



Об утверждении Правил выдачи заключений о соответствии компьютерной системы техническим требованиям для включения в государственный реестр контрольно-кассовых машин

Утративший силу

Постановление Правительства Республики Казахстан от 1 ноября 2011 года № 1265. Утратило силу постановлением Правительства Республики Казахстан от 22 августа 2016 года № 475

Сноска. Утратило силу постановлением Правительства РК от 22.08.2016 № 475 (вводится в действие по истечении десяти календарных дней со дня его первого официального опубликования).

П р и м е ч а н и е Р Ц П И !

В соответствии с Законом РК от 29.09.2014 г. № 239-V ЗРК по вопросам разграничения полномочий между уровнями государственного управления см. приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 117.

В соответствии с подпунктом 19-1) статьи 5 Закона Республики Казахстан от 11 января 2007 года "Об информатизации" Правительство Республики Казахстан **П О С Т А Н О В Л Я Е Т :**

1. Утвердить прилагаемые Правила выдачи заключений о соответствии компьютерной системы техническим требованиям для включения в государственный реестр контрольно-кассовых машин.
2. Настоящее постановление вводится в действие по истечении десяти календарных дней со дня первого официального опубликования.

П р е м ь е р - М и н и с т р

Республики Казахстан

К. Масимов

У т в е р ж д е н ы

постановлением

Правительства

Р е с п у б л и к и К а з а х с т а н

от 1 ноября 2011 года № 1265

Правила

выдачи заключений о соответствии компьютерной системы

техническим требованиям для включения в государственный реестр контрольно-кассовых машин

1. Общие положения

1. Настоящие Правила выдачи заключений о соответствии компьютерной системы техническим требованиям для включения в государственный реестр контрольно-кассовых машин (далее - Правила) определяют порядок выдачи уполномоченным органом в области информатизации заключений о соответствии контрольно-кассовых машин, являющихся компьютерной системой (далее - КС), техническим требованиям для включения в государственный реестр контрольно-кассовых машин (далее - Государственный реестр).

2. В настоящих Правилах используются следующие понятия:

1) уполномоченный орган в сфере информатизации (далее - уполномоченный орган) - государственный орган, осуществляющий руководство в сфере информатизации и "электронного правительства";

2) администратор безопасности информационных систем (далее - администратор) - работник организации, обеспечивающий функционирование КС электронного получения и/или передачи данных, реализацию мер по их защите ;

3) комплекс мер по защите информационной системы - организационно-технические мероприятия, направленные на обеспечение безопасного функционирования КС, в том числе, программно-аппаратная защита электронных средств и компьютеров от несанкционированного доступа, обеспечивающая контроль доступа к установленному программному обеспечению и информации, предоставляющая средства разграничения полномочий зарегистрированных пользователей;

4) государственный реестр контрольно-кассовых машин - перечень моделей контрольно-кассовых машин, разрешенных уполномоченным органом, осуществляющий руководство в сфере обеспечения поступлений налогов и других обязательных платежей в бюджет, к использованию на территории Республики Казахстан ;

5) аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа имеющимся в информационной системе;

6) ответственное лицо - оператор, администратор и иные работники организации, обеспечивающие реализацию процесса получения фискальных отчетов и фиксирования всех проводок, фиксирующих денежные расчеты без

возможности их дальнейшей корректировки, осуществляемых при торговых операциях, оказании услуг посредством наличных денег;

7) АРМ кассира (автоматизированное рабочее место кассира или программно-аппаратный комплекс для торговли) - специализированная программное обеспечение, являющееся модулем КС, позволяющее персоналу пункта обслуживания осуществлять регистрацию операций в КС при приеме оплаты за товары и услуги;

8) функциональная копия КС - комплекс программных средств необходимых для полной установки КС;

9) терминал оплаты услуг - электронно-механическое устройство, осуществляющее прием наличных денег в качестве оплаты за услуги в автоматическом режиме;

10) оператор - работник организации, непосредственно осуществляющий подготовку, обработку, прием и передачу сообщений с использованием подсистемы защиты;

11) пользователь - субъект, обращающийся к информационной системе за получением необходимых услуг и товаров;

12) пос-терминал - торговый терминал (программно-аппаратный комплекс для торговли или АРМ кассира), установленный на месте, где кассир осуществляет прием платежей от клиентов;

13) торговый автомат - электронно-механическое устройство, осуществляющее реализацию товаров посредством наличных денег в автоматическом режиме;

14) идентификация - процесс присвоения или определение соответствия предъявленного для получения доступа в систему и/или к ресурсу системы идентификатора перечню идентификаторов, имеющихся в КС;

