

ЕГАИС-РОЗНИЦА

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

к кассовому программному обеспечению
организаций розничной торговли,
осуществляющих реализацию алкогольной продукции

Версия изменений 15.0

ОГЛАВЛЕНИЕ

1.ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ	3
2.СОСТАВ ИНФОРМАЦИИ НА МАРКЕ	3
3.СПРАВОЧНИК	4
4.ПРОДАЖА	4
5.ДАННЫЕ ЧЕКА.....	5
6.ПРОВЕРКА НА ПОВТОР В ЧЕКЕ	6
7.ВОЗВРАТ.....	6
8.СКАНЕР	6
9.ПОДОТЧЕТ.....	7
10.КРИПТОПРОВАЙДЕР	7
11.ТРЕБОВАНИЯ К КОМПЬЮТЕРУ МАГАЗИНА.....	7
12.КВИТИРОВАНИЕ.....	8
13.БУФЕР.....	8
14.ОБНОВЛЕНИЕ.....	8
15.ПОЛУЧЕНИЯ КЛЮЧА RSA.....	9
16.ПОЛУЧЕНИЕ КЛЮЧА ГОСТ	9
ПРИЛОЖЕНИЕ А	9
ПРИЛОЖЕНИЕ Б	12
ПРИЛОЖЕНИЕ В	15
Глоссарий.....	16

Введение

Повышение ставок акцизов на алкогольную продукцию (в период с 2013 по 2015 ставки акцизов в среднем увеличатся еще на 35%) создает дополнительные риски расширения нелегального рынка алкогольной продукции. В настоящее время система ЕГАИС содержит не полную информацию о движении маркированной алкогольной продукции, поскольку ее розничная реализация не фиксируется в ЕГАИС. Такая ситуация позволяет реализовывать в розничной сети контрафактную алкогольную продукцию.

Документирование в кассовом чеке ответственности предприятия розничной торговли за качество каждой реализуемой единицы алкогольной продукции позволяет не допустить контрафактную продукцию к продаже потребителю.

Регистрация информации о розничной реализации каждой единицы алкогольной продукции в целях осуществления мероприятий по контролю легальности этой алкогольной продукции.

1. Принципы функционирования

При продаже каждой единицы алкогольной продукции, оклеенной федеральной специальной (ФСМ, отечественная продукция) или акцизной маркой (АМ, импортированная продукция), необходимо сохранять в чеке информацию, содержащуюся на федеральной специальной марке либо акцизной марке.

Информация, содержащаяся на марке, считывается при продаже сканером двумерного штрихкода и сохраняется в чеке.

Данные, сохраненные в чеке, необходимо передавать в центр обработки данных.

На основании данных об алкогольной продукции, проданной по данному чеку, на самом чеке должна быть напечатана информация в виде qr-кода с содержимым, описанным далее. Такой штриховой код предназначен для использования покупателем при проверке с использованием смартфона, подключенного к сети интернет, легальности товара, приобретенного по этому чеку.

В соответствии с ниже описанными требованиями кассовое программное обеспечение должно быть модифицировано.

Технические требования основываются на процессе продажи, осуществляющемся по кодам EAN-8, 12, 13.

2. Состав информации на марке

Состав информации на марке определяется приказом Росалкогольрегулирования № 33н от 12.05.2010. При осуществлении продажи (см. п. 6) требуется сканировать двумерный штриховой код (Рисунок 1). Штрих код имеет формат PDF-417. Так же требуется сканировать EAN-код.



Рисунок 1. Изображен номер марки (EAN), формируемый ФГУП «Гознак» при ее производстве, обведен желтой рамкой. Двумерный штрих код PDF-417 обведен красной рамочкой.

Пример набора символов, содержащихся в штрихкоде PDF-417 имеет вид:

19N00000XORP13MM66T0NHVF311210120003676539219152175585956302712947109

Символы представлены цифрами либо строчными латинскими буквами. Длина набора символов – 68 единиц.

3. Справочник

В справочнике кассовой программы установить у товара признак «Алкогольная продукция». Для товара с этим признаком установить свойство: если такой товар необходимо записать в чек, обязательно запрашивать сканирование двумерного штрих кода PDF-417 марки.

