64 символов	Логин, выданный Мёрчанту при создании учётной записи в системе Uniteller.
3	Password	Строка 80 символов	Пароль, выданный Мёрчанту при создании учётной записи в системе Uniteller
4	Customer_IDP	Может быть любой строкой максимальной длиной 64символа.	Идентификатор пользователя, используемый некоторыми интернет-магазинами.
5	TempCard_IDP	Может быть любой строкой максимальной длиной 128 символов.	Идентификатор карты для данного Shop_IDP, например, инвентарный номер выпущенной карты. Генерируется либо магазином, либо банком.

Табл. 20 — Необязательные параметры запроса привязки карт «по реестру»

№	Параметр	Тип	Значение по умолчанию	Описание
1	Format	Возможные значения: 1 (CSV); 2 (WDDX); 3 (XML).	1	Формат выдачи результата. В формате 1 поля разделены точкой с запятой.

Ответ на запрос будет содержать поля, указанные в табл. 21.

Табл. 21 — Поля ответа на запрос привязки карт «по реестру»

№	Поле	Тип	Значение
1	ErrorCode	Число (целое не отрицательное)	0 – в случае успеха или номер ошибки
2	ErrorMessage	Строка	Текстовое описание ошибки

Возможные сообщения об ошибках соответствуют указанным в табл. 14 на стр. 41.

4.5. Отмена платежа и возврат средств

4.5.1. Суть терминов «отмена платежа» и «возврат средств». Особенности реализации отмен у разных банков-эквайеров

Оплата платежа банком-эквайером происходит в несколько этапов. Наиболее важными для нас являются:

1. Блокировка средств на карте покупателя (авторизация) — этап после всех проверок плательщика со стороны Uniteller и банка-эквайера, в результате которого средства, необходимые для оплаты заказа, резервируются (блокируются) на счёте покупателя. Если блокировка средств проведена, то есть все основания ожидать, что заказ будет оплачен.
2. Списание средств — этап, в результате которого денежные средства фактически списываются со счёта Покупателя и зачисляются на счёт Продавца.

Этапы блокировки средств и списания происходят в указанной последовательности и могут быть разнесены по времени.

Под термином «**Отмена платежа**» («отмена блокировки средств», «отмена авторизации») подразумевается снятие блокировки с ранее заблокированных денежных средств на счёте Покупателя. Последующего списания средств не происходит (если разблокирована вся сумма) или оно происходит на оставшуюся сумму (если разблокирована только часть первоначальной суммы).

Под термином «**Возврат средств**» подразумевается операция, обратная списанию средств, то есть возврат ранее переведённых средств со счёта Продавца на счёт Покупателя (обратный платёж). О возврате средств можно говорить только после проведённого списания средств.

Запрос для инициирования в системе Uniteller возврата средств идентичен запросу отмены платежа (см. ниже в этом разделе). Если на момент обработки этого запроса деньги по операции продажи ещё не были списаны, то будет инициирована операция отмены платежа, если же деньги уже были списаны, то будет инициирована операция возврата средств.

Для эквайеров ОАО «ТрансКредитБанк», «Банк Москвы», ЗАО «КОКК», ООО «МультиКарта», ОАО «АК БАРС», а также для оплат с помощью Яндекс.Деньги поддерживаются частичные отмены платежа (возврат средств) — отмены на сумму, меньшую суммы первоначального платежа (или первоначальную сумму за вычетом уже произведённых отмен (текущий баланс)). Для всех остальных эквайеров поддерживаются только отмены на полную сумму платежа.

Для эквайера ОАО «ТрансКредитБанк», ЗАО «КОКК» (см. п. 4.5.2.2 ниже), ООО «МультиКарта» и для оплат Яндекс.Деньгами поддерживаются многократные отмены (возвраты) по первоначальному платежу, для всех остальных эквайеров разрешена только одна отмена.

4.5.2. Запрос отмены платежа и возможные форматы ответа

4.5.2.1. Общий вид запроса отмены платежа

Для отмены совершённой продажи необходимо выполнить POST- или GET-запрос на адрес: <https://wpay.uniteller.ru/unblock/> с указанием параметров, указанных в табл. 22 и табл. 23.

В ответ вернутся значения, перечисленные в параметре **S_FIELDS** (см. п. 7.1 «Возможные поля параметра S_FIELDS» на стр. 60).

Формат ответа будет зависеть от переданного параметра **Format**:

- 1 – Ответ в формате CSV. В качестве разделителя используется точка с запятой «;».
- 2 – Ответ в формате WDDX.
- 3 – Ответ в формате XML.
- 4 – Ответ в формате SOAP.

Если параметр **Format** не установлен, ответ будет в формате CSV.

Табл. 22 — Обязательные параметры запроса отмены платежа

№	Параметр	Тип	Описание
1	Billnumber	12 цифр	Номер платежа в системе Uniteller
2	Shop_ID	Строка до 64 символов	Идентификатор точки продажи в системе Uniteller. Доступен Мёрчанту в Личном кабинете в пункте меню «Точки продажи», столбец Uniteller Point ID .
3	Login	Строка до 64 символов	Логин, выданный Мёрчанту при создании учётной записи в системе Uniteller.
4	Password	80 символов	Пароль, выданный Мёрчанту при создании учётной записи в системе Uniteller

Табл. 23 — Необязательные параметры запроса отмены платежа

№	Параметр	Тип	Значение по умолчанию	Описание
1	Subtotal_P	Число	Сумма авторизации	Сумма возврата средств. Должна быть в диапазоне от 0,01 руб. до суммы платежа включительно. В качестве десятичного разделителя используется точка.
2	Currency	3-символа	Код валюты авторизации	Код валюты отмены или возврата средств. Может быть использован только код валюты авторизации.

№	Параметр	Тип	Значение по умолчанию	Описание
3	RVRReason	1 (отказ магазина от операции), 2 (отказ держателя от операции), 3 (мошенническая операция)	1	Причина отмены операции
4	Language	2 символа	ru	Язык выдачи результатов
5	Format	1 (CSV), 2 (WDDX), 3 (XML), 4 (SOAP).	1	Формат выдачи результата. В формате 1 поля разделены точкой с запятой.
6	S_FIELDS		пустое значение (или не передаётся) — все поля	Набор информационных полей, возвращаемых в ответе на запрос. Формат представления информации в ответе определяется параметром Format . (Подробно поддерживаемые поля параметра S_FIELDS описаны в п. 7.1 «Возможные поля параметра S_FIELDS» на стр. 60)

В случае возникновения ошибки будет возвращено 2 параметра: **firstcode** и **secondcode**, значения которых приведены в табл. 24.

Табл. 24 — Возможные сообщения об ошибках при запросе отмены платежа

Код (firstcode)	Сообщение (secondcode)	Расшифровка
1	Authentication error	Некорректные данные авторизации (Login, Password)
3	Mandatory parameter '%fieldName%' is not present in the request	Не указан обязательный параметр (%fieldName% - имя параметра)
4	Bill not found	Не найден платёж
5	Field %fieldName% has bad format	Неверный формат значения или значение не входит в область допустимых (%fieldname% - имя параметра)
10	S_FIELDS contains field '%name%' which is not allowed	В поле S_FIELDS присутствует не поддерживаемый параметр. %name% - код параметра
15	The operation failed	По некоторым причинам операция была прервана. Попробуйте в другой раз.
16	The order has already been cancelled	Транзакция была отменена ранее
17	Authorization reversal is not allowed	Невозможно выполнить отмену.
35	Partial return is not supported	Частичный возврат не поддерживается

4.5.2.2. Особенности отмены платежа для эквайера ЗАО «КОКК»

При работе с ЗАО «КОКК» отмены платежа имеют следующие особенности:

- Блокировка средств на карте покупателя проводится эквайером on-line, а последующая операция списания заблокированных средств происходит с задержкой и проводится в течение следующего дня.
- Первая отмена блокировки средств (полная или частичная), проведённая до операции списания средств, проводится эквайером on-line, а все последующие отмены блокировки средств проводятся уже не on-line, а через 2–3 дня после операции списания средств (при этом списание происходит на корректную сумму, с учётом всех сделанных к этому моменту заявок на отмену блокировки средств).
- Если сделаны несколько отмен блокировки средств, в результате которых выбрана вся сумма первоначального платежа, то происходит существенная задержка с отменой блокировки (до 30 дней). Если после первой отмены блокировки средств требуется возврат всех оставшихся средств по первоначальному платежу, рекомендуется дожидаться списания средств (в течение следующего дня) и после этой операции инициировать возврат средств (см. п. 4.5.4 «Возврат средств» ниже) на требуемую сумму, который осуществляется в течении 2-3 дней.

4.5.2.3. Особенности отмены платежа электронной валютой Яндекс.Деньги

Отмена платежа, произведённого электронной валютой Яндекс.Деньги, имеет следующие особенности:

- В параметре **Billnumber** должен указываться номер операции с электронной валютой (см. в Личном кабинете Uniteller > страница «**Подробная информация о заказе**» (для заказа, оплачиваемого электронной валютой) > область «**Список операций с электронной валютой:**» > столбец «**Номер операции**»; строка от 20 до 30 символов).
- Должен быть указан параметр **Emoney=1** (для операций по карте данный параметр не используется).
- Должен быть указан параметр **Cause** (для операций по карте данный параметр не используется) — причина возврата средств (строка длиной до 255 символов; может содержать русские/латинские буквы, цифры, пробелы, знаки «-», «:», «;», «(», «)»).
- Может использоваться параметр **Subtotal_P** для указания суммы частичного возврата.
- При передаче параметра **EMoney** код валюты (значение параметра **Currency**) не учитывается.
- Сообщение об ошибке с кодом **17 «Authorization reversal is not allowed»** меняется на «**Reversal is not allowed**» — эта ошибка будет выдана при попытке вернуть деньги не по операции с Яндекс.Деньгами.
- Если он-лайн возврат не прошёл, то выдается ошибка с кодом **18 «Reversal in progress»** — при получении такой ошибки нужно через некоторое время выполнять запрос получения результатов авторизации для данного заказа (см. п. 4.6.2 «Запрос результата авторизации» на стр. 51).
- По-умолчанию (если в запросе не передаётся параметр **S_FIELDS**) в ответе на запрос будут возвращены следующие параметры: **OrderNumber, Comment, Date, Total, Currency, IPAddress, Status, PacketDate, PaymentType=3, BillNumber**.
- Значения параметров **Response_Code, Recommendation, Message, CardType, CardNumber, LastName, FirstName, MiddleName, Address, Email, ApprovalCode, CVC2, BankName, Error_Code, Error_Comment** будут пустыми.