15) идентификатор - уникальные персональный код и/или имя, присвоенные субъекту и/или объекту системы, и предназначенные для регламентирования доступа в систему и/или к ресурсам системы;

16) регистрационное свидетельство - документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи";

17) фискальные данные - фиксируемая в фискальной памяти контрольно-кассовой машины информация о денежных расчетах;

18) фискальный отчет - отчет об изменении показаний в фискальной памяти контрольно-кассовой машины за определенный период;

19) фискальная память - комплекс программно-аппаратных средств,

обеспечивающих некорректируемую ежесменную регистрацию и энергонезависимое долговременное хранение итоговой информации о произведенных денежных расчетах;

20) фискальный режим - режим функционирования контрольно-кассовой машины, обеспечивающий некорректируемую регистрацию и энергонезависимое долговременное хранение информации в фискальной памяти;

21) электронная цифровая подпись (далее - ЭЦП) - набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

22) электронный документ - документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;

23) средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи.

3. Для выдачи заключения о соответствии компьютерной системы техническим требованиям для включения в Государственный реестр КС должна соответствовать следующим требованиям:

1) применяться для регистрации информации о произведенных денежных расчетах при реализации товаров и оказании услуг;

2) обеспечивать некорректируемую ежесменную регистрацию всех фискальных данных;

3) обеспечивать информационную безопасность, включая устранение возможности раскрытия фискальных данных;

4) обеспечивать энергонезависимое долговременное хранение фискальных данных;

5) обеспечивать равный доступ на государственном и русском языках к модулям КС, используемых при фискальном режиме (интерфейс, выходные формы КС);

6) обеспечивать создание резервных копий, архивирование фискальных данных и их восстановление;

7) обеспечивать использование информационных систем, имеющих средства защиты, с контролем прав доступа;

8) основное и резервное серверное оборудование КС, в том числе фискальная память и средства электронной цифровой подписи, должны находиться на территории Республики Казахстан;

9) наличие и функционирование фискального режима, эксплуатируемого на программно-аппаратных средствах владельца КС;

10) доступ к фискальным данным КС должен осуществляться только с использованием программных средств КС, WEB приложений (с возможностью удаленного доступа).

2. Порядок выдачи заключений о соответствии компьютерной системы техническим требованиям для включения в Государственный реестр

4. Для включения КС в Государственный реестр в соответствии с Кодексом Республики Казахстан от 10 декабря 2008 года "О налогах и других обязательных платежах в бюджет" (Налоговый Кодекс) владелец КС (далее - заявитель) представляет в уполномоченный орган или через веб-портал "электронного правительства": www.e.gov.kz или веб-портал "Е-лицензирование" www.elicense.kz (далее - портал) следующие документы в бумажном или электронном виде, которые удостоверены электронной цифровой подписью заявителя :

1) заполненную анкету-заявление по форме, установленной в приложении 1 к настоящим Правилам ;

2) справку либо свидетельство о государственной регистрации (перерегистрации) юридического лица – для юридического лица, свидетельство о государственной регистрации индивидуального предпринимателя – для физического лица ;

3) описание функциональных возможностей и характеристик КС;

4) инструкцию по эксплуатации модуля "Рабочее место налогового инспектора " ;

5) электронный информационный носитель, содержащий функциональную копию КС, за исключением применяемой в банках и организациях, осуществляющих отдельные виды банковских операций;

6) инструкцию по установке и запуску КС, за исключением применяемой в банках и организациях, осуществляющих отдельные виды банковских операций;

7) сертификат соответствия требованиям информационной безопасности технических и программных средств фискального режима, фискальной памяти, входящих в состав КС и участвующих в информационном процессе (СТ РК ГОСТ Р ИСО/МЭК 15408-2006 "Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий").

При обращении заявителя через портал электронный информационный носитель, содержащий функциональную копию КС, за исключением применяемой в банках и организациях, осуществляющих отдельные виды банковских операций, направляется в уполномоченный орган по почте.

Представление документов, указанных в подпунктах 3), 4), 6), 7) настоящего пункта, в уполномоченный орган или через портал осуществляется в виде " формы сведений", установленной в приложении 4 к настоящим Правилам.

Сноска. Пункт 4 в редакции постановления Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

5. Уполномоченный орган рассматривает вопрос о выдаче заключения о соответствии КС техническим требованиям для включения в Государственный реестр и осуществляет проверку сведений, представленных заявителем.

