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

Утративший силу

Приказ Председателя Агентства Республики Казахстан по информатизации и связи от 27 июля 2009 года № 330. Зарегистрирован в Министерстве юстиции Республики Казахстан 31 июля 2009 года № 5732. Утратил силу приказом Министра транспорта и коммуникаций Республики Казахстан от 26 марта 2012 года № 132

Сноска. Утратил силу приказом Министра транспорта и коммуникаций РК от 26.03.2012 № 132.

В соответствии с пунктом 3 статьи 651 Кодекса Республики Казахстан "О налогах и других обязательных платежах в бюджет" (Налоговый Кодекс), с целью установления порядка выдачи заключений для включения компьютерных систем в Государственный реестр контрольно-кассовых машин, **ПРИКАЗЫВАЮ**:

1. Утвердить прилагаемые Правила выдачи заключений о соответствии компьютерной системы техническим требованиям для включения в государственный реестр контрольно-кассовых машин.

2. Департаменту информационных технологии Агентства Республики Казахстан по информатизации и связи (Елеусизова К.Б.) обеспечить в установленном порядке:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан его официальное опубликование в средствах массовой информации.

3. Признать утратившим силу приказ и.о. Председателя Агентства Республики Казахстан по информатизации и связи от 3 сентября 2004 года № 186 -п "Об утверждении Правил выдачи заключений для включения (исключения) компьютерных систем в (из) Государственный(-ого) реестр(а) контрольно-кассовых машин с фискальной памятью, разрешенных к использованию на территории Республики Казахстан" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов за № 3139, опубликованный в газетах "Юридическая газета" и "Заң газеті" от 18 ноября 2005

г о д а) .

4. Контроль за исполнением настоящего приказа возложить на заместителя Председателя Агентства Республики Казахстан по информатизации и связи Д у р м а г а м б е т о в а Е . Д .

5. Настоящий приказ вводится в действие со дня официального опубликования.

Председатель *К. Есекеев*

С о г л а с о в а н о
М и н и с т р ф и н а н с о в
Р е с п у б л и к и К а з а х с т а н
_ _ _ _ _ _ _ _ _ _ *Б . Ж а м и ш е в*

28 июля 2009 года

У т в е р ж д е н ы
п р и к а з о м П р е д с е д а т е л я
А г е н т с т в а Р е с п у б л и к и К а з а х с т а н
п о и н ф о р м а т и з а ц и и и с в я з и
от 27 июля 2009 года № 330

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 и связи (далее - Уполномоченный орган) 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 понятия, предусмотренные Кодексом Республики Казахстан "О налогах и других обязательных платежах в бюджет" (Н а л о г о в ы й к о д е к с) .

3. Для включения в Государственный реестр КС должны соответствовать с л е д у ю щ и м т р е б о в а н и я м :

применяться для регистрации денежных расчетов при реализации товаров и оказании услуг;

обеспечивать некорректируемую ежесменную регистрацию каждого отдельного платежа;

обеспечивать информационную безопасность, включая устранение возможности раскрытия информации;

обеспечивать энергонезависимое долговременное хранение информации;

обеспечивать равный доступ ко всем функциям системы на государственном и русском языках;

обеспечивать создание резервных копий, архивирование данных;

обеспечивать использование информационных систем, имеющих штатные средства защиты, с контролем за правами доступа.

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

4. Для включения КС в Государственный реестр, в соответствии с законодательством Республики Казахстан, владелец КС (далее - заявитель) представляет в Уполномоченный орган заявку, состоящую из следующих документов заполненных как на государственном и русском языках:

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

2) полное описание функциональных возможностей и характеристик КС и инструкцию по эксплуатации режима "Рабочее место налогового инспектора";

3) компакт диск, содержащий функциональную копию КС;

4) инструкцию по установке и запуску КС;

5) нотариально засвидетельствованную копию свидетельства о государственной регистрации, перерегистрации юридического лица или свидетельства о государственной регистрации без образования юридического лица (индивидуального предпринимателя);

6) нотариально засвидетельствованную копию свидетельства о регистрации в качестве налогоплательщика;

7) нотариально засвидетельствованные копии учредительных документов юридического лица;

8) нотариально засвидетельствованную копию лицензии на право занятия предпринимательской деятельностью, подлежащей обязательному лицензированию в соответствии с Законом Республики Казахстан "О лицензировании";

9) нотариально засвидетельствованную копию статистической карточки юридического лица;

10) нотариально засвидетельствованные копии сертификатов соответствия требованиям информационной безопасности технических и программных средств, входящих в состав КС и подлежащих подтверждению соответствия в соответствии с законодательством Республики Казахстан.