4.5.3. Отмена платежа с преавторизацией

Мёрчант имеет возможность в любой момент времени отменить заказ (из Личного кабинета или отправив запрос на определённый URL) с помощью операции «Отмена платежа». В случае если Мёрчант отменяет операцию, по которой уже было отправлено подтверждение, но еще не отправлялась команда завершения платежа, то операция будет отменена, а команда завершения платежа отправляться не будет. Если Мёрчант отменяет операцию, по которой уже отправлялась команда завершения платежа, то по такой операции будет выполнена команда возврата средств.

4.5.4. Возврат средств

В случае возникновения необходимости возврата средств Держателю карты в системе Uniteller возможна операция «Возврат средств». Возврат средств осуществляется только применительно к конкретной операции продажи.

Проведение возврата средств должен осуществлять уполномоченный сотрудник Мёрчанта, имеющий авторизованный доступ к Личному кабинету и надлежащим образом проинструктированный по вопросам безопасности при обращении с данными Держателей карт.

Операция возврата средств может быть инициирована или путём отсылки запроса на адрес: <https://wpay.uniteller.ru/unblock/>, или через Личный кабинет системы Uniteller.

Запрос для инициирования возврата средств идентичен запросу отмены платежа (см. п. 4.5.2 «Запрос отмены платежа и возможные форматы ответа» на стр. 46). Если на момент обработки этого запроса деньги по операции продажи ещё не были списаны, то будет инициирована операция отмены платежа, если же деньги уже были списаны, то будет инициирована операция возврата средств.

Порядок проведения операции «Возврат средств» через Личный кабинет описан в п. 5 «Порядок работы в Личном кабинете» (см. стр. 58).

4.6. Получение результатов авторизации

4.6.1. Уведомление сервера интернет-магазина о статусе оплаты

После успешной оплаты картой Покупателя система Uniteller уведомляет сервер интернет-магазина Мёрчанта об изменении статуса заказа на **authorized**.

Также уведомление отсылается в следующих случаях:

- выполнение транзакции по снятию блокировки средств;
- выполнение операции по возврату списанных средств;
- выполнение списания средств;
- оплата заказа в электронной платёжной системе.

Уведомление происходит путём отправки **HTTP POST** запроса на адрес, который Мёрчант задаёт в Личном кабинете системы Uniteller в параметре «**URL-адрес уведомления магазина**» на странице «**Редактирование точки продажи**» (раздел «**Точки продажи**»⁶). Запрос имеет параметры, указанные в табл. 25.

⁶ **Примечание:** При настройке тестового подключения на тестовом сервере ищите этот параметр на странице «**Редактирование интернет-магазина**» в разделе ЛК «**Договоры**».

Табл. 25 — Параметры запроса уведомления сервера интернет-магазина о статусе оплаты

№	Параметр	Описание
1	Order_ID	Номер заказа в системе расчётов интернет-магазина
2	Status	<p>Статус заказа. Статус заказа может принимать следующие значения:</p> <ul style="list-style-type: none"> • authorized — средства успешно заблокированы (выполнена авторизационная транзакция); • not authorized — средства не заблокированы (авторизационная транзакция не выполнена) по ряду причин. • paid — оплачен (выполнена финансовая транзакция или заказ оплачен в электронной платёжной системе); • canceled — отменён (выполнена транзакция разблокировки средств или выполнена операция по возврату платежа после списания средств). • waiting — ожидается оплата выставленного счёта. Статус используется только для оплат электронными валютами, при которых процесс оплаты может содержать этап выставления через систему Uniteller счёта на оплату и этап фактической оплаты этого счёта Покупателем, которые существенно разнесены во времени. <p>См. также Примечание 7 внизу страницы.</p>
3	Signature	<p>Цифровая подпись, которая вычисляется по алгоритму:</p> <pre>Signature = uppercase(md5(Order_ID + Status + password)),</pre> <p>где:</p> <ul style="list-style-type: none"> • password — пароль из раздела «Параметры Авторизации» Личного кабинета системы Uniteller. • '+' — операция конкатенации текстовых строк (все строки преобразуются в байты в кодировке ASCII). • md5 — криптографическая хеш-функция. • uppercase — функция приведения к верхнему регистру.

Если уведомление по каким-либо причинам не получено сервером интернет-магазина (например, в момент уведомления сервер недоступен), то система Uniteller сделает дополнительные попытки посылки уведомления. Всего (вместе с первым уведомлением, закончившимся неудачей) будет сделано 10 попыток уведомления сервера интернет-магазина за период около 6,5 мин. или больше (реальные интервалы между уведомлениями интернет-магазина зависят от загрузки системы Uniteller и размера очереди операций).

В случае, если все 10 попыток уведомить сервер интернет-магазина об изменении статуса оплаты не будут приняты, дальнейшие попытки прекращаются, а интернет-магазину для уточнения статуса интересующей оплаты следует самостоятельно инициировать запрос, как описано в п. 4.6.2 «Запрос результата авторизации» ниже.

⁷ **Примечание:** Обращаем ваше внимание на то, что в текущей версии сервиса Uniteller в **уведомлении** сервера интернет-магазина о статусе оплаты значения статусов передаются со строчной (маленькой) буквы (например, **authorized, paid** и др.), а в **ответе на запрос** результата авторизации — с заглавной (большой) (например, **Authorized, Paid** и др.).

4.6.2. Запрос результата авторизации

4.6.2.1. Общий вид запроса результата авторизации

Для того чтобы получить результат проведения авторизации, нужно выполнить запрос на адрес: <https://wpay.uniteller.ru/results/> (для ответа в формате SOAP адрес: <https://wpay.uniteller.ru/result/wsdl/>) с GET- или POST-параметрами, указанными в табл. 26 и табл. 27.

База данных платёжной системы Uniteller хранит информацию о финансовых транзакциях за последний год. Информация по более ранним транзакция, в том числе и запрос результата авторизации по ним, недоступна.

Формат ответа на этот запрос зависит от отправленного значения параметра **Format** (см. табл. 27 на стр. 52).

Возможные форматы ответа:

- CSV;
- «В скобках»;
- WDDX;
- XML;
- SOAP.

Подробное описание формата ответа приведено в п. 7.3 «Форматы ответов» (см. стр. 62).

Табл. 26 — Обязательные параметры запроса результатов авторизации

№	Параметр	Описание
1	Shop_ID	Идентификатор точки продажи в системе Uniteller. Доступен Мёрчанту в Личном кабинете на странице « Точки продажи компании » (пункт меню « Точки продажи ») в столбце Uniteller Point ID .
2	Login	Логин. Доступен Мёрчанту в Личном кабинете, пункт меню « Параметры Авторизации ».
3	Password	Пароль. Доступен Мёрчанту в Личном кабинете, пункт меню « Параметры Авторизации ».
4	Format (1 — CSV, 2 — WDDX, 3 — «в скобках», 4 — XML, 5 — SOAP)	Формат выдачи результата. Значением параметра могут быть числа в диапазоне 1–5. При значении 1 (формат=CSV) поля разделены разделителем, указанным в поле Delimiter (см. ниже), при значении 3 (формат=«в скобках») каждое поле заключено в разделители, указанные в OpenDelimiter и CloseDelimiter (см. ниже). Детальная информация о каждом из форматов представлена в п. «Форматы ответов» (см. стр. 62).

Табл. 27 — Необязательные параметры запроса результатов авторизации

№	Параметр	Описание
1	ShopOrderNumber	<p>Номер заказа в системе расчётов интернет-магазина. Если этот параметр указывается, то ответ содержит результат авторизации по указанному заказу.</p> <p>Если при запросе результатов авторизации по номеру заказа не указывается период операций (параметры Start... и End..., см. ниже), то возвращаются результаты за всю историю операций с этим номером заказа.</p>
2	Success	<p>Какие операции включать в ответ. Возможные значения: 0 — неуспешные (со статусами Canceled, Waiting, Not Authorized), 1 — успешные (со статусами Authorized, Paid), 2 — все. По умолчанию — 2.</p>
3	StartDay	<p>Параметры Start... (...Day, ...Month и т. д.) и End... определяют начало/конец периода (включительно), операции за который будут включены в отчёт.</p> <p>Ограничения при осуществлении запроса результатов авторизации указаны в п. 4.6.3 на стр. 55.</p> <p>Для получения результатов авторизации за определенный период задавать параметры Start... и End... следует одним из следующих образов:</p> <ul style="list-style-type: none"> • Не задавать ни одного параметра Start... и End... — будет выполнен запрос за последние 24 часа до момента запроса. • Задавать 3 параметра: Год, Месяц, День (без Часов и Минут; все 3 параметра обязательны) — будет выполнен запрос за полные сутки указанного периода. При отсутствии хотя бы одного из параметров будет возвращено сообщение об ошибке: You need to specify EndYear, EndMonth and EndDay to setEndDate. • Задавать 5 параметров: Год, Месяц, День, Час, Минуты (все 5 параметров обязательны) — будет выполнен запрос за указанный период с точностью до минут. При отсутствии хотя бы одного из параметров будет возвращено сообщение об ошибке: You need to specify EndYear, EndMonth, EndDay, EndHour and EndMin to set EndDate with time. <p>Если в запросе передан параметр Header=1, то в ответе на запрос заданный период будет возвращён параметрами StartDate и EndDate в формате dd.mm.yyyy hh:mm:ss.</p> <p>Если одновременно задан (с помощью параметров Start... и End...) период запрашиваемых операций и передан номер заказа (ShopOrderNumber), то эти 2 условия обрабатываются по принципу «И», то есть будет возвращён ответ по операциям, соответствующим заданному номеру заказа и совершённым в заданный период времени.</p>
4	StartMonth	
5	StartYear	
6	StartHour	
7	StartMin	
8	EndDay	
9	EndMonth	
10	EndYear	
11	EndHour	
12	EndMin	