Сноска. Пункт 5 в редакции постановления Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

6. Уполномоченный орган при выявлении ошибок в оформлении документов, предоставления неполного пакета документов и ненадлежащего оформления документов в течение двух рабочих дней после получения пакета документов оставляет обращение без рассмотрения и возвращает документы заявителю с письменным обоснованием причин отказа в рассмотрении.

7. При соответствии представленных документов требованиям, установленным пунктом 4 настоящих Правил, уполномоченный орган согласно Закону Республики Казахстан от 6 января 2011 года "О государственном контроле и надзоре в Республике Казахстан" назначает проверку на соблюдение заявителем организационно-технических, технологических требований по защите программного обеспечения, соответствие используемых КС требованиям, установленным настоящими Правилами.

Сноска. Пункт 7 в редакции постановления Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

7-1. По итогам проверки уполномоченным органом составляется акт о соответствии КС техническим требованиям (далее - акт), в котором указываются соответствие или причины не соответствия КС к предъявляемым требованиям.

Акт подписывается уполномоченным органом и представителем заявителя. В случае, если представитель заявителя не согласен с принятым решением и отказывается от подписания акта, он представляет в уполномоченный орган в письменной форме информацию о причинах своего отказа и прилагает их к акту.

Сноска. Правила дополнены пунктом 7-1 в соответствии с постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

7-2. На основании акта о соответствии КС техническим требованиям уполномоченный орган выдает заявителю заключение о соответствии КС

техническим требованиям для включения в Государственный реестр или направляет заявителю мотивированное письмо с указанием причин отказа в виде электронного документа, удостоверенного электронной цифровой подписью уполномоченного должностного лица.

В случае обращения в уполномоченный орган за получением заключения на бумажном носителе, заключение оформляется в электронном формате, распечатывается, заверяется печатью ведомства уполномоченного органа.

Сноска. Правила дополнены пунктом 7-2 в соответствии с постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

7-3. Рассмотрение и выдача заключения о соответствии КС техническим требованиям для включения в Государственный реестр или мотивированный отказ уполномоченным органом осуществляются в течение тридцати календарных дней со дня поступления документов, установленных пунктом 4 настоящих Правил.

Сноска. Правила дополнены пунктом 7-3 в соответствии с постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

8. Заявитель должен обеспечить в КС обязательное наличие модуля "Рабочего места налогового инспектора", посредством которого должна производиться постановка КС в режим фискализации и/или снятие КС с режима фискализации. При этом заявитель обеспечивает регистрацию регистрационного свидетельства ответственных сотрудников уполномоченного органа, осуществляющий руководство в сфере обеспечения поступлений налогов и других обязательных платежей в бюджет (далее - налоговый орган) для последующего доступа к фискальным данным КС.

Процесс разработки, внедрения и сопровождения КС включает определение этапов разработки, порядка внесения изменений, приема, тестирования и ввода в эксплуатацию, требования к документированию всех этапов. Разработка, внедрение и сопровождение фискального режима КС выполняется в соответствии с внутренними документами заявителя и действующими стандартами на территории Республики Казахстан.

Заявителем используются лицензионное программное обеспечение, сертифицированное компьютерное, телекоммуникационное оборудование, терминалы оплаты услуг, торговые автоматы, пос-терминалы и иное оборудование, применяемое в информационном процессе фискального режима КС.

Заявитель обеспечивает обязательность фиксирования всех операций КС без возможности их дальнейшей корректировки, связанных с торговыми операциями

, оказанием услуг посредством наличных денег, а также при формировании фискальных отчетов. Выходные формы фискальных отчетов КС содержат ЭЦП заявителя либо его уполномоченного сотрудника.

Контрольные чеки, формируемые КС, должны содержать реквизиты согласно постановлению Правления Национального Банка Республики Казахстан от 31 декабря 2008 года № 117 "Об установлении формы и содержания контрольного чека компьютерных систем, применяемых банками и организациями, осуществляющими отдельные виды банковских операций" и приказа Министра финансов Республики Казахстан от 30 декабря 2008 года № 636 "Об утверждении технических требований и формы соответствия техническим требованиям контрольно-кассовых машин".

9. Организация модуля "Рабочее место налогового инспектора", формирование фискальных отчетов обеспечивается в соответствии техническому требованию и форме соответствия техническим требованиям контрольно-кассовой машины, установленным приказом Министра финансов Республики Казахстан от 30 декабря 2008 года № 636 "Об утверждении технических требований и формы соответствия техническим требованиям контрольно-кассовых машин".

Модуль "Рабочее место налогового инспектора" должен обеспечить возможность блокировки (запрета) выполнения всех операций для торговых точек, касс, терминалов оплаты услуг, торговых автоматов, пос-терминалов и других объектов, участвующих в информационном процесса фискального режима.