4. Продажа

Реализовать дополнительную логику в работе кассовой программы в соответствии со схемой (см. Приложение А). Под дополнительной обработкой акцизного товара при его продаже подразумевается следующий алгоритм работы кассы:

1. При сканировании штрихового кода EAN, касса находит в своей базе данных товар
2. При принадлежности товара к группе «Алкогольная продукция» на экране кассы появится окно (Рисунок 2).

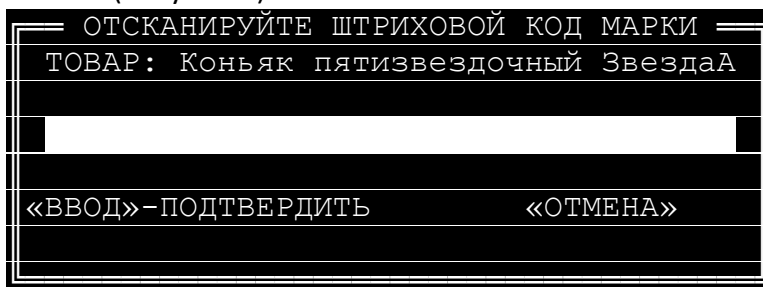


Рисунок 2. Отображение на экране запроса на сканирование двумерного штрих кода марки

3. Кассир сканирует марку
4. Если штриховой код марки отсканируется успешно, то данное окно автоматически закроется, в символы баркода заносятся в чек (в СУБД).
5. Если штриховой код не представляется возможным отсканировать (испорчен, плохое качество штрихкода и т. п.), то кассир должен нажать на кнопку «Отмена» и товар в чек добавлен не будет.
6. По окончании формирования чека в случае, если он содержит алкогольную продукцию, данные о чеке и алкогольной продукции передаются в транспортный модуль. Перечень данных о чеке описан в Приложении Б. Выбор момента отправки xml-файла с ТМ должен обеспечивать невозможность корректировки чека после (имеется в виду исключение возможности добавления алкогольной продукции, которая в соответствии со схемой, уже не будет в чеке отправлена в транспортный модуль для проверки) и возможность удаления алкогольных позиций в случае неуспешного ответа. Рекомендовано реализовать первой задачей в едином блоке транзакций записи чека в БД, ФП, ЭКЛЗ. Если от транспортного модуля получен положительный ответ - транзакция продолжается. Если не получен положительный ответ – откат транзакции и возврат в режим формирования.
7. Транспортный модуль осуществляет подписание чека ЭП и возвращает в кассовую программу ответ в виде отпечатка ЭП.
8. Дополнительно в ответе содержится уникальный идентификатор ЕГАИС.
9. Если кассовая программа успешно получила отпечаток и идентификатор от транспортного модуля, то касса выводит на печать подотчет, содержащий отпечаток ЭП в виде символов и идентификатор ЕГАИС в виде qr-кода.

10. Чек закрывается. В случае сбоя при регистрации чека (xml-файл отправлен в ТМ, получен успешный ответ, но произошел сбой при регистрации в БД, ФП, ЭКЛЗ), в ТМ необходимо отправить обратную транзакцию, аналогичную операции возврат.

5. Данные чека

Транспортный модуль предоставляется организации для осуществления подписания чеков и их гарантированной отправки на сервер обработки данных. Перечень данных чека для передачи в транспортный модуль описывается xsd-схемой (см. Приложение Б). Из транспортного модуля так же приходит квитанция в xml-файле, описанном xsd-схемой (см. Продолжение Приложения Б).

6. Проверка на повтор в чеке

При продаже в рамках одного открытого чека должна выполняться проверка на сканирование марки с теми же значениями баркода. Проверка требуется во избежание умышленного сканирования кассиром одной той же единицы продукции в случае, если реализуется товар одного и того же наименования в количестве, большим одного.

При обнаружении повторного сканирования в рамках одного чека, необходимо выдавать предупреждение (Рисунок 3).