№	Параметр	Описание
13	MeanType (0 — любым, 1 — VISA, 2 — MasterCard, 3 — DinersClub, 4 — JCB, 5 — AMEX (пока не поддерживается))	Операции с каким типом платёжного средства нужно включать в отчёт.
14	EMoneyType (значения см. в табл. 3 на стр. 18)	Операции с каким типом электронного платёжного средства нужно включать в отчёт.
15	ZipFlag (0 — браузер, 1 — файл, 2 — архивированный файл)	Режим выдачи результата. По умолчанию 0. В режиме 2 результат архивируется в файл формата *.zip.
16	Header (0 — нет, 1 — да)	Будут ли возвращаться в ответе параметры запроса. По умолчанию 0.
17	Header1 (0 — нет, 1 — да)	Будут ли возвращаться в ответе заголовки полей. По умолчанию 0.
18	Delimiter («;», «,», «:», «/»)	Разделитель полей в CVS-формате. Если указан другой символ, будет использован символ по умолчанию — «;».
19	OpenDelimiter («[», «{», «(»)	Открывающий разделитель полей в формате «в скобках». Если указан другой символ, будет использован символ по умолчанию — «[».
20	CloseDelimiter («]», «}», «)»)	Закрывающий разделитель полей в формате «в скобках». Если указан другой символ, будет использоваться символ по умолчанию — «]».
21	RowDelimiter («13», «10», «13,10», «10,13»)	Разделитель строк. По умолчанию «13,10».
22	S_FIELDS	Набор информационных полей, возвращаемых в ответе на запрос. Формат представления информации в ответе определяется параметром Format . (Подробно поддерживаемые поля параметра S_FIELDS описаны в п. 7.1 «Возможные поля параметра S_FIELDS» на стр. 60).

Значения параметров **MeanType** и **EMoneyType** определяют наборы данных в ответе на запрос (см. табл. 28).

Табл. 28 — Наборы данных в ответе на запрос результатов авторизации в зависимости от значений параметров MeanType и EMoneyType

№	Значение параметра MeanType	Значение параметра EMoneyType	Набор данных
1	Не передаётся	Не передаётся	Список всех операций по картам и электронным валютам
2	0	Не передаётся	Список всех операций только по картам
3	N (целочисленный идентификатор)	Не передаётся	Список всех операций по указанному типу карт
4	Не передаётся	0	Список всех операций только по электронным валютам
5	Не передаётся	N (целочисленный идентификатор)	Список всех операций по указанному типу электронной валюты
6	0	0	Список всех операций по картам и электронным валютам
7	N (целочисленный идентификатор)	0	Список всех операций по электронным валютам и операции по указанному типу карт
8	0	N (целочисленный идентификатор)	Список всех операций по картам и операции по указанному типу электронной валюты
9	N (целочисленный идентификатор)	N (целочисленный идентификатор)	Список операций по указанному типу карт и по указанному типу электронной валюты

В ответе на запрос результата авторизации будут возвращены данные последней транзакции по каждому заказу (согласно запросу), независимо от того, сколько попыток оплаты и с какими результатами было произведено по каждому из них.

Примеры ответов на запрос результата авторизации приведены в п. 7.3.1 «Запрос состояния транзакции» на стр. 62.

Обращаем ваше внимание на то, что текущая версия сервиса Uniteller имеет особенность с использованием строчных/заглавных букв в написании статусов платежа. См. примечание 7 на стр. 50.

4.6.2.2. Особенности запроса результата авторизации платежа электронной валютой

Для операций по оплате заказа с помощью электронной валюты, помимо общих данных о заказе (**OrderNumber**, **Comment**, **Date**, **Total**, **Currency**, **IPAddress**, **Status**, **PacketDate**) и данных, относящихся к электронной валюте (**PaymentType=3** (оплата с помощью электронной валют), **EMoneyType** (тип электронной валюты), **EOrderData** (данные заказа, выставленного в электронной платежной системе (опционально))), будет возвращён параметр **BillNumber** — уникальный номер операции с электронной валютой.

4.6.2.3. Особенности запроса результатов авторизации платежа для оплат авиабилетов через ГДС

Подробная информация об организации в системе Uniteller оплат, связанных с авиаперевозками, приведена в Приложении к этому техническому порядку — «**Дополнительные функции для оплаты авиаперевозок**».

Для платежей, связанных с оплатой авиаперевозок через системы ГДС, ответ на запрос результатов авторизации содержит 2 записи (оплата комиссионного вознаграждения и оплата билетов). Возвращаемый параметр `gds_payment_purpose_id` (назначение платежа через ГДС) имеет значение: 10 или 20 для оплаты комиссионного вознаграждения Агентства и платежа за билеты соответственно. Для всех остальных платежей этот параметр будет пустым.

4.6.3. Ограничения при осуществлении запроса результатов авторизации

На выполнение запросов результатов авторизации накладываются следующие ограничения:

- Частота запросов не должна превышать 1 запроса в 5 сек.
- При запросе результатов авторизации с указанием периода, операции за который будут включены в отчёт (параметры **Start...** и **End...**), длительность указанного периода не может превышать 7 суток, в противном случае запрос не будет выполнен с сообщением об ошибке. Если параметры **Start...**, **End...** не задаются, то по умолчанию запрос выполняется за последние 24 часа до момента запроса.

4.7. Автоматический контроль статусов заказов

4.7.1. Общая информация об автоматическом контроле статуса заказов

В системе Uniteller реализована функция автоматического контроля статуса заказа в информационной системе Мерчанта.

Многие Мерчанты (клиенты Uniteller) имеют собственные мощные информационные системы, отслеживающие состояние заказов своих клиентов. Компания Uniteller заинтересована в том, чтобы состояния (статусы) заказов, созданных в магазинах Мерчантов и переданных для оплаты в Uniteller, были синхронизированы между платёжной системой Uniteller и информационной системой Мерчанта. Более того, отсутствие такой синхронизации в некоторых случаях препятствует отслеживанию актуальности заказов, направленных в Uniteller для оплаты, что может приводить к ошибочным оплатам и нерациональному использованию ресурсов для отмены этих оплат. Например, заказ, направленный Мерчантом в Uniteller для оплаты, может быть по каким-то причинам быстро отменён Мерчантом, но, не имея этой информации, сервис Uniteller будет продолжать оплату этого заказа, пока оплата не завершится. Для дополнительного контроля подобных ситуаций в системе Uniteller реализован автоматический контроль статуса заказа.

Функция автоматического контроля статуса заказов имеет следующий общий алгоритм:

- После получения Uniteller от Мерчанта запроса на оплату и успешной блокировки средств по заказу через настраиваемый промежуток времени (по умолчанию 10 мин.) сервер Uniteller делает запрос на сервер Мерчанта о статусе оплачиваемого заказа.
- В зависимости от полученного от сервера Мерчанта ответа предпринимаются следующие действия:
 - Если статус заказа у Мерчанта — «**Оплачен**», то никакие дополнительные действия не требуются и оплата заказа продолжается до конца по обычной схеме.
 - Если статус заказа у Мерчанта — «**Аннулирован**», то это означает, что заказ уже неактуален, Uniteller делает автоматическую разблокировку средств на карте и отправляет Мерчанту по e mail письмо с уведомлением о том, что «оплата пришла с

задержкой, средства вернули плательщику».

- Если статус заказа у Мерчанта — **«Новый»**, то это означает, что Мерчант не знает об оплате заказа. Uniteller повторно высылает Мерчанту стандартное уведомление о статусе оплаты, и дополнительно высылает по e-mail на указанный адрес Мерчанта письмо, информирующее о том, что заказ оплачен.
- Если сервер Мерчанта не ответил на запрос статуса заказа (или формат ответа неверен), то Uniteller отправляет по e-mail на указанный адрес письмо, информирующее Мерчанта о возможных технических проблемах на его стороне. После этого сервис Uniteller несколько раз с заданной периодичностью повторяет запрос статуса заказа. Если после всех попыток сервер не ответил, Uniteller считает, что Мерчант не знает об оплате заказа. В этом случае Uniteller действует схеме, описанной в предыдущем подпункте — повторяет уведомление о статусе оплаты и дополнительно высылает письмо об оплате.

Схематично алгоритм работы функции автоматического контроля статусов заказов представлен на рис. 9.