10. Уполномоченный орган для проведения проверки специализированного технического оборудования и программного обеспечения, используемых в фискальном режиме, может привлекать специалистов подведомственных организаций и государственных органов в качестве консультантов, экспертов на договорной или безвозмездной основе.

11. Используемые в КС средства криптографической защиты информации (далее - СКЗИ) должны быть сертифицированы согласно СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" и в зависимости от криптографической стойкости, должны соответствовать уровням безопасности согласно СТ РК 1073-2007.

12. КС должна средствами фискальной памяти заявителя обеспечивать невозможность корректировки фискальных данных, а также ежедневную регистрацию и энергонезависимое долговременное хранение итоговой информации о произведенных денежных расчетах.

13. Заявителем принимается комплекс мер по обеспечению информационной безопасности рабочего места (оператора, пользователя, ответственного лица) в

соответствии с требованиями, установленными в пункте 7 приложения 2
н а с т о я щ и х П р а в и л .

14. Исключен постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

15. Исключен постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

16. В случаях изменений версии, модулей КС, используемых для фискального режима, условий формирования операций фискального режима, заявитель представляет соответствующую информацию на бумажном и электронном носителях в уполномоченный орган в течение семи рабочих дней с момента внедрения доработанной КС в промышленную эксплуатацию. Уполномоченный орган проводит проверку измененных версий, модулей КС, используемых для фискального режима, условий формирования операций фискального режима на соответствие техническим требованиям в срок, установленный пунктом 7-3
н а с т о я щ и х П р а в и л .

Сноска. Пункт 16 в редакции постановления Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

П р и л о ж е н и е 1
к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в государственный
реестр контрольно-кассовых машин

Анкета-заявление

Сноска. Приложение 1 с изменением, внесенным постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

Наименование заявителя _____

(ИИН, БИН) |||||

Местонахождение заявителя
Область _____ город _____
Район _____ Улица _____ Дом _____

Название КС _____

Разработчик КС _____

Версия _____ Дата разработки КС _____

Размер инсталляционного пакета _____

Дата создания инсталляционного пакета _____

Местонахождение _____ разработчика _____ КС

Область _____ город _____

Район _____ Улица _____ Дом _____

Заявитель подтверждает, что вышеназванная КС соответствует
с л е д у ю щ и м т р е б о в а н и я м :

В конкретной регистрируемой КС осуществляется описание режима
фискализации (да/нет какими средствами обеспечивается) _____

Идентификация пользователя сервера осуществляется на уровне
операционной системы (ОС) (да/нет, какими средствами обеспечивается)
какими именно _____

Идентификация пользователей КС осуществляется на уровне системы
управления базой данных (далее - СУБД) (да/нет, какими средствами
обеспечивается) _____

Блокировка доступа к серверу средствами СУБД, в случае подбора
пароля (да/нет, какими средствами обеспечивается) _____

Срок действия пароля (кол-во дней):
Пользователя _____ не менее 8-ми знаков

администратор системы _____

администратор базы данных _____

Минимальная длина пароля (кол-во символов):
для пользователя _____

для администратора системы _____

для администратора базы данных _____

Проверка сложности пароля в КС (обязательное использование цифр
и специальных символов) (да/нет, какими средствами обеспечивается)

КС обеспечивает автоматический контроль длины пароля (да/нет,
какими средствами обеспечивается) _____

КС исключает возможность подключения к серверному и клиентскому приложению двух и более пользователей под одной учетной записью (да/нет, какими средствами обеспечивается) _____

Невозможность подключения пользователей приложения к КС средствами, отличными от самого приложения (да/нет, какими средствами обеспечивается) _____

Разграничение прав доступа пользователей к информации в КС средствами СУБД (да/нет, какими средствами обеспечивается) _____

Каждая операция идентифицируется по пользователю, дате и времени (да/нет, какими средствами обеспечивается) _____

Каждая операция однозначно определяется последовательным уникальным номером (да/нет, какими средствами обеспечивается) _____

КС представляет собой архитектуру: клиент-сервер, хост-терминал
(нужное подчеркнуть)

Любая информация вносится в КС только с помощью приложения (да/нет, какими средствами обеспечивается) _____

Невозможность корректировки внесенной в КС и находящихся на клиентской стороне информации различными средствами после начала операции (да/нет, какими средствами обеспечивается) _____

Ошибочно введенная операция исправляется путем осуществления операции "сторно" (да/нет, какими средствами обеспечивается) _____

Конечный пользователь имеет права доступа к КС только в рамках выполняемых им функций (да/нет, какими средствами обеспечивается) _____