Документы представляются на бумажном носителях либо электронным документом удостоверенной электронной цифровой подписью заявителя.

5. Рассмотрение вопроса о выдаче заключения о соответствии компьютерной системы техническим требованиям и документам для включения КС в Государственный реестр и проверка сведений, представленных заявителем на соответствие установленным требованиям осуществляется Уполномоченным органом в течение тридцати календарных дней со дня поступления анкеты-заявления с приложением всех необходимых материалов.

6. Уполномоченный орган при выявлении ошибок в оформлении документов, предоставления неполного пакета документов, и ненадлежащем оформлении документов, в течение трех рабочих дней после получения пакета документов оставляет заявку без рассмотрения и возвращает документы заявителю письменным обоснованием причин отказа.

7. Уполномоченный орган в пределах своей компетенции осуществляет проверку специализированного технического оборудования и программного обеспечения согласно требованиям, установленным в приложении 2 к настоящим Правилам.

8. Уполномоченный орган для проведения проверки специализированного технического оборудования и программного обеспечения может привлекать специалистов, консультантов, экспертов подведомственных организаций и государственных органов (далее - эксперты) на договорной или безвозмездной основе.

9. Уполномоченный орган в ходе рассмотрения вопроса о выдаче заключения о соответствии КС техническим требованиям и документам в Государственный реестр производит тестирование режимов КС. В случае невозможности запуска системы в Уполномоченном органе допускается проведения тестирования на территории заявителя (на стенде заявителя) с обязательным участием представителей компании разработчика КС.

10. Уполномоченный орган в пределах своей компетенции осуществляет запрос у заявителя детальную информацию о технических характеристиках КС, посещение заявителей с целью проведения экспертизы КС на месте.

11. При подготовке заключения о соответствии КС техническим требованиям и документам для включения КС в Государственный реестр необходимо

учитывать наличие "Рабочего места налогового инспектора", с помощью которого должна производиться постановка КС в режим фискализации.

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 КС выполняется в соответствии с их внутренними документами и действующими на территории Республики Казахстан стандартами.

При формировании и использовании КС и средств защиты применяются сертифицированные оборудование и программное обеспечение.

Осуществляется проверка на отсутствие иного доступа к некорректируемой фискальной информации. Также необходимо учитывать создание запроса на формирование крипто-ключей и выдачу их для доступа к фискальным данным КС, обязательность фиксирования всех проводок фиксирующих денежные расчеты без возможности их дальнейшей корректировки, осуществляемых при торговых операциях, оказании услуг посредством наличных денег, платежных банковских карточек, чеков, получении фискальных отчетов.

12. Средства криптографической защиты информации, используемые системой при формировании крипто-ключей доступа к фискальным данным и ассиметричного шифрования должны быть сертифицированы в соответствии с законодательством Республики Казахстан о техническом регулировании.

13. Организация модуля "Рабочее место налогового инспектора", а также печать фискальных отчетов должны осуществляться согласно Техническому требованию и форме соответствия техническим требованиям контрольно-кассовой машины, утвержденной приказом Министра финансов Республики Казахстан от 30 декабря 2008 года № 636.

14. Наличие в КС защиты программно-операционной среды от несанкционированного доступа и проникновения вирусных программ. КС должна иметь полное руководство по использованию системы и ее защиты в целом.

15. КС должна собственными средствами обеспечивать невозможность корректировки данных в любое время, как на серверах, так и на клиентских машинах КС.

16. КС должна обеспечивать информационную безопасность рабочего места (оператора, налогового инспектора) в соответствии с инструкцией по обеспечению информационной безопасности рабочего места, пользователя/оператора.