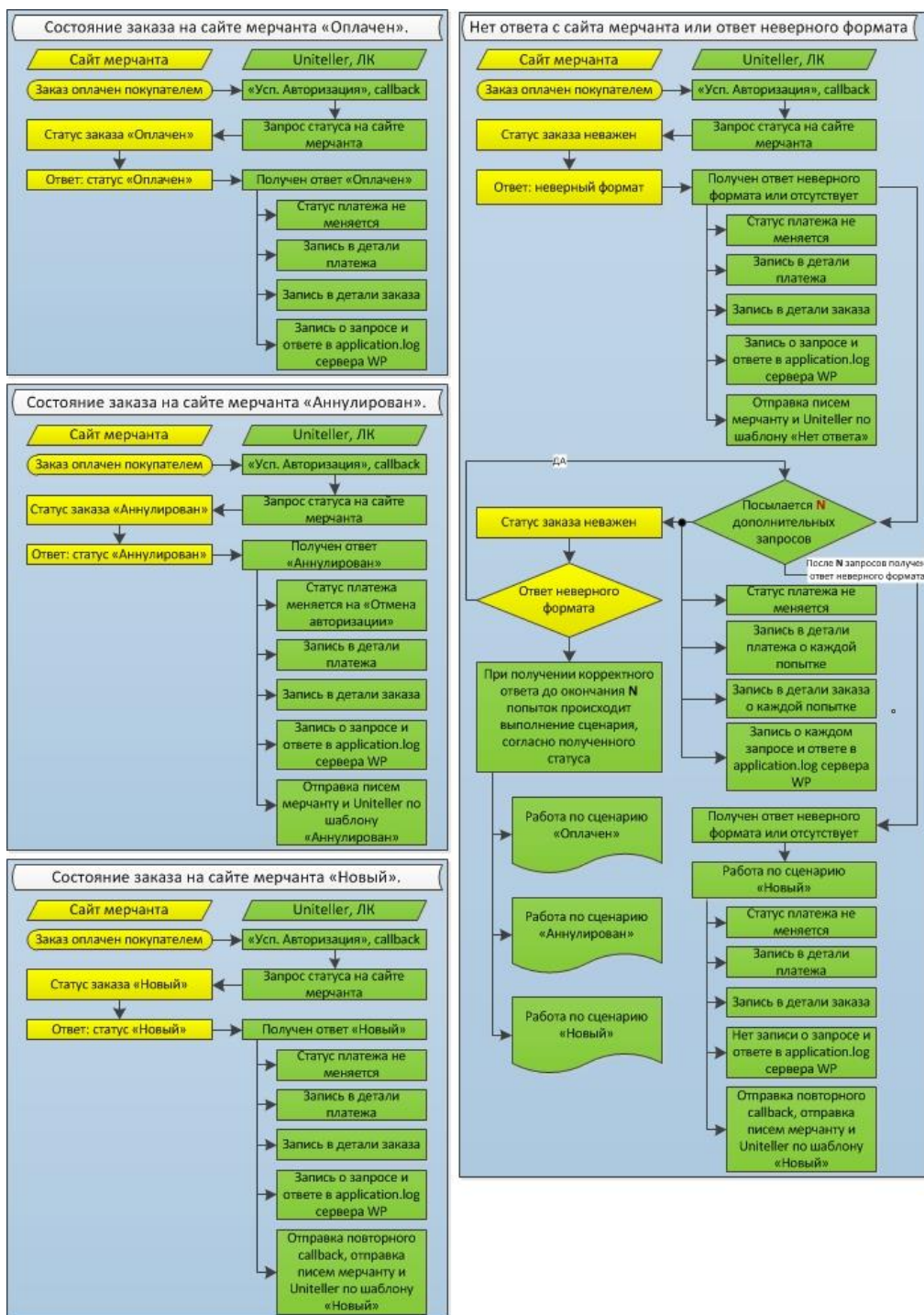


Рис. 9 — Алгоритм работы функции автоматического контроля статусов заказов

Автоматический контроль статуса заказов работает для платежей по банковским картам при услугах Интернет-эквайринг (включая платежи через ГДС) и Интернет-эквайринг в сфере самообслуживания. На момент создания этой версии документации также имелись следующие ограничения:

- Функция автоматического контроля статусов заказов не поддерживается для оплат с помощью электронных валют.
- Функция автоматического контроля статусов заказов не поддерживается для оплат через эквайера «АК БАРС».

4.7.2. Протокол запроса статуса заказа с сервера мерчанта

Для определения статуса заказа на сервер мерчанта (точный адрес указывается администратором в Личном кабинете системы в поле «**URL для запроса статуса заказа**» на странице «**Настройки контроля статуса заказа**», см. Руководство пользователя Личного кабинета Uniteller) отправляется HTTP POST запрос, содержащий следующие параметры:

- **order_id** — номер заказа;
- **upoint_id** — идентификатор точки продажи (Shop_IDP, Uniteller Point ID), от которой поступил заказ на оплату.

В качестве ответа от сервера мерчанта ожидается строка, содержащая один из следующих возможных статусов заказа в системе мерчанта:

PAID — мерчант знает о том, что заказ оплачен;

NEW — мерчант не знает об этом заказе или считает, что заказ все еще не оплачен;

CANCELLED — заказ был отменен на сайте мерчанта.

HTTP ответ от сервера мерчанта должен иметь код ответа 200. Любой другой код приводит к тому, что ответ от сервера мерчанта считается некорректным.

5. Порядок работы в Личном кабинете

5.1. Просмотр списка операций

Сотрудники Мёрчанта имеют возможность отслеживать операции с банковскими картами, а также получать сводную финансовую отчётность, используя функциональные возможности Личного кабинета системы Uniteller.

Личный кабинет платёжной системы Uniteller — это специализированный сайт с набором страниц и интерактивных форм, посредством которых авторизовавшийся в Личном кабинете пользователь получает общую или запрашиваемую информацию, а также пользуется другими функциональными возможностями системы в соответствии с имеющимися у него правами.

Реквизиты для работы с Личным кабинетом сервера Uniteller передаются Мёрчанту в момент подключения первой точки продажи.

Авторизованный доступ в Личный кабинет осуществляется с помощью логина и пароля. Доступ к любым данным об операциях по карте доступен только после авторизации.

Информация об операциях доступна в пункте меню «**Операции по карте**». При выборе этого пункта меню в области данных окна Личного кабинета отображается страница отчёта «**Операции по карте**» интерфейс которой содержит область с полями критериев запроса (фильтрами) и таблицу с результатами выполненного запроса, содержащую информацию об операциях, отвечающих установленным критериям.

Подробно работа в Личном кабинете описана в документе «Личный кабинет платёжной системы Uniteller. Руководство сотрудника мерчанта».

5.2. Возврат средств из Личного кабинета

Для операций с успешными неотменёнными платежами доступна возможность возврата средств на банковскую карту.

Для инициализации процедуры возврата средств по конкретной операции необходимо на странице «**Операции по карте**» Личного кабинета нажать кнопку **[Возврат средств]** в строке таблицы

с результатами запроса, соответствующей требуемой операции. Операция изменит статус, запись о ней в таблице с результатами запроса изменит цвет, а в столбце «**Пояснение по операции**» появится новое текстовое описание.

Подробно выполнение возврата средств по операции описано в документе «Вычислительный комплекс платёжной системы Uniteller. Руководство сотрудника мерчанта».

Время выполнения операции «Возврат средств» заранее не определено и может занимать несколько дней. В случае неудачи автоматического прохождения операции «**Возврат средств**» уполномоченный сотрудник Мёрчанта должен обратиться к техническому специалисту компании Uniteller для проведения этой операции в «ручном» режиме.

6. Техническая поддержка пользователей

Общую информацию о компании Uniteller вы можете найти на официальном сайте по адресу: <http://uniteller.ru/>, или позвонив по телефону +7 (495) 987-19-60.

Техническая поддержка пользователей осуществляется Службой технической поддержки компании Uniteller круглосуточно по телефонам +7 (495) 987-19-60, 8-800-100-19-60 или электронной почте support@uniteller.ru.

Обо всех ошибках и неточностях, обнаруженных в настоящем документе, а также ваши предложения по совершенствованию технического порядка просим сообщать в Службу технической поддержки компании Uniteller.

7. Справочная информация

7.1. Возможные поля параметра S_FIELDS

Параметр **S_FIELDS** определяет набор информационных полей, возвращаемых в ответе на запрос. В значении параметра **S_FIELDS** через «;» перечисляются названия поддерживаемых полей, возвращаемых в ответе на запрос. Последовательность полей в **S_FIELDS** определяет последовательность полей в результате. Если параметр **S_FIELDS** не передается или передается пустое значение, то будет возвращён полный список полей, перечисленный в таблице ниже. Если название поля в параметре **S_FIELDS** задано с ошибкой, в ответе на запрос будет возвращено сообщение об ошибке с соответствующим поясняющим текстом.

№	Поле	Описание
1	Address	Адрес Держателя карты
2	ApprovalCode	Код подтверждения транзакции от процессингового центра
3	BankName	Имя банка-эмитента
4	BillNumber	Номер платежа в системе Uniteller
5	Card_IDP	Идентификатор зарегистрированной карты
6	CardNumber	Первые 6 цифр и последние 4 цифры номера карты (PAN), соединённые звёздочками
7	CardType	Тип платёжной системы карты (возможные значения: visa, mastercard, dinnersclub, jcb)
8	Comment	Комментарий к оплате (передается в запросе на оплату)
9	Currency	Код валюты
10	CVC2	Наличие CVC2/CVV2/4DBC (0 — авторизация без CVC2, 1 — авторизация с CVC2)
11	Date	Дата и время оплаты в формате dd.mm.yyyy hh:mm:ss
12	Email	Адрес электронной почты Держателя карты
13	EMoneyType	Тип электронной валюты. Возможные значения представлены в табл. 3 на стр. 18.
14	EOrderData	Данные заказа, выставленного в электронной платёжной системе. В формате «title1=value1, title2=value2, ...».
15	Error_Code	Код ответа процессингового центра
16	Error_Comment	Расшифровка кода ответа процессингового центра
17	FirstName	Имя Держателя карты
18	gds_payment_purpose_id	Назначение платежа через ГДС «10» — оплата комиссионного вознаграждения Агентства; «20» — оплата билетов; для платежей без участия ГДС этот параметр пустой. В ответе в формате SOAP на запрос результата авторизации в текущей версии сервиса этот параметр не возвращается.
19	IPAddress	IP-адрес Покупателя