Разделение прав между администраторами приложения, СУБД и операционной системы (указать акты, регламентирующие действия администраторов) _____

Журналы аудита автоматически фиксируют все действия пользователей с административными правами и пользовательскими правами (да/нет, какими средствами обеспечивается) _____

Журналы аудита автоматически фиксируют все действия пользователей (да/нет, какими средствами обеспечивается) _____

Отключение клиентского приложения от КС в случае простоя в течение определенного времени (да/нет, какими средствами обеспечивается, временной интервал) _____

Ограничение действий клиентского приложения при работе с КС по времени (да/нет, какими средствами обеспечивается, временной интервал) _____

Блокировка учетных записей, имеющие доступ без авторизации (guest, anonymous и другие) средствами ОС (да/нет, какими средствами обеспечивается, временной интервал) _____

Меры по резервированию данных в случае сбоев компьютерной системы, электропитания и других:

Меры по резервированию данных	Да	Нет
использование дублирующего сервера, использование «кластерной» системы применение на серверах подсистемы RAID разных уровней (1-5) создание резервных копий журналов транзакций и БД		

Иное (указать) _____

Создание резервных копий КС и системного журнала транзакций:

	для КС	Д л я журнала транзакций
периодичность создания резервных копий (раз/месяц, год) количество резервных копий (шт.) срок хранения резервных копий (лет) место хранения резервных копий (резервный центр/сейф и т.д.)		

время полного восстановления системы _____

наличие журнала восстановления КС резервных копий (да/нет)

;

Наличие модуля "Рабочее место налогового инспектора" (да/нет)

;

Наличие подробных процедур по фискализации компьютерной системы в документации по использованию "Рабочее место налогового инспектора" (да/нет) _____;

Реализация в "Рабочее место налогового инспектора" фискального режима КС (да/нет, какими средствами обеспечивается) _____;

Реализация режима формирования криптографических ключей для доступа к фискальным данным (да/нет, какие алгоритмы и стандарты используются) _____;

Реализация в КС криптографических функций при сохранении данных во время закрытия смены, для последующей подготовки фискальных отчетов (да/нет, какие алгоритмы и стандарты используются) _____;

Реализация в модуле "Рабочее место налогового инспектора" формирования фискальных отчетов (да/нет, какими средствами обеспечивается) _____;

Наличие документации по использованию модуля "Рабочее место налогового инспектора" (да/нет) _____.

(Ф.И.О. заявителя или его руководителя) подпись

М.П.

П р и л о ж е н и е 2
к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в государственный
реестр контрольно-кассовых машин

Формирование системы безопасности КС и минимальные требования к помещениям, электронному и техническому оборудованию КС

1. Серверное оборудование КС размещается в нежилом помещении с ограниченным доступом. Помещение ограниченного доступа - помещение, в котором разрешается пребывание ограниченного круга лиц, и доступ других лиц в эти помещения может происходить только в сопровождении специально допущенных работников.

2. Система безопасности КС должна отвечать следующим требованиям, установленным настоящими Правилами:

- 1) к серверному помещению и помещению ограниченного доступа;
- 2) к системному программному обеспечению, используемому для автоматизации деятельности;
- 3) к специализированному программному обеспечению (информационной

системе), используемому для автоматизации деятельности;

4) к техническим средствам (информационным ресурсам);

5) к обеспечению безопасности информации.

3. Оборудованное серверное помещение КС находится в собственности заявителя и/или на условиях "co-location" и оснащено:

1) системой контроля доступа (индивидуальный электронный пропуск);

2) системой видеоконтроля входа в серверное помещение и кроссовые комнаты ;

3) автоматической системой газового пожаротушения с обязательным полным резервом баллонов с газом и подключенной к системе гарантированного питания ;

4) системой охранной сигнализации при наличии дверей, окон и датчиками движения внутри гермозоны ;

5) системой гарантированного чистого питания всей электрической сети серверной и кроссовых комнат, включая круглосуточное, дежурное освещение;

6) системой кондиционирования с полным резервом;

7) металлическими решетками окна помещений при расположении помещения ограниченного доступа на первых или последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц.

4. Серверное помещение должно располагаться в местах, где возможно впоследствии расширение пространства и есть возможность размещения крупногабаритной аппаратуры, и отвечать следующим требованиям:

1) минимальный допустимый размер серверной комнаты - не менее 4 квадратных метров ;

2) серверная комната должна быть соединена с главным электродом системы заземления здания кондуитом размером 1,5.