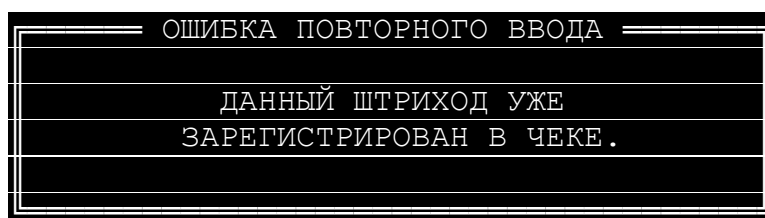


Рисунок 3. Окно, отображающееся на экране в случае повторного ввода продукции.

7. Возврат

Возврат алкогольных товаров на кассе осуществлять по тому же принципу, что и продажа. Если в возвратном чеке кассовая программа обнаружит, что возвращается алкогольный товар, на экране будет показано окно (Рисунок 2). В операции возврата требуется производить проверку на повтор согласно информации из предыдущей главы.

Стоимость возвращённого товара должна быть указана с отрицательным знаком. Данные об акцизном ШК, будут переданы на сервер вместе с чеком, по аналогии с чеками продажи.

8. Сканер

Технологические разъемы кассы должны обеспечивать возможность подключения дополнительного сканера для чтения штрих кодов PDF-417. Пример модели сканера для использования на кассе: Motorola DS-4208. Сканер должен использоваться при работе кассира в режиме, когда раскладка клавиатуры кассы переключена на английский язык. Сканер должен быть настроен на сканирование только кодов EAN-8, 12, 13 и PDF-417.

9. Подотчет

Программное обеспечение кассы обрабатывает ответ от транспортного модуля и формирует печатную форму с макетом (см. Приложение В).

Длина стороны изображения qr-кода должна составлять 30 мм. Сканирование потребителем qr-кода обеспечивает автоматизированное получение ссылки в сети интернет на информацию об алкогольной продукции, проданной по данному чеку.

10. Криптопровайдер

Для подписания чеков, установления и шифрования авторизованного соединения используется аппаратный крипто-ключ JaCarta SE PKI/ГОСТ. Данное изделие обеспечивает неизвлекаемость закрытого ключа ГОСТ. На USB-ключе расположены:

- закрытый ключ ГОСТ
- закрытый ключ RSA
- криптографические библиотеки

Закрытый ключ ГОСТ (квалифицированная электронная подпись) используется в транспортном модуле для подписания xml-файла чека. Закрытый ключ RSA используется для отправки подписанного чека по защищенному каналу связи.

Скорость пакетного подписания файла размером 256 бит составляет 1,4 сек. Средний xml-чек составляет 560 бит.

11. Требования к компьютеру магазина

Чек подписывается КЭП в соответствии с ГОСТ Р 34.10-2001. КЭП выдается на директора магазина в произвольном уполномоченном УЦ. Открытый ключ должен быть зарегистрирован на сервере приема контроля чеков. Отправка чеков должна выполняться в разрезе структурных подразделений (магазинов), указанных в розничной лицензии. Каждый магазин должен быть оснащен компьютером, работающим под одной из операционных систем согласно спецификации производителя: <http://www.aladdin-rd.ru>. На компьютере должна быть установлена Java-машина JRE 8. Кассы магазина должны находиться в одной сети с данным компьютером. На компьютере устанавливается транспортный модуль из дистрибутива, выдаваемого Росалкогольрегулированием. Для отправки данных от

компьютера до сервера ЕГАИС должен быть открыт исходящий порт TCP 443. Порт должен быть открыт на адрес <https://balancer.fsrar.ru>. Время выполнения команды ping по данному адресу не должно быть более чем 300 мс. Перед отправкой данных устанавливается ssl-соединение с использованием ключа, сформированного по алгоритму RSA, длиной 2048 бит. В рамках каждого сеанса связи осуществляются:

- проверка валидности ключа (зарегистрирован, кем выдан, срок действия и т. п.)
- отправка новых подписанных чеков
- получение квитанций по чекам, отправленным в предыдущие сеансы связи.