17. Соблюдение заявителем организационно-технических, технологических требований по защите программного обеспечения, соответствие используемых

КС установленным настоящими Правилами и законодательством Республики Казахстан условиям и требованиям, подтверждается экспертной группой Уполномоченного органа, в которую также могут входить представители Национального банка Республики Казахстан, Налогового комитета Министерства финансов Республики Казахстан и эксперты. Форма подтверждения - Акт о соответствии требованиям.

Акт о соответствии подписывается всеми членами экспертной группы и представителем заявителя. В случае, если один из членов экспертной группы не согласен с принятым решением и не подписывает акт о соответствии, он представляет в письменной форме информацию о причинах своего отказа экспертной группы и прилагает их к акту о соответствии.

Акт о соответствии считается принятым при наличии двух третей подписей членов экспертной группы.

18. По итогам рассмотрения заявки Уполномоченный орган выдает заключение о соответствии компьютерной системы техническим требованиям и документам для включения КС в государственный реестр контрольно-кассовых машин, предусмотренным Кодексом Республики Казахстан "О налогах и других обязательных платежах в бюджет" (Налоговый кодекс).

19. Заключение о соответствии КС техническим требованиям и документам выдается по форме, установленной в приложении 3 к настоящим Правилам.

20. В случае несоответствия КС к техническим требованиям и документам, Уполномоченный орган направляет заявителю мотивированное письмо с указанием причин отказа.

21. После устранения выявленных несоответствий КС техническим требованиям и документам Заявитель вносит повторную заявку.

22. В случаях изменений версии, модулей КС, а также условий их формирования, заявитель представляет соответствующую информацию на бумажном и электронном носителях в Уполномоченный орган в течение семи рабочих дней с момента ее внедрения в промышленную эксплуатацию.

Уполномоченный орган проводит проверку измененных версий и модулей КС на соответствие техническим требованиям.

Приложение 1
к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в государственный
реестр контрольно-кассовых машин

Анкета-заявление

Наименование заявителя

_____

_____

_____

РНН |__|__|__|__| | | | | | | | | |

Местонахождение заявителя

Область _____ Город _____

Район _____ Улица _____ Дом _____

Название КС _____

_____

Разработчик КС _____

Версия _____ Дата создания КС _____

Местонахождение разработчика КС

Область _____ Город _____

Район _____ Улица _____ Дом _____

Заявитель подтверждает, что вышеназванная КС соответствует следующим требованиям:

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

_____

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

(_____

Идентификация пользователя базой данных (БД) осуществляется на уровне системы управления базой данных (СУБД) (да/нет, какими средствам обеспечивается)

_____

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

_____

Срок действия паролей (кол-во дней):

Пользователя ___ не менее 8-ми знаков _____

администратора системы _____

администратора 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 одним системным именем (да/нет, какими средствами обеспечивается)

_____

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

_____

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

_____

Разграничение прав доступа пользователей к информации в БД средствами приложения (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 БД только с помощью приложения (да/нет, какими средствами обеспечивается) _____

_____

Невозможность корректировки внесенной в БД 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 владения БД только в рамках

выполняемых им функций (да/нет, какими средствами обеспечивается)

_____

Разделение прав между администраторами приложения, СУБД и сервера (указать акты, регламентирующие действия администраторов)

_____

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

_____

Аудиторские журналы автоматически фиксируют все действия пользователей (да/нет, какими средствами обеспечивается) _____

_____

Отключение клиентского приложения от БД в случае простоя в течение определенного времени (5 минут) (да/нет, какими средствами обеспечивается, временной интервал) _____

_____

Ограничение действий клиентского приложения при работе с БД 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 восстановлению данных в случае сбоев компьютерной системы, электропитания и других:

Меры по восстановлению 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 БД и системного журнала транзакций:

	для БД	Для 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 БД резервных копий (да/нет) ____

Наличие "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" режима фискализации компьютерной системы (да/нет, какими средствами обеспечивается) _____;

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

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

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

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

_____ _____

Ф.И.О. заявителя или его руководителя подпись

М.П.