5. Рабочее место пользователя (ответственное лицо, оператор) КС должно соответствовать следующим требованиям:

1) программное обеспечение устанавливается на специально выделенном персональном компьютере, на который оформлен паспорт с указанием месторасположения, конфигурации, а также аппаратных и программных средств, установленные на нем. Паспорт оформляется за подписью руководителя организации/руководителя филиала и хранится у ответственного лица;

2) персональный компьютер должен иметь комплекс защиты, включающий в себя :

средства идентификации и аутентификации пользователей;

возможность ведения электронных журналов в течение срока хранения электронных документов, с целью контроля деятельности, связанной с доступом к компьютеру и действиями пользователей;

3) наличие одного системного имени пользователя (ответственного лица), по которому идентифицируется пользователь, при входе в информационную систему должно соответствовать одному физическому лицу;

4) персональный компьютер должен быть защищен лицензионным или свободно распространяемым антивирусным программным обеспечением с актуальной базой сигнатур;

5) доступ к сетевым ресурсам, внешним носителям информации, а также к портам ввода-вывода информации с персонального компьютера должен быть отключен, в том числе и в настройках базовой системы ввода-вывода (BIOS). В случае, если архитектура КС для корректной работы предполагает использование общих сетевых ресурсов (например, использование сетевого ресурса с содержанием шаблонов выходных форм КС), то условие отключения доступа к сетевым ресурсам исключается. В случае использования порта ввода-вывода информации с персонального компьютера (например, для подключения принтера посредством USB-шнура) необходимо обеспечить применение средств контроля доступа к сменным носителям и устройствам;

6) системный блок, неиспользуемые порты ввода-вывода информации персонального компьютера опечатываются либо пломбируются администратором. Процесс опечатывания (пломбирования) фиксируется в специальном журнале с указанием фамилии, имени, при наличии - отчества, должности, даты, времени и цели нанесения пломбы (печати). Для ноутбуков разрешается использовать только отключение устройств в базовой системе ввода-вывода без опечатывания портов. Выносить из здания компьютеры и ноутбуки, используемые в фискальном режиме, не допускается, за исключением случаев проведения профилактических и ремонтных работ, которые проводятся на основании заявки ответственного лица руководителю службы информационной безопасности;

7) порядок доступа к иным ресурсам (дисковое пространство, директории, базы данных и резервные копии базы данных), выделенным для накопления в них информации для передачи в информационную среду с использованием системы защиты, получения информации из информационной среды, хранения, архивирования либо другой обработки информации, должен исключать возможность несанкционированного доступа к этим ресурсам;

8) доступ к рабочему месту и в помещение ограниченного доступа обеспечивается в соответствии с его должностными обязанностями.

6. Использование системного и программного обеспечений (операционные системы, системы управления базами данных, офисные, антивирусные программы) заявителем должно подтверждаться соответствующими лицензиями, сертификатами.

7. В целях информационной безопасности программного обеспечение КС должно обеспечивать следующее:

1) доступ к просмотру фискальных данных КС имеет только ответственный сотрудник налогового органа с обязательным использованием закрытого ключа и СКЗИ КС посредством идентификации и аутентификации;

2) разграничение прав доступа пользователей;

3) работу на уровне ядра программного обеспечения таким образом, чтобы ни одно значимое действие в рамках системы (будь то действие пользователя или процесса) не происходило без авторизации пользователя и аудита операций;

4) схема безопасности, реализованная в программном обеспечении КС, должна быть отделена от средств безопасности самой операционной системы, на которой будет реализовано программное обеспечение КС, в том смысле, что уязвимость средств безопасности операционной системы не должна влиять на работу безопасности программного обеспечения КС;

5) замкнутое сохранение фискальных данных в программном обеспечении КС должно быть организовано способом, обеспечивающим:

невозможность получения логического доступа к фискальным данным вне рамок работы приложения программного обеспечения КС;

любые перемещения фискальных данных в фискальной памяти программного обеспечения КС под контролем механизмов безопасности;

6) фиксирование информации, необходимой для идентификации факта, объекта и субъекта процесса удаления, изменение и возможность восстановления удаленных данных;

7) возможность устойчивой работы при появлении сбоев;

8) использование архитектуры "клиент-сервер" с тем, чтобы вывод из строя рабочего места пользователя или получение злоумышленником несанкционированного доступа к нему не сказывался на работе серверной части КС, а сбой сервера приложений не влиял на состояние фискальной памяти;

9) аудит системно-значимых событий с фиксированием в регистрационный журнал, а также с возможностью защиты со стороны любого субъекта;

10) аудит действий пользователей и администраторов, как успешных, так и неудачных, начиная от попытки установления связи;

11) контроль экспортируемых и импортируемых фискальных данных в фискальную память;

12) возможность разработки (доработки) модулей и механизмов безопасности

.