12. Квитирование

Сервер ЕГАИС осуществляет проверку чека:

- на валидность подписи xml-файла
- на валидность ключа подписи
- на список отзыва
- на валидность xml-файла
- на соответствие xml схеме
- на соответствие реквизитов в подписи и в xml-файле
- на соответствие реквизитов ключа ГОСТ и ключа RSA

По результату проверки сервер ЕГАИС формирует квитанцию. Транспортный модуль за сеанс связи опрашивает сервер ЕГАИС о наличии квитанций по ранее отправленным чекам. Когда чек принят успешно, он отмечается в транспортном модуле, как зафиксированный в ЕГАИС, и удаляется из буфера.

13. Буфер

Совокупность подписанных чеков транспортного модуля, еще не зафиксированных в ЕГАИС, называется буфером. Время, прошедшее с момента подписания чека, находящегося в буфере, до настоящего момента времени, называется возрастом чека. Момент подписания чека фактически совпадает с датой чека. Максимальный возраст чека, находящегося в буфере, называется возрастом буфера. Возраст буфера не должен превышать трех календарных дней. Буфер возрастом более трех календарных дней называется устаревшим. Буфер устаревает, если транспортный модуль перестает отправлять подписанные ранее чеки. Подписание чеков транспортным модулем останавливается, когда буфер устаревает. Транспортный модуль с устаревшим буфером не возвращает идентификатор чека и его контрольную сумму. Подписание новых чеков не возобновляется до тех пор, пока старые чеки не будут зафиксированы в ЕГАИС.

14. Обновление

В зависимости от изменения в законодательстве транспортный модуль будет обновляться. Получение обновления для транспортного модуля осуществляется с сервера ЕГАИС по исходящему запросу от транспортного модуля с использованием ssl-туннеля. Если обновление готово для распространения, оно закачивается на компьютер магазина. Обновление, закачанное на компьютер, устанавливается автоматизировано по сигналу от сервера ЕГАИС на исходящий запрос от транспортного терминала.