№	Поле	Описание
20	LastName	Фамилия Держателя карты
21	Message	Сообщение об ошибке (текст ошибки, если она произошла)
22	MiddleName	Отчество Держателя карты
23	need_confirm	Признак необходимости подтверждения преавторизации (см. п. «Преавторизация платежа» на стр. 28). «0» — платёж без преавторизации или уже подтверждён; «1» — необходимо подтверждение. В ответе в формате SOAP на запрос результата авторизации в текущей версии сервиса этот параметр не возвращается.
24	OrderNumber	Номер заказа в интернет-магазине Мёрчанта
25	PacketDate	Дата и время запроса в формате dd.mm.yyyy hh:mm:ss
26	parent_order_number	Идентификатор «родительского» платежа (значение параметра OrderNumber) для рекуррентного платежа (см. п. «Рекуррентные платежи» на стр. 31). Пустое значение, если платёж нерекуррентный. В ответе в формате SOAP на запрос результата авторизации в текущей версии сервиса этот параметр не возвращается.
27	PaymentType	«1» — оплата кредитной картой; «3» — оплата с помощью электронной валюты. В ответе в формате SOAP на запрос результата авторизации в текущей версии сервиса этот параметр не возвращается.
28	PT_Code	Тип платежа
29	Recommendation	Расшифровка кода возврата
30	Response_Code	Код возврата (см. ниже)
31	Status	Состояние заказа
32	Total	Сумма всех средств, уплаченных по одному заказу. Десятичный разделитель — точка

7.2. Значения поля response_code

№	Значение	Расшифровка
1	AS000	АВТОРИЗАЦИЯ УСПЕШНО ЗАВЕРШЕНА
2	AS100	ОТКАЗ В АВТОРИЗАЦИИ
3	AS101	ОТКАЗ В АВТОРИЗАЦИИ. Ошибочный номер карты
4	AS102	ОТКАЗ В АВТОРИЗАЦИИ. Недостаточно средств
5	AS104	ОТКАЗ В АВТОРИЗАЦИИ. Неверный срок действия карты
6	AS105	ОТКАЗ В АВТОРИЗАЦИИ. Превышен лимит
7	AS107	ОТКАЗ В АВТОРИЗАЦИИ. Ошибка приёма данных

№	Значение	Расшифровка
8	AS108	ОТКАЗ В АВТОРИЗАЦИИ. Подозрение на мошенничество
9	AS109	ОТКАЗ В АВТОРИЗАЦИИ. Превышен лимит операций Uniteller
10	AS200	ПОВТОРИТЕ АВТОРИЗАЦИЮ
11	AS998	ОШИБКА СИСТЕМЫ. Свяжитесь с Uniteller

7.3. Форматы ответов

7.3.1. Запрос состояния транзакции

7.3.1.1. Формат сообщения об ошибке

В случае возникновения ошибки для всех типов кроме SOAP ответ придёт в виде:

```
ERROR: <текст ошибки>
```

7.3.1.2. CSV

Если в запросе указан **Header=1**, то в ответ включается:

```
ZipFlag;ShopOrderNumber;Shop_ID;Format;Delimiter;OpenDelimiter;CloseDelimiter;RowDelimit
er;MeanType;StartDate;EndDate;Success;PaymentType;
значение ZipFlag;значение ShopOrderNumber;значение Shop_ID;значение Format;значение
Delimiter;значение OpenDelimiter;значение CloseDelimiter;значение RowDelimiter;значение
MeanType;значение StartDate;значение EndDate;значение Success;значение PaymentType;
```

Если в запросе указан **Header1=1**, то в ответ включается:

```
Название поля1;.....Название поляМ;
```

Далее следуют строки с данными по конкретным авторизационным запросам:

```
Значение поля1;.....Значение поляМ;
```

7.3.1.3. "В скобках"

Если в запросе указан **Header=1**, то в ответ включается:

```
[ZipFlag][ShopOrderNumber][Shop_ID][Format][Delimiter][OpenDelimiter][CloseDelimiter][R
owDelimiter][MeanType][StartDate][EndDate][Success][PaymentType]
[значение ZipFlag][значение ShopOrderNumber][значение Shop_ID][значение
Format][значение Delimiter][значение OpenDelimiter][значение CloseDelimiter][значение
RowDelimiter][значение MeanType][значение StartDate][значение EndDate][значение
Success][значение PaymentType]
```

Если в запросе указан **Header1=1**, то в ответ включается:

```
[Название поля1].....[Название поляМ]
```

Далее следуют строки с данными по конкретным авторизационным запросам:

[Значение поля1].....[Значение поляМ]

7.3.1.4. WDDX

```
<wddxPacket version='1.0'>
<header></header>
<data>
  <struct>
    <var name='FIELD'>
      <array length='1'>
        <array length='Кол-во полей вывода'>
          <string>Название поля1</string>
          <string>.....</string>
          <string>Название поляМ</string>
        </array>
      </array>
    </var>
    <var name='COUNT'><number>Кол-во объектов</number></var>
    <var name='FIRSTCODE'><string>Первый код</string></var>
    <var name='SECONDCODE'><string>Второй код</string></var>
    <var name='ORDERS'>
      <array length='Кол-во объектов'>
        <array length='Кол-во полей вывода'>
          <string>Значение поля1</string>
          <string>.....</string>
          <string>Значение поляМ</string>
        </array>
      </array>
    </var>
    <var name='REQUEST'>
      <array length='13'>
        <array length='2'>
          <string>ZipFlag</string>
          <string>Значение ZIPFLAG</string>
        </array>
        <array length='2'>
          <string>ShopOrderNumber</string>
          <string>Значение SHOPORDERNUMBER</string>
        </array>
        <array length='2'>
          <string>Shop_ID</string>
          <string>Значение SHOP_ID</string>
        </array>
        <array length='2'>
          <string>Format</string>
          <string>Значение FORMAT</string>
        </array>
        <array length='2'>
          <string>Delimiter</string>
          <number>Значение DELIMITER</number>
        </array>
        <array length='2'>
          <string>OpenDelimiter</string>
          <number>Значение OPENDELIMITER</number>
        </array>
        <array length='2'>
```

```

        <string>CloseDelimiter</string>
        <number>Значение CLOSEDELIMITER</number>
    </array>
    <array length='2'>
        <string>RowDelimiter</string>
        <string>Значение ROWDELIMITER</string>
    </array>
    <array length='2'>
        <string>MeanType</string>
        <string>Значение MEANTYPE</string>
    </array>
    <array length='2'>
        <string>PaymentType</string>
        <string>Значение PAYMENTTYPE</string>
    </array>
    <array length='2'>
        <string>StartDate</string>
        <string>Значение STARTMONTH/STARTDAY/STARTYEAR</string>
    </array>
    <array length='2'>
        <string>EndDate</string>
        <string>Значение ENDMONTH/ENDDAY/ENDYEAR</string>
    </array>
    <array length='2'>
        <string>Success</string>
        <string>Значение SUCCESS</string>
    </array>
</array>
</var>
</struct>
</data>
</wddxPacket>

```

7.3.1.5. XML

```

<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<unitellerresult firstcode='Первый код' secondcode='Второй код' count='Кол-во
объектов'>
  <request>
    <zipflag>Значение ZIPFLAG</zipflag>
    <shopordernumber>Значение SHOPORDERNUMBER</shopordernumber>
    <shop_id>Значение SHOP_ID</shop_id>
    <format>Значение FORMAT</format>
    <delimiter>Значение DELIMITER</delimiter>
    <opendelimiter>Значение OPENDELIMITER</opendelimiter>
    <closedelimiter>Значение CLOSEDELIMITER</closedelimiter>
    <rowdelimiter>Значение ROWDELIMITER</rowdelimiter>
    <meantype>Значение MEANTYPE</meantype>
    <paymenttype>Значение PAYMENTTYPE</paymenttype>
    <startdate>Значение STARTMONTH/STARTDAY/STARTYEAR</startdate>
    <enddate>Значение ENDMONTH/ENDDAY/ENDYEAR</enddate>
    <success>Значение SUCCESS</success>
  </request>
  <orders>
    <field>
      <ordernumber>Название поля</ordernumber>
      <response_code>Название поля</response_code>
      <recommendation>Название поля</recommendation>
      <message>Название поля</message>
      <comment>Название поля</comment>
      <date>Название поля</date>
    </field>
  </orders>
</unitellerresult>

```



```
<total>Название поля</total>
<currency>Название поля</currency>
<cardtype>Название поля</cardtype>
<cardnumber>Название поля</cardnumber>
<lastname>Название поля</lastname>
<firstname>Название поля</firstname>
<middlename>Название поля</middlename>
<address>Название поля</address>
<email>Название поля</email>
<approvalcode>Название поля</approvalcode>
<cvc2>Название поля</cvc2>
<cardholder>Название поля</cardholder>
<ipaddress>Название поля</ipaddress>
<billnumber>Название поля</billnumber>
<bankname>Название поля</bankname>
<status>Название поля</status>
<error_code>Название поля</error_code>
<error_comment>Название поля</error_comment>
<packetdate>Название поля</packetdate>
<paymenttype>Название поля</paymenttype>
<parent_order_number>Значение поля</parent_order_number>
<need_confirm>Название поля</need_confirm>
<pt_code>Название поля</pt_code>
<card_idp>Название поля</card_idp>
<eorderdata>Название поля</eorderdata>
</field>
<order>
<ordernumber>Номер заказа</ordernumber>
<response_code>Код возврата</response_code>
<recommendation>Рекомендации</recommendation>
<message>Сообщение</message>
<comment>Комментарий</comment>
<date>Дата</date>
<total>Сумма</total>
<currency>Код валюты</currency>
<cardtype>Тип карты</cardtype>
<cardnumber>Номер карты</cardnumber>
<lastname>Фамилия</lastname>
<firstname>Имя</firstname>
<middlename>Отчество</middlename>
<address>Адрес</address>
<email>Адрес электронной почты</email>
<approvalcode>Код авторизации</approvalcode>
<cvc2>Флаг использования</cvc2>
<cardholder>Держатель карты</cardholder>
<ipaddress>IP-адрес покупателя</ipaddress>
<billnumber>Номер платежа</billnumber>
<bankname>Название банка-эмитента</bankname>
<status>Состояние заказа</status>
<error_code>Код ответа процессингового центра</error_code>
<error_comment>Расшифровка кода ответа процессингового центра</error_comment>
<packetdate>Дата получения пакета</packetdate>
<paymenttype>Тип платежа</paymenttype>
<parent_order_number>«Родительский» платеж</parent_order_number>
<need_confirm>Необходимость подтверждения преавторизации</need_confirm>
<pt_code>Тип платежа</pt_code>
<card_idp>Идентификатор зарегистрированной карты</card_idp>
<eorderdata>Данные заказа, оплачиваемого электронной валютой</eorderdata>
</order>
<order>.....</order>
</orders>
</unitellerresult>
```