8. Требования к техническим средствам заявителя:

1) наличие собственного аппаратного обеспечения (компьютерное и серверное оборудование, аппаратные и программные средства защиты,

комплектующие и другое оборудование), также наличие документов, подтверждающих принадлежность аппаратного обеспечения заявителю;

2) наличие системы гарантированного питания - щита автоматического включения резерва, дизельного генерирующего устройства, работающих от сигнала с двух источников бесперебойного питания (далее - ИБП) и непрерывно поддерживающей электричество в сети чистого питания.

9. Серверы КС должны составлять отказоустойчивую завершенную архитектуру и представлять собой кластер со стопроцентным дублированием аппаратной части. Резервный сервер фискальных данных, приложений КС должен быть расположен на расстоянии не менее одного километра от основного сервера.

10. Требования к организации по обеспечению безопасности информации:

1) наличие защищенного канала передачи данных между территориально разделенными подразделениями организации с шифрованием трафика с помощью аппаратных граничных маршрутизаторов;

2) наличие системы обнаружения (предотвращения) атак из сети Интернет посредством межсетевого экрана;

3) наличие систем идентификации и аутентификации пользователя;

4) наличие аппаратного сетевого анализатора трафика по идентификатору управления доступом к носителю сетевых карт основного и резервного серверного оборудования КС, используемых в фискальном режиме;

5) наличие системы резервного копирования КС.

Для реализации вышеуказанных требований заявитель проводит анализ и оценку рисков, уязвимостей и угроз для обеспечения безопасности информации.

11. Заявитель в процессе своей деятельности выполняет следующие требования:

1) наличие службы информационной безопасности;

2) наличие ответственных лиц по КС;

3) наличие политики информационной безопасности (нормы и практические приемы, регулирующие управление, защиту и распределение информации ограниченного доступа);

4) наличие политики формирования и использования паролей;

5) наличие политики резервного копирования (архивирования);

6) наличие документации с описанием процедур по ограничению доступа и обязанностей пользователей, администраторов безопасности, системных администраторов.

12. Заявитель принимает внутренний документ, который определяет порядок работы с информационной системой, включающий:

1) порядок назначения сотрудников, на которых возлагаются обязанности

о т в е т с т в е н н ы х

л и ц ;

2) р е ж и м р а б о т ы ;

3) права и обязанности ответственных лиц, включая должностные инструкции ;

4) список сотрудников, допущенных к рабочему месту (оператора, ответственного лица) ;

5) список сотрудников, допускаемых к рабочему месту (оператора, ответственного лица) в особых случаях (в кризисных ситуациях, а также в случаях замещения сотрудника).

13. Ответственные лица :

1) обеспечивают обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;

2) не допускают получения права доступа к информационным ресурсам неавторизованными пользователями;

3) контролируют регулярность выполнения резервного копирования информации, обрабатываемой информационной системой;

4) проводят плановую и внеплановую проверку надежности защиты ресурсов с и с т е м ы ;

5) обеспечивают защиту оборудования корпоративной сети, в том числе специальных межсетевых программных средств;

6) принимают меры по отражению угрозы и выявлению нарушителей;

7) регулярно просматривают журнал событий, проводят анализ с записями, где были попытки несанкционированного доступа к информации.

14. Заявитель на постоянной основе осуществляет контроль использования действительных регистрационных свидетельств следующих пользователей:

1) ответственного сотрудника налогового органа;

2) ответственных лиц заявителя;

3) владельцев терминалов оплаты услуг, пос-терминалов;

4) других лиц взаимодействующих с КС.

15. Порядок хранения и использования внешних носителей информации, на которых хранится закрытый ключ уполномоченного сотрудника заявителя, должен исключать возможность несанкционированного доступа к нему.

16. Порядок обеспечения фискального режима, минимальные требования к модулю "рабочее место налогового инспектора", требования к применению ЭЦП должны отвечать следующим требованиям:

1) создаваемые в КС операции подлежат заверению ЭЦП;

2) при проверке операций необходимо проверять ЭЦП на действительность: регистрационное свидетельство выпущено доверенным УЦ; регистрационное свидетельство разрешено применять для подписи

т р а н з а к ц и й ;

регистрационное свидетельство не отозвано;
срок действия регистрационного свидетельства не истек;

3) идентификация и аутентификация в КС ответственного сотрудника
налогового органа должна происходить с использованием СКЗИ и его закрытого
к л ю ч а .