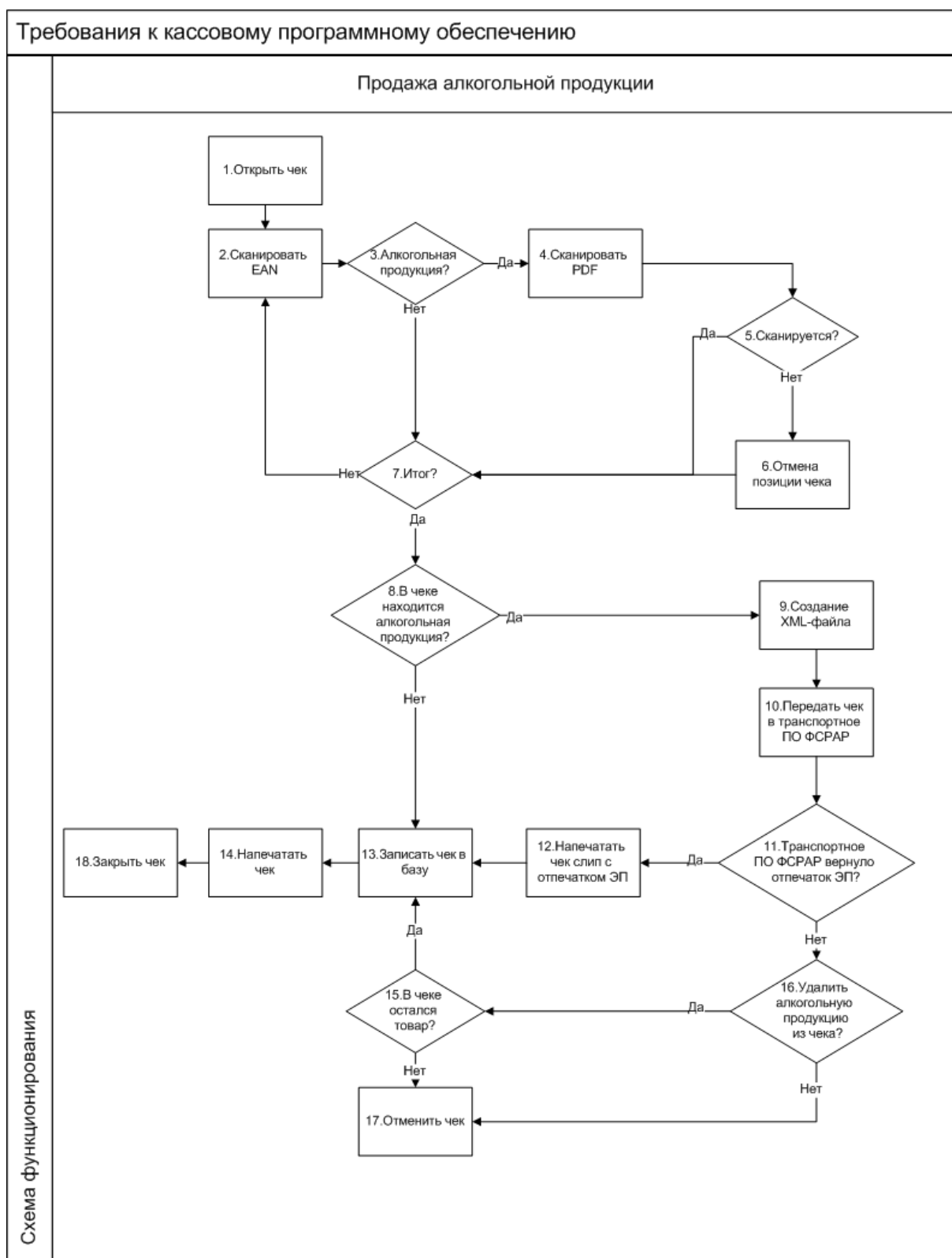
15. Получения ключа RSA

На компьютер пользователя скачивается крипто-плагин для работы с eToken ГОСТ. Организация в личном кабинете, раздел «Персональные данные» выбирает место осуществления деятельности, вставляет крипто – носитель (eToken ГОСТ) и нажимает на кнопку сформировать ключ доступа (ключ – RSA). Ключ RSA генерируется и сохраняется на носителе.

16. Получение ключа ГОСТ

Организация в личном кабинете заполняет форму запроса на ключ ГОСТ, закрытый ключ сохраняется на носителе. Файл запроса ожидает регистрации в Удостоверяющем центре. После получения сертификата открытого ключа, сертификат с помощью функционала личного кабинета сохраняется на носителе. Допускается получение КЭП ГОСТ организацией в соответствии с общими правилами УЦ.

ПРИЛОЖЕНИЕ А



Детальное описание шагов схемы:

1. Кассир открывает чек.
2. Кассир считывает при помощи сканера EAN-код продукции.

3. Если код EAN имеет свойство алкогольной продукции, на экране кассира появится окно (Рисунок 2). Если не имеет свойство алкогольной продукции, продажа осуществляется в обычном режиме.
4. С помощью сканера PDF кассир считывает двумерный ШК продукции.
5. Если двумерный ШК считывается, кассовое ПО добавляет продукцию в чек.
6. Кассир нажимает кнопку отмена, если код не считывается.
7. Если весь товар внесен в чек, кассир нажимает кнопку “Итог”.
8. Если среди товара нет алкогольной продукции, продажа товара осуществляется в обычном режиме. Иначе п. 9.
9. Кассовое ПО генерирует xml в соответствии с данными чека.
10. Касса отправляет xml-файл в транспортный модуль.
11. Транспортный модуль формирует квитанцию в соответствии с приложением Б. Иначе п. 13.
12. Касса напечатает слип к чеку.
13. Данные чека записываются в БД, ФП, ЭКЛЗ.
14. Касса печатает обычный чек и слип к нему (Приложение В).
15. Если после удаления алкогольной продукции в чеке остался прочий товар, продажа осуществляется в обычном режиме.
16. Происходит удаление алкогольной продукции, либо автоматическое, либо вручную самим кассиром.
17. Чек отменяется, если в нем не осталось товара.
18. Конец