7.3.1.6. SOAP

WSDL: <https://wpay.uniteller.ru/results/wsd/>

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<ASS-NS:GetPaymentsResultResponse xmlns:ASS-NS="http://www.uniteller.ru/message/">
<return xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="SOAP-ENC:Array" xmlns:si="http://www.uniteller.ru/type/"
SOAP-ENC:arrayType="si:SOAPStruct[Кол-во объектов]">
<payment xmlns:si=" http://www.uniteller.ru/type/" xsi:type="si:SOAPStruct">
<ordernumber xsi:type="xsd:string">Номер заказа</ordernumber>
<response_code xsi:type="xsd:string">Код возврата</response_code>
<recommendation xsi:type="xsd:string">Рекомендации</recommendation>
<message xsi:type="xsd:string">Сообщение</message>
<comment xsi:type="xsd:string">Комментарий</comment>
<date xsi:type="xsd:string">Дата</date>
<total xsi:type="xsd:string">Сумма</total>
<currency xsi:type="xsd:string">Код валюты</currency>
<cardtype xsi:type="xsd:string">Тип карты</cardtype>
<cardnumber xsi:type="xsd:string">Номер карты</cardnumber>
<lastname xsi:type="xsd:string">Фамилия</lastname>
<firstname xsi:type="xsd:string">Имя</firstname>
<middlename xsi:type="xsd:string">Отчество</middlename>
<address xsi:type="xsd:string">Адрес</address>
<email xsi:type="xsd:string">Адрес электронной почты</email>
<country xsi:type="xsd:string">Код страны банка-эмитента</country>
<rate xsi:type="xsd:string">Курс валюты</rate>
<approvalcode xsi:type="xsd:string">Код авторизации</approvalcode>
<cardsubtype xsi:type="xsd:string">Подтип карты</cardsubtype>
<cvc2 xsi:type="xsd:string">Флаг использования</cvc2>
<cardholder xsi:type="xsd:string">Держатель карты</cardholder>
<ipaddress xsi:type="xsd:string">IP-адрес покупателя</ipaddress>
<protocoltypename xsi:type="xsd:string">Тип протокола</protocoltypename>
<billnumber xsi:type="xsd:string">Номер платежа</billnumber>
<bankname xsi:type="xsd:string">Название банка-эмитента</bankname>
<status xsi:type="xsd:string">Состояние заказа</status>
<error_code xsi:type="xsd:string">Код ответа процессингового центра</error_code>
<error_comment xsi:type="xsd:string">Расшифровка кода ответа процессингового
центра</error_comment>
<packetdate xsi:type="xsd:string">Дата получения пакета</packetdate>
<signature xsi:type="xsd:string">Электронная цифровая подпись</signature>
<processingname xsi:type="xsd:string">Процессинг</processingname>
<paymenttransactiontype_id xsi:type="xsd:string">Тип
транзакции</paymenttransactiontype_id>
<phone xsi:type="xsd:string">Телефон</phone>
</payment>
<payment>.....</payment>
</return>
</ASS-NS:GetPaymentsResultResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

В случае возникновения ошибки:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
```

```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Fault>
<faultcode>Первый код</faultcode>
<faultstring>Второй код</faultstring>
<detail />
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

7.3.2. Запрос отмены платежа

7.3.2.1. CSV

7.3.2.1.1. Успешный результат

OrderNumber;Response_Code;Recommendation;Message;Comment;Date;Total;Currency;CardType;CardNumber;LastName;FirstName;MiddleName;Address;Email;ApprovalCode;CVC2;CardHolder;IPAddress;BillNumber;BankName;Status;Error_Code;Error_Comment;PacketDate;PaymentType;Phone; значение OrderNumber;значение Response_Code;значение Recommendation;значение Message;значение Comment;значение Date;значение Total;значение Currency;значение CardType;значение CardNumber;значение LastName;значение FirstName;значение MiddleName;значение Address;значение Email;значение ApprovalCode;указан ли CVC2;значение CardHolder;значение IPAddress;значение BillNumber;значение BankName;значение Status;значение Error_Code;значение Error_Comment;значение PacketDate;значение PaymentType;значение Phone;

7.3.2.1.2. Получение ошибки

ErrorCode;ErrorMessage;
Код ошибки;Сообщение ошибки;

7.3.2.2. WDDX

7.3.2.2.1. Успешный результат

```

<?xml version="1.0" encoding="utf-8"?>
<wddxPacket version="1.0">
  <header/>
  <data>
    <struct>
      <var name="ordernumber"><string>значение ordernumber</string></var>
      <var name="response_code"><string>значение response_code</string></var>
      <var name="recommendation"><string>значение recommendation</string></var>
      <var name="message"><string>значение message</string></var>
      <var name="comment"><string>значение comment</string></var>
      <var name="date"><string>значение date</string></var>
      <var name="total"><string>значение total</string></var>
      <var name="currency"><string>значение currency</string></var>
      <var name="cardtype"><string>значение cardtype</string></var>
      <var name="cardnumber"><string>значение cardnumber</string></var>
      <var name="lastname"><string>значение lastname</string></var>
      <var name="firstname"><string>значение firstname</string></var>
      <var name="middlename"><string>значение middlename</string></var>
      <var name="address"><string>значение address</string></var>
      <var name="email"><string>значение email</string></var>
      <var name="approvalcode"><string>значение approvalcode</string></var>
      <var name="cvc2"><string>значение cvc2</string></var>
      <var name="cardholder"><string>значение cardholder</string></var>
      <var name="ipaddress"><string>значение ipaddress</string></var>
      <var name="billnumber"><string>значение billnumber</string></var>
    </struct>
  </data>
</wddxPacket>

```

```

    <var name="bankname"><string>значение bankname</string></var>
    <var name="status"><string>значение status</string></var>
    <var name="error_code"><string>значение error_code</string></var>
    <var name="error_comment"><string>значение error_comment</string></var>
    <var name="packetdate"><string>значение packetdate</string></var>
    <var name="paymenttype"><string>значение paymenttype</string></var>
    <var name="phone"><string>значение phone</string></var>
  </struct>
</data>
</wddxPacket>

```

7.3.2.2.2. Получение ошибки

```

<?xml version="1.0" encoding="utf-8"?>
<wddxPacket version="1.0">
  <header/>
  <data>
    <struct>
      <var name="error_code"><string>Код ошибки</string></var>
      <var name="error_message"><string>Сообщение ошибки</string></var>
    </struct>
  </data>
</wddxPacket>

```

7.3.2.3. XML

7.3.2.3.1. Успешный результат

```

<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!DOCTYPE unitellerresult [
  <!ATTLIST unitellerresult
    firstcode CDATA #REQUIRED
    secondcode CDATA #REQUIRED
    count CDATA #REQUIRED
  >
  <!ELEMENT result (orders?)>
  <!ELEMENT orders (order)>
  <!ELEMENT order (ordernumber?, response_code?, recommendation?, message?, comment?,
    date?, total?, currency?, cardtype?, cardnumber?,
    lastname?, firstname?, middlename?, address?, email?,
    approvalcode?, cvc2?, cardholder?, ipaddress?, billnumber?,
    bankname?, status?, error_code?, error_comment?, packetdate?,
    paymenttype?, phone?)>
  <!ELEMENT ordernumber (#PCDATA)>
  <!ELEMENT response_code (#PCDATA)>
  <!ELEMENT recommendation (#PCDATA)>
  <!ELEMENT message (#PCDATA)>
  <!ELEMENT comment (#PCDATA)>
  <!ELEMENT date (#PCDATA)>
  <!ELEMENT total (#PCDATA)>
  <!ELEMENT currency (#PCDATA)>
  <!ELEMENT cardtype (#PCDATA)>
  <!ELEMENT cardnumber (#PCDATA)>
  <!ELEMENT lastname (#PCDATA)>
  <!ELEMENT firstname (#PCDATA)>
  <!ELEMENT middlename (#PCDATA)>
  <!ELEMENT address (#PCDATA)>
  <!ELEMENT email (#PCDATA)>
  <!ELEMENT approvalcode (#PCDATA)>
  <!ELEMENT cvc2 (#PCDATA)>
  <!ELEMENT cardholder (#PCDATA)>
  <!ELEMENT ipaddress (#PCDATA)>
  <!ELEMENT billnumber (#PCDATA)>