Приложение 2
к Правилам выдачи заключений
о соответствии компьютерной
системы техническим требованиям
для включения в Государственный
реестр контрольно-кассовых машин

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

1. Компьютерная система размещается в нежилом здании, помещении с ограниченным доступом.

2. Система безопасности компьютерной системы должна отвечать 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 компьютерной системы содержит:

1) систему контроля доступа (индивидуальный электронный пропуск);

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

3) автоматическую систему газового пожаротушения с обязательным, полным резервом баллонов с газом, и подключенной к системе гарантированного питания;

4) систему охранной сигнализации дверей, окон и датчиками движения внутри гермозоны;

5) безотказную систему чистого питания находящуюся в гермозоне серверной комнаты;

6) систему гарантированного питания всей электрической сети серверной и кроссовых комнат, включая круглосуточное, дежурное освещение;

7) систему кондиционирования с полным резервом;

8) запрещается располагать в помещении рабочие места, не имеющие отношения к деятельности владельца КС;

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

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 - 20 квадратных метров;

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

3) требуемая минимальная высота потолка серверной комнаты должна составлять 2,44 метра.

5. Рабочее место пользователя КС должно соответствовать следующим требованиям:

1) программное обеспечение устанавливается на специально выделенном персональном компьютере, имеющем паспорт, в котором указано его

месторасположение, конфигурация, а также аппаратные и программные средства , установленные на нем. Паспорт оформляется за подписью руководителя организации и хранится у ответственного лица;

2) не допускается эксплуатация персонального компьютера ответственного лица и установка на нем программных средств, не связанных с целями подготовки, обработки, передачи или ведения электронных документов в рамках участия в информационной системе;

3) персональный компьютер ответственного лица 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;

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

5) персональный компьютер должен иметь средства обеспечения целостности и конфиденциальности программного обеспечения;

6) доступ к сетевым ресурсам и внешним носителям, а также к портам ввода-вывода информации с персонального компьютера оператора должен быть отключен, в том числе и в настройках базовой системы ввода-вывода;

7) системный блок, 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 не допускается, за исключением случаев проведения профилактических и ремонтных работ, которые проводятся на основании заявки ответственного лица руководителю службы информационной безопасности;

8) 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;

9) доступ к рабочему месту ответственного лица и в помещение ограниченного доступа осуществляется в соответствии с его должностными

обязанностями.

6. Использование заявителем системных программных обеспечений (операционные системы, системы управления базами данных, офисные программы, антивирусные программы) должны подтверждаться лицензиями, сертификатами.

7. В целях информационной безопасности программное обеспечение должно обеспечивать следующее:

1) идентификацию и аутентификацию с криптографическим преобразованием ;

2) разграничение прав 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 участия механизма безопасности;

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

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

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

любые перемещения данных в/из базу данных программного обеспечения 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) трехуровневую архитектуру "клиент-сервер" с тем, чтобы вывод из строя рабочего места пользователя или получение злоумышленником несанкционированного доступа к нему не сказывался на работе серверной части системы, а сбой сервера приложений не влиял на состояние данных системы;

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 данных;

12) возможность разработки (доработки) модулей и механизмов безопасности .

8. Требования к техническим средствам заявителя:

1) наличие собственного аппаратного обеспечения (компьютерное оборудование, серверы, аппаратные средства защиты, комплектующие и другое оборудование), также наличие документов, подтверждающих принадлежность аппаратного обеспечения заявителю;

2) наличие сертификатов соответствия аппаратного обеспечения на соответствие требованиям безопасности, выданных органом подтверждения соответствия;

3) 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 во всей организации. При этом, нагрузка каждого ИБП должна быть не более сорока процентов в штатном режиме.

9. Серверы КС должны составлять отказоустойчивую завершенную систему и представлять собой кластер со стопроцентным дублированием аппаратной части. Резервный сервер базы данных кредитного бюро должен быть расположен от основного сервера на расстоянии не менее десяти километров.