ПРИЛОЖЕНИЕ Б

Xsd-схема описывает данные чека для передачи в транспортный модуль:

```

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" id="Cheque">
  <xs:simpleType name="IN">
    <xs:restriction base="xs:string">
      <xs:pattern value="(\d{10}|\d{12})"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="KP">
    <xs:restriction base="xs:string">
      <xs:pattern value="(\d{9}|" )"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="DT">
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-3][0-9][0-1][0-9][0-9]{2}[0-2][0-9][0-5][0-9]"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="BK">
    <xs:restriction base="xs:string">
      <xs:pattern value="\d\dN\w{20}\d[0-1]\d[0-3]\d{10}\w{31}"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="EAN">
    <xs:restriction base="xs:string">
      <xs:pattern value="(\d{8}|\d{12}|\d{13})"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="PRICE">
    <xs:restriction base="xs:string">
      <xs:pattern value="[-]?\d+\.\d{0,2}"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="VOLUME">
    <xs:restriction base="xs:string">
      <xs:pattern value="(\d+\.\d{0,4}|" )"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="ADDRESS">
    <xs:restriction base="xs:string">
      <xs:maxLength value="128"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:element name="Bottle">
    <xs:complexType>
      <xs:attribute name="price" type="PRICE" use="required"/>
      <xs:attribute name="barcode" type="BK" use="required"/>
      <xs:attribute name="ean" type="EAN" use="required"/>
      <xs:attribute name="volume" type="VOLUME"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Cheque">
    <xs:complexType>
      <xs:sequence>
        <xs:choice minOccurs="1" maxOccurs="unbounded">
          <xs:element ref="Bottle"/>
        </xs:choice>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

```

</xs:choice>
</xs:sequence>
<xs:attribute name="inn" type="IN" use="required"/>
<xs:attribute name="kpp" type="KP"/>

<xs:attribute name="address" type="ADDRESS" use="required"/>
<xs:attribute name="name" type="xs:string" use="required"/>
<xs:attribute name="kassa" type="xs:string" use="required"/>
<xs:attribute name="shift" type="xs:int" use="required"/>
<xs:attribute name="number" type="xs:int" use="required"/>
<xs:attribute name="datetime" type="DT" use="required"/>
</xs:complexType>
<xs:unique name="bottleBarcode">
<xs:selector xpath="Bottle"/>
<xs:field xpath="@barcode"/>
</xs:unique>
</xs:element>
</xs:schema>

```

Пояснения полей в чеке:

Bottle – позиция чека с алкогольной продукцией. Содержит следующие параметры:

- **Price** – цена алкогольной продукции.
Формат:
 - Отрицательное число в случае возврата алкогольной продукции
 - Разделитель – “точка”
 - Копейки указываются
- **Barcode** – символы штрих кода PDF-417. Формат определяется Росалкогольрегулированием.
- **Ean** – EAN код алкогольной продукции. Длина: 8 , 12 или 13 цифр. Осуществляется проверка контрольной суммы.
- **Volume** – емкость алкогольной продукции в литрах, необязательное значение.
Формат:
 - Разделитель – “точка”
 - Точность - 4 знака после разделителя

Inn – ИНН организации. Длина: 10 или 12 цифр. Осуществляется проверка контрольной суммы.

Kpp – КПП обособленного подразделения по розничной лицензии. Формат: ничего, если ИНН 12-тизначный; 9 знаков, если ИНН 10-тизначный.

Address – адрес обособленного подразделения по розничной лицензии. Длина: до 128 символов.

Name – наименование магазина. Длина: до 128 символов.

Kassa– заводской номер ККМ. Длина: до 128 символов.

Shift– номер смены, целое число.

Number– номер чека, целое число.

Datetime– Дата, время чека. Формат: ДДММГГЧЧММ – день, месяц, год, часы, минуты.

BottleBarcode – проверка уникальной алкогольной продукции в чеке.

Пример xml-файла, отправляемого на вход ПО транспортный терминал:

```

<?xml version="1.0" encoding="UTF-8"?>
<Cheque inn="5036032527"
kpp="525745007"
address="Нижний Новгород, К.Маркса пр-т, 7, А"
name="Пятёрочка"

```

```

kassa="3"
shift="735"
number="2187"
datetime="2003141459">
<Bottle price="352.89"
barcode="19N00000XOPN13MM66T0HVF311220130003476539219152175585956302712947109"
ean="177736216338" volume="1.0000" />
<Bottle price="123.45"
barcode="19N00000XOPN13MM66T0HVF311220130003476539219152175585956302712947109"
ean="177736216338" volume="0.7500" />
</Cheque>

```

Xsd-схема описывает данные квитанции, возвращаемой в кассу из транспортного модуля:

```

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" id="Answer">
<xs:element name="sign">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="256"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="A">
<xs:complexType>
<xs:sequence>
<xs:element name="url" type="xs:string"/>
<xs:element ref="sign"/>
<xs:element name="ver" type="xs:int"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

Пояснения полей:

Sign – отпечаток электронной подписи. Длина 128 символов.