```

```

<!ELEMENT bankname (#PCDATA)>
<!ELEMENT status (#PCDATA)>
<!ELEMENT error_code (#PCDATA)>
<!ELEMENT error_comment (#PCDATA)>
<!ELEMENT packetdate (#PCDATA)>
<!ELEMENT paymenttype (#PCDATA)>
<!ELEMENT phone (#PCDATA)>
<unitellerresult firstcode="" secondcode="" count="1">
  <orders>
    <order>
      <ordernumber>Значение ordernumber</ordernumber>
      <response_code>Значение response_code</response_code>
      <recommendation>Значение recommendation</recommendation>
      <message>Значение message</message>
      <comment>Значение comment</comment>
      <date>Значение date</date>
      <total>Значение total</total>
      <currency>Значение currency</currency>
      <cardtype>Значение cardtype</cardtype>
      <cardnumber>Значение cardnumber</cardnumber>
      <lastname>Значение lastname</lastname>
      <firstname>Значение firstname</firstname>
      <middlename>Значение middlename</middlename>
      <address>Значение address</address>
      <email>Значение email</email>
      <approvalcode>Значение approvalcode</approvalcode>
      <cvc2>Значение cvc2</cvc2>
      <cardholder>Значение cardholder</cardholder>
      <ipaddress>Значение ipaddress</ipaddress>
      <billnumber>Значение billnumber</billnumber>
      <bankname>Значение bankname</bankname>
      <status>Значение status</status>
      <error_code>Значение error_code</error_code>
      <error_comment>Значение error_comment</error_comment>
      <packetdate>Значение packetdate</packetdate>
      <paymenttype>Значение paymenttype</paymenttype>
      <phone>Значение phone</phone>
    </order>
  </orders>
</unitellerresult>

```

7.3.2.4. SOAP

WSDL: <https://wpay.uniteller.ru/unblock/wSDL/>

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<ASS-NS:MakeReversalResponse xmlns:ASS-NS="http://www.uniteller.ru/message/">
<return xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="SOAP-ENC:Array" xmlns:si="http://www.uniteller.ru/type/"
SOAP-ENC:arrayType="si:SOAPStruct[Кол-во объектов]">
<payment xmlns:si="http://www.uniteller.ru/type/" xsi:type="si:SOAPStruct">
<ordernumber xsi:type="xsd:string">Номер заказа</ordernumber>
<response_code xsi:type="xsd:string">Код возврата</response_code>
<recommendation xsi:type="xsd:string">Рекомендации</recommendation>
<message xsi:type="xsd:string">Сообщение</message>
<comment xsi:type="xsd:string">Комментарий</comment>
<date xsi:type="xsd:string">Дата</date>

```

```

<total xsi:type="xsd:string">Сумма</total>
<currency xsi:type="xsd:string">Код валюты</currency>
<cardtype xsi:type="xsd:string">Тип карты</cardtype>
<cardnumber xsi:type="xsd:string">Номер карты</cardnumber>
<lastname xsi:type="xsd:string">Фамилия</lastname>
<firstname xsi:type="xsd:string">Имя</firstname>
<middlename xsi:type="xsd:string">Отчество</middlename>
<address xsi:type="xsd:string">Адрес</address>
<email xsi:type="xsd:string">Адрес электронной почты</email>
<country xsi:type="xsd:string">Код страны банка-эмитента</country>
<rate xsi:type="xsd:string">Курс валюты</rate>
<approvalcode xsi:type="xsd:string">Код авторизации</approvalcode>
<cardsubtype xsi:type="xsd:string">Подтип карты</cardsubtype>
<cvc2 xsi:type="xsd:string">Флаг использования</cvc2>
<cardholder xsi:type="xsd:string">Держатель карты</cardholder>
<ipaddress xsi:type="xsd:string">IP-адрес покупателя</ipaddress>
<protocoltypename xsi:type="xsd:string">Тип протокола</protocoltypename>
<billnumber xsi:type="xsd:string">Номер платежа</billnumber>
<bankname xsi:type="xsd:string">Название банка-эмитента</bankname>
<status xsi:type="xsd:string">Состояние заказа</status>
<error_code xsi:type="xsd:string">Код ответа процессингового центра</error_code>
<error_comment xsi:type="xsd:string">Расшифровка кода ответа процессингового
центра</error_comment>
<packetdate xsi:type="xsd:string">Дата получения пакета</packetdate>
<signature xsi:type="xsd:string">Электронная цифровая подпись</signature>
<processingname xsi:type="xsd:string">Процессинг</processingname>
<paymenttransactiontype_id xsi:type="xsd:string">Тип
транзакции</paymenttransactiontype_id>
<phone xsi:type="xsd:string">Телефон</phone>
</payment>
<payment>.....</payment>
</return>
</ASS-NS:MakeReversalResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

В случае возникновения ошибки:

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Fault>
<faultcode>Первый код</faultcode>
<faultstring>Второй код</faultstring>
<detail />
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Получение ошибки:

```

<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!DOCTYPE unitellerresult [
  <!ATTLIST unitellerresult
    firstcode CDATA #REQUIRED
    secondcode CDATA #REQUIRED
    count CDATA #REQUIRED
  >
  <!ELEMENT result (orders?)>
  <!ELEMENT orders (order)>

```

```

<!ELEMENT order (ordernumber?, response_code?, recommendation?, message?, comment?,
                date?, total?, currency?, cardtype?, cardnumber?,
                lastname?, firstname?, middlename?, address?, email?,
                approvalcode?, cvc2?, cardholder?, ipaddress?, billnumber?,
                bankname?, status?, error_code?, error_comment?, packetdate?,
                paymenttype?, phone?)>
<!ELEMENT ordernumber (#PCDATA)>
<!ELEMENT response_code (#PCDATA)>
<!ELEMENT recommendation (#PCDATA)>
<!ELEMENT message (#PCDATA)>
<!ELEMENT comment (#PCDATA)>
<!ELEMENT date (#PCDATA)>
<!ELEMENT total (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT cardtype (#PCDATA)>
<!ELEMENT cardnumber (#PCDATA)>
<!ELEMENT lastname (#PCDATA)>
<!ELEMENT firstname (#PCDATA)>
<!ELEMENT middlename (#PCDATA)>
<!ELEMENT address (#PCDATA)>
<!ELEMENT email (#PCDATA)>
<!ELEMENT approvalcode (#PCDATA)>
<!ELEMENT cvc2 (#PCDATA)>
<!ELEMENT cardholder (#PCDATA)>
<!ELEMENT ipaddress (#PCDATA)>
<!ELEMENT billnumber (#PCDATA)>
<!ELEMENT bankname (#PCDATA)>
<!ELEMENT status (#PCDATA)>
<!ELEMENT error_code (#PCDATA)>
<!ELEMENT error_comment (#PCDATA)>
<!ELEMENT packetdate (#PCDATA)>
<!ELEMENT paymenttype (#PCDATA)>
<!ELEMENT phone (#PCDATA)>
]>
<unitellerresult firstcode="Код ошибки" secondcode="Сообщение ошибки" count="0">
  <orders></orders>
</unitellerresult>

```

7.3.3. Запрос рекуррентного платежа

7.3.3.1. CSV

7.3.3.1.1. Получение результата

В полученном ответе поле **Response_Code** содержит код возврата (см. п. 7.2 «Значения поля response_code» на стр. 61).

```

OrderNumber;Response_Code;Recommendation;Message;Comment;Date;Total;Currency;CardType;CardNumber;LastName;FirstName;MiddleName;Address;Email;ApprovalCode;CVC2;CardHolder;IPAddress;BillNumber;BankName;Status;Error_Code;Error_Comment;PacketDate;PaymentType;Phone;Signature;
значение OrderNumber;значение Response_Code;значение Recommendation;значение Message;значение Comment;значение Date;значение Total;значение Currency;значение CardType;значение CardNumber;значение LastName;значение FirstName;значение MiddleName;значение Address;значение Email;значение ApprovalCode;указан ли CVC2;значение CardHolder;значение IPAddress;значение BillNumber;значение BankName;значение Status;значение Error_Code;значение Error_Comment;значение PacketDate;значение PaymentType;значение Phone;значение Signature;

```

Значение **Signature** = uppercase(md5(значение **OrderNumber** + значение **Total** + **Password**))

7.3.3.1.2. Получение ошибки

```
ErrorCode;ErrorMessage;  
Код ошибки;Сообщение ошибки;
```

7.4. Примеры кода на PHP

7.4.1. Получение отчёта о выполненной транзакции через SOAP

Используется модуль **PHP SOAP**.

Получить подтверждение того, что транзакция с **Order_ID** прошла успешно:

```
ini_set('soap.wsdl_cache_enabled', '0');  
ini_set('soap.wsdl_cache_ttl', '0');  
  
$client = new SoapClient("https://wpay.uniteller.ru/results/wsdl/",  
    array(  
        'trace'      => 0,  
        'exceptions' => 1,  
    )  
);  
  
// Настройки заказа  
$Order_ID = "Эту строку заменить на Order_ID";  
// Настройки магазина  
$Shop_ID = "Эту строку заменить на Shop_ID";  
$login = "Эту строку заменить на AuthorizationLogin";  
$password = "Эту строку заменить на AuthorizationPassword";  
  
$result = $client->GetPaymentsResult(  
    $Shop_ID  
    , $login  
    , $password  
    , $Order_ID  
    , $success = 1  
    , $startmin = null  
    , $starthour = null  
    , $startday = null  
    , $startmonth = null  
    , $startyear = null  
    , $endmin = null  
    , $endhour = null  
    , $endday = null  
    , $endmonth = null  
    , $endyear = null  
    , $meantype = null  
    , $paymenttype = null  
    , $english = null  
);  
  
// проверяем что запись об этой транзакции есть и сумма транзакции та,  
// которая была указана на странице "корзина"  
if (count($result) == 1) {  
    // Транзакция выполнена  
}  
else {  
    // Транзакция не выполнена
```