17. Требования к операциям, осуществляемым с КС:

1) запрос на проведение операции, связанных с денежными расчетами, в КС
формируется в форме электронного документа;

2) запрос на проведение операции в КС содержит информацию:
порядковый номер операции в КС;
порядковый номер операции за смену;
реквизиты оператора (терминал оплаты услуг, пос-терминал, касса и т.д.);
реквизиты получателя операции;
наименования операции, товара, работы, услуги;
о б щ а я с у м м а о п е р а ц и и ;
с у м м а к о м и с с и и ;
дата и время совершения операции, покупки товаров, выполнения работ,
о к а з а н и я у с л у г ;

3) формирование отчетов по операциям с наличными деньгами;

4) исключение возможности удаления подтвержденных контролем операций
и исправление ошибочно введенных операций путем осуществления операции "
с т о р н о " ;

5) запрет корректировки информации, внесенной в фискальную память КС,
средствами приложения КС после подтверждения операции.

18. Требование к паролю пользователей КС:

1) установление для каждого пользователя индивидуального, уникального (в
рамках соответствующей подсистемы регистрации) идентификатора (системное
и м я и п а р о л ь) ;

2) блокирование пользовательской записи средствами СУБД или средствами
программного обеспечения КС в случае подбора пароля после третьей неудачной
п о п ы т к и р е г и с т р а ц и и К С ;

3) минимальная длина пароля пользователя должна составлять 6 символов,
администраторов - 8 символов, с обязательным включением, помимо букв, цифр
и специальных символов. Система должна предусматривать автоматический
к о н т р о л ь д л и н ы п а р о л я ;

4) срок действия пароля должен составлять не более 30 календарных дней и
контролироваться средствами операционной системы (далее - ОС) и
программного обеспечения КС.

19. Требования по доступу к информации:

- 1) разграничение прав доступа пользователей к фискальным данным, как средствами СУБД, так и средствами приложения;
- 2) идентификация пользователя сервера и базы данных, как на уровне ОС, так и на уровне СУБД;
- 3) исключение возможности подключения к приложению КС двух и более пользователей под одним системным именем, а также подключения пользователей приложения КС к базе данных средствами, отличными от своего приложения;
- 4) возможность внесения информации в БД только с помощью приложения;
- 5) возможность создания индивидуальных графиков работ в рабочие и выходные дни;
- 6) создание с помощью СУБД журнала аудита для отслеживания действий конкретного пользователя, включая пользователей с административными правами, по вводу, корректировке и удалению информации;
- 7) оператор должен иметь права владения БД только в рамках выполняемых им функций;
- 8) блокирование учетных записей, имеющих доступ без авторизации (guest, anonymous и другие) средствами ОС в целях исключения несанкционированного доступа к серверу и его ресурсам;
- 9) автоматическое блокирование доступа к приложению с последующей проверкой идентификации средствами приложения, ОС и СУБД, в случаях, когда приложение пользователя неактивно.

Приложение 3
к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в государственный
реестр контрольно-кассовых машин

Заключение

**о соответствии компьютерной системы техническим требованиям
для включения в государственный реестр
контрольно-кассовых машин**

Сноска. Приложение 3 исключено постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

П р и л о ж е н и е 4

к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в государственный
реестр контрольно-кассовых машин

Форма сведения

Сноска. Правила дополнены приложением 4 в соответствии с постановлением Правительства РК от 15.04.2013 № 348 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

1. Общая информация

1. Заявитель _____
2. ИИН/БИН _____
3. Наименование _____

4. Представленные документы:

Инструкция по эксплуатации модуля «Рабочее место налогового инспектора» _____ (да/нет)

Инструкция по установке и запуску компьютерной системы, за исключением применяемой в банках и организациях, осуществляющих отдельные виды банковских операций _____ (да/нет)

Номер входящего письма ведомства уполномоченного органа _____ (да/нет)

Дата входящего письма ведомства уполномоченного органа _____ (да/нет)

2. Описание КС

5. Н а и м е н о в а н и е К С
_____ (да/нет)

В е р с и я
_____ (да/нет)

Д а т а р а з р а б о т к и К С
_____ (да/нет)

Размер инсталляционного пакета
_____ (да/нет)

Дата создания инсталляционного пакета
_____ (да/нет)

Д а т а р е г и с т р а ц и и

_____ (да/нет)
Дата изменений сведений
_____ (да/нет)

3. Сертификат соответствия

6. Номер протокола испытаний аккредитованной испытательной
лаборатории

Дата протокола испытаний аккредитованной испытательной
лаборатории

Наименование испытательной лаборатории

Номер сертификата

Дата выдачи сертификата

Дата окончания действия сертификата

№ К С