Url – адрес страницы просмотра чека в сети интернет.

Ver – версия формата квитанции.

Пример xml-файла квитанции:

```

<?xml version="1.0" encoding="UTF-8"?>
<A>
<url>https://check.egais.ru?id=a9e56cb9-21d6-4404-9f24-
668020fadf6a&dt=0910141104&cn=Magazin2014</url>
<sign>418E6A105B60250CEB20F9F9A556FA4A9575B0C07EC536DE89CA868C884E296E56BA7EC776
2C9BEC285CB4D8CD90EEE9F9FC16F92CCF324829E70862F0DFEC1B418E6A105B60250CEB20F9F9A5
56FA4A9575B0C07EC536DE89CA868C884E296E56BA7EC7762C9BEC285CB4D8CD90EEE9F9FC16F92C
CF324829E70862F0DFEC1B</sign>
<ver>1</ver>
</A>

```

Пример команды отправки чека (check.xml) в транспортный модуль:

```
curl -F 'xml_file=@check.xml' http://localhost:8080/xml
```

ПРИЛОЖЕНИЕ В

Схема подотчета чека:

[линия отреза_____линия отреза]	
[пустая строка]	
[форма собственности/пробел/наименование организации]	
ИНН: [10 или 12 цифр]	КПП: [10 или 0 цифр]
КАССА: [12 символов]	СМЕНА: [6 цифр]
ЧЕК: [6 цифр]	ДАТА: [ДД.ММ.ГГГГ ЧЧ:ММ]
[пустая строка]	
[qr-код с содержимым	
http://check.egais.ru?id=UUID&dt=ДДММГГЧЧММ&cn=Common_Name	
длина стороны qr-кода — 30 мм]	
[пустая строка]	
[надпись	
«http://check.egais.ru?id=UUID&dt=ДДММГГЧЧММ&cn=Common_Name»]	
ОТПЕЧАТОК КЭП [128 символов]	
[пустая строка]	
[линия отреза_____линия отреза]	

Пример подотчета чека:

ООО «Магазин-2014»	
ИНН: 4959166101	КПП: 495901001
КАССА: 11022	СМЕНА: 693
ЧЕК: 3027	ДАТА: 13.12.2012 11:22
	
http://check.egais.ru?id=88a7a3ed-39ae-45de-a3cc-644639f36f4e&dt=0910141104&cn=Magazin2014	
04 40 EA 2B C7 08 75 5D F0 43 C1 04 5C 06 96 71 69 DD BF 30 D9 2D 6B 7D F0 FE 81 43 F9 C4 51 21 E3 42 C9 67 63 4F 24 D5 42 B1 8B 1D 3D F8 6F 91 21 00 6D 8B DE 56 91 CA BB ED 0D 36 11 96 B4 33	

Глоссарий

QR-код — двумерный штрих код.

Баркод – штриховой код.

ЕГАИС – (Единая государственная автоматизированная информационная система) — автоматизированная система, предназначенная для государственного контроля над объёмом производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции.

Квалифицированная электронная подпись (КЭП) подходит для работы с основными государственными информационными системами, а также для организации закупок по 223-ФЗ.

Отпечаток ЭП – результат применения закрытого ключа к данным.

Слип – подотчет к чеку.

Транзакция — группа последовательных операций с базой данных, которая представляет собой логическую единицу работы с данными.

Транспортный модуль - устройство (ПК), осуществляющее приём данных от внешних устройств (кассовая программа), подписание файлов с помощью закрытого ключа, и обеспечивающее последующую отправку отпечатка электронной подписи на кассу.

Форм-фактор — стандарт, задающий габаритные размеры технического изделия.

Электронная подпись (ЭП), электронная цифровая подпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи владельцу сертификата ключа подписи.