7.4.2. Пример PHP-кода на странице оплаты мерчанта

```

<?php
function getOrderID() {
    // запрос в БД на получение нового значения платежа в переменную $orderID
    ...
    // возврат полученного нового значения
    return $orderID;
}

function getFromSession( $name ) {
    // получение значения переменной по ее имени из сессии в переменную $result
    ...
    return $result;
}

function getSignature( $Shop_IDP, $Order_IDP, $Subtotal_P, $MeanType, $EMoneyType,
    $Lifetime, $Customer_IDP, $Card_IDP, $IData, $PT_Code, $password ) {
    $Signature = strtoupper(
        md5(
            md5($Shop_IDP) . "&" .
            md5($Order_IDP) . "&" .
            md5($Subtotal_P) . "&" .
            md5($MeanType) . "&" .
            md5($EMoneyType) . "&" .
            md5($Lifetime) . "&" .
            md5($Customer_IDP) . "&" .
            md5($Card_IDP) . "&" .
            md5($IData) . "&" .
            md5($PT_Code) . "&" .
            md5($password)
        )
    );
    return $Signature;
}

// Инициализация параметров для формы платежа
// Параметры могут извлекаться из БД или из других хранилищ данных, либо содержаться
внутри кода
$Shop_IDP = "5001300"; // идентификатор точки продажи
$Lifetime = 3600; // время жизни формы оплаты в секундах
$Order_ID = getOrderID();
// Сумма для оплаты и идентификатор зарегистрированного пользователя могут храниться в
данных сессии
$Subtotal_P = getFromSession("Subtotal_P");
$Customer_IDP = getFromSession("Customer_IDP");
// Параметры из справочников, описанных в Техническом порядке
$MeanType = 0; // платежная система кредитной карты (0 - любая)
$EMoneyType = 0; // тип электронной валюты (0 - любая)
// Адреса возврата после успешной и неуспешной оплат покупателями
$URL_RETURN_OK = "http://example.com/pay/ok/";
$URL_RETURN_NO = "http://example.com/pay/fail/";

$password = "adadadadadadaddasdasdasdasdsadsd"; // пароль из ЛК Uniteller
// Подпись для формы, вместо неиспользуемых параметров передаются пустые строки
$Signature = getSignature( $Shop_IDP, $Order_ID, $Subtotal_P, $MeanType, $EMoneyType,
    $Lifetime, $Customer_IDP, "", "", "", $password );
?>
<form action="https://wpay.uniteller.ru/pay/" method="POST">
<input type="hidden" name="Shop_IDP" value="<?=$Shop_IDP?>">
<input type="hidden" name="Order_IDP" value="<?=$Order_ID?>">
<input type="hidden" name="Subtotal_P" value="<?=$Subtotal_P?>">

```

```

<input type="hidden" name="Lifetime" value="<?=$Lifetime?>">
<input type="hidden" name="Customer_IDP" value="<?=$Customer_IDP?>">
<input type="hidden" name="Signature" value="<?=$Signature?>">
<input type="submit" name="Submit" value="Оплатить">
<input type="hidden" name="URL_RETURN_OK" value="<?=$URL_RETURN_OK?>">
<input type="hidden" name="URL_RETURN_NO" value="<?=$URL_RETURN_NO?>">
<input type="hidden" name="MeanType" value="<?=$MeanType?>">
<input type="hidden" name="EMoneyType" value="<?=$EMoneyType?>">
</form>

```

7.4.3. Пример PHP-кода запроса результата авторизации на сервере Uniteller

```

<?php

function checkSignature( $Order_ID, $Status, $Signature ) {
    $password = "adadadadadadaddasdasdasdasdsadsd"; // пароль из ЛК Uniteller
    // проверка подлинности подписи и данных
    return ( $Signature == strtoupper(md5($Order_ID . $Status . $password)) );
}

function getData($Order_ID) {
    // Параметры могут извлекаться из БД или из других хранилищ данных, либо
    содержаться внутри кода
    $Shop_ID = "5001300"; // идентификатор точки продажи
    $Login = 1; // логин из ЛК Uniteller
    $Password = "adadadadadadaddasdasdasdasdsadsd"; // пароль из ЛК Uniteller

    // Format=1 - получить данные в виде строки с разделителем ";", можно получать
    данные и в других форматах (см. Технический порядок), например, XML, тогда обработка
    полученного ответа изменится
    $sPostFields =
"Shop_ID=".$Shop_ID."&Login=".$Login."&Password=".$Password."&Format=1&ShopOrderNumber="
.$Order_ID."&S_FIELDS=Status;ApprovalCode;BillNumber";
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "https://wpay.uniteller.ru/results/");
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
    curl_setopt($ch, CURLOPT_VERBOSE, 0);
    curl_setopt($ch, CURLOPT_TIMEOUT, 60);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $sPostFields);
    curl_setopt($ch, CURLOPT_BINARYTRANSFER, 1);
    curl_setopt($ch, CURLINFO_HEADER_OUT, 1);
    $curl_response = curl_exec($ch);
    $curl_error = curl_error($ch);

    $data = array(); // результат для возврата
    if ($curl_error) {
        // обработка ошибки обращения за статусом платежа
    } else {
        // данные получены
        // обработка данных из переменной $curl_response
        $arr = explode(";", $curl_response);
        if ( count($arr) > 2 ) {
            $data = array(
                "Status" => $arr[0]
                , "ApprovalCode" => $arr[1]
                , "BillNumber" => $arr[2]
            );
        } else {
            // что-то не так, обработчик полученного ответа
            ...

```

```

    }
    return $data;
}

// Пришел callback с параметрами Order_ID, Status, Signature
if ( count($_POST) && isset($_POST["Order_ID"]) && isset($_POST["Status"]) &&
isset($_POST["Signature"]) ) {
    // проверка подписи
    if ( checkSignature( $_POST["Order_ID"], $_POST["Status"], $_POST["Signature"] ) )
    {
        // подпись сошлась
        ... // какие-то действия: сохранение полученных данных в БД
        // можно сделать дополнительный запрос статуса платежа для еще одной
        проверки и/или получения дополнительных параметров платежа
        $data = getData($_POST["Order_ID"]);
        // далее можно проверить совпадение статусов, сохранить дополнительные
        данные в БД, выполнить необходимые действия
    } else {
        // не сошлась подпись
        ... // какие-то действия по обработке этого случая
    }
}
?>

```

7.4.4. Пример PHP-кода отмены платежа по RRN

```

<?php
function unblock($Shop_ID,$Login,$Password,$Billnumber) {
    // Format=1 - получить данные в виде строки с разделителем ";", можно получать
    данные и в других форматах (см. ТП), например, XML, тогда обработка полученного ответа
    изменится
    $sPostFields =
"Shop_ID=".$Shop_ID."&Login=".$Login."&Password=".$Password."&Format=1&Billnumber=".$Bill
number."&S_FIELDS=Status;ApprovalCode;BillNumber";
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "https://wpay.uniteller.ru/unblock/");
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
    curl_setopt($ch, CURLOPT_VERBOSE, 0);
    curl_setopt($ch, CURLOPT_TIMEOUT, 60);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $sPostFields);
    curl_setopt($ch, CURLOPT_BINARYTRANSFER, 1);
    curl_setopt($ch, CURLINFO_HEADER_OUT, 1);
    $curl_response = curl_exec($ch);
    $curl_error = curl_error($ch);

    $data = array(); // результат для возврата
    if ($curl_error) {
        // обработка ошибки обращения за отменой платежа
    } else {
        // данные получены
        // обработка данных из переменной $curl_response
        $arr = explode(";", $curl_response);
        if ( count($arr) > 2 ) {
            $data = array(
                "Status" => $arr[0]
                , "ApprovalCode" => $arr[1]
            );
        }
    }
}

```

```
        , "BillNumber" => $arr[2]
    );
    } else {
        // что-то не так, обработчик полученного ответа
        ...
    }
}
return $data;
}

// Параметры могут извлекаться из БД или из других хранилищ данных, либо содержаться
внутри кода
$Shop_ID = "5001300"; // идентификатор точки продажи
>Login = 1; // логин из ЛК Uniteller
>Password = "adadadadadadaddasdasdasdasdasdsadsd"; // пароль из ЛК Uniteller
$Billnumber = "100100100100"; // номер платежа в системе Uniteller

// отмена платежа с номером из переменной $Billnumber
$data = unblock( $Shop_ID,$Login,$Password,$Billnumber );
if (!count($data)) {
    // отмена не произошла
    ... // какие-то действия
} else {
    // проверка статуса
    if ($data["Status"] == "canceled") {
        // успешная отмена
        ... // какие-то действия
    } else {
        // что-то не так
        ... // какие-то действия
    }
}
?>
```

7.5. Необходимость подписания формы оплаты

Отсутствие подписи формы оплаты на сайте интернет-магазина Мёрчанта делает возможным ряд атак со стороны злоумышленников. Например.

Мёрчант на сайте интернет-магазина показывает Покупателю страницу «Корзина», на которой сформирована форма с полями **Shop_IDP**, **Order_IDP** и **Subtotal_P** (последнее поле — сумма платежа). Атакующий меняет значение скрытого (hidden) поля **Subtotal_P** на меньшее в надежде на то, что код на стороне Мёрчанта в ходе запроса успешности транзакции не проверяет корректность оплаченной суммы. Атакующий нажимает кнопку «Оплатить», оплачивает меньшую сумму и, если ему повезло, получает товар/услугу «со скидкой», а если не повезло, то жалуется в поддержку магазина, что он заплатил, сколько сказали, а товар/услугу не получил.

Подпись формы оплаты позволяет защититься от этой распространённой атаки ещё на этапе загрузки формы оплаты.

Подписью формы оплаты является значение параметра **Signature**, алгоритм вычисления которого приведён в табл. 1 на стр. 15 (см. п. 4.1.2 «Форма оплаты на сайте интернет-магазина Мёрчанта и её параметры» на стр. 14).

В случае если подпись неверна (атакующий поменял одно или несколько полей формы оплаты на сайте интернет-магазина), то Покупателю будет показана ошибка вместо формы оплаты, и процесс оплаты даже не начнётся.