10. Требования к организации по обеспечению безопасности информации:

1) наличие защищенного канала передачи данных с шифрованием трафика с помощью аппаратных граничных маршрутизаторов;

2) наличие системы обнаружения (предотвращения) атак из сети Интернет в компьютерную сеть организации с помощью межсетевого экрана;

3) наличие системы криптографической защиты компьютеров с помощью криптоключей и систем идентификации пользователя;

4) наличие аппаратного сетевого анализатора трафика по идентификатору управления доступом к носителю сетевых карт пользователей;

5) наличие системы резервного копирования - библиотеки на внешние носители информации.

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;

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 ответственных лиц;

2) режим работы;

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

4) список сотрудников, допущенных к рабочему месту оператора;

5) список сотрудников, допускаемых к рабочему месту оператора 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 системы;

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. Сотрудники заявителя (ответственное лицо, администратор, оператор) дают письменное обязательство о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими служебных обязанностей.

15. При увольнении ответственного лица производится внеплановая смена ключевой информации заявителя. Новая ключевая информация вводится в действие со дня их увольнения.

16. Порядок хранения и использования внешних носителей с ключевой информацией у заявителя должен исключать возможность несанкционированного доступа к ним.

17. Требования к доступу информации:

1) разграничение прав доступа операторов к информации в БД как средствами СУБД, так и средствами приложения;

2) идентификация операторов сервером и БД, как на уровне ОС, так и на уровне СУБД;

3) исключение возможности подключения к приложению двух и более операторов под одним системным именем, а также подключения операторов к БД 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 аудиторского журнала для отслеживания действий администратора по вводу, корректировке и удалению информации из БД;

7) оператор рабочей станции должен иметь права владения БД только в рамках выполняемых им функций;

8) автоматическое блокирование доступа к приложению с последующей проверкой идентификации средствами приложения, ОС и СУБД в случаях, когда приложение оператора неактивно в течение нескольких минут.

18. Требования к операциям, осуществляемым с КС:

1) идентификация каждой кассовой операции по оператор, дате и времени. Каждая операция должна однозначно определяться последовательным уникальным номером, а не клиентским приложением;

2) формирование отчетов по операциям с наличными деньгами, платежными карточками и чеками о количестве полученных наличных денег за определенный период времени;

3) исключение возможности удаления подтвержденных контролем операций и исправление ошибочно введенных операций путем осуществления операции "сторно";

4) запрет корректировки внесенной в БД информации средствами приложения после подтверждения операции.

19. Требования к паролю БКС:

1) установление для каждого пользователя БКС индивидуального, уникального (в рамках соответствующей подсистемы регистрации) идентификатора (системное имя и пароль);

2) блокирование рабочей станции средствами СУБД в случае подбора пароля после третьей неудачной попытки регистрации БКС;

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 контроль длины пароля;

4) срок действия пароля должен составлять не более 30 дней и

контролироваться средствами ОС и СУБД.

20. Требования по доступу к информации:

1) разграничение прав доступа пользователей к информации в БД как средствами СУБД, так и средствами приложения;

2) идентификация пользователя сервера и БД, как на уровне ОС, так и на уровне СУБД;

3) исключение возможности подключения к приложению двух и более пользователей под одним системным именем, а также подключения пользователей приложения к БД 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 аудиторского журнала для отслеживания действий конкретного пользователя, включая пользователей с административными правами, по вводу, корректировке и удалению информации из БД;

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 в течение 5 минут.

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

Заключение

Агентства Республики Казахстан по информатизации и связи о соответствии компьютерной системы техническим требованиям для включения в государственный реестр контрольно-кассовых машин

г. Астана "____"_____ 200__ г.

1. Заявитель _____
2. Местонахождение заявителя: _____

Область _____ Город _____

Район _____ Улица _____ Дом _____

Телефон _____ Факс _____

3. _____

(наименование КС)

_____,

версия _____, дата создания _____,

Разработчик _____

Местонахождение разработчика:

Страна _____ Область _____ Город _____

Район _____ Улица _____ Дом _____

Телефон _____ Факс _____

Соответствует техническим требованиям, предусмотренным законодательством Республики Казахстан.

Председатель Агентства Республики Казахстан по информатизации и связи _____

(подпись)

М.П.