ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Руководящий документ

ЗАЩИТА ИНФОРМАЦИИ В КОНТРОЛЬНО-КАССОВЫХ МАШИНАХ И АВТОМАТИЗИРОВАННЫХ КАССОВЫХ СИСТЕМАХ. КЛАССИФИКАЦИЯ КОНТРОЛЬНО-КАССОВЫХ МАШИН, АВТОМАТИЗИРОВАННЫХ КАССОВЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Москва – 1998

Руководящий документ Гостехкомиссии России «Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации». – М.: ГТК РФ, 1998. – 11 с.

Настоящий руководящий документ распространяется на электронные контрольно-кассовые машины (ККМ) и автоматизированные кассовые системы (АКС), которые осуществляют обработку информации, подлежащей контролю налоговыми органами.

Руководящий документ устанавливает термины и основные понятия в области защиты информации в ККМ и АКС, классификацию ККМ, АКС и требования по защите информации, связанной с налогообложением, в ККМ и АКС различных сфер применения.

Документ должен использоваться как нормативно-методический материал для производителей, разработчиков и поставщиков ККМ и АКС при формулировке и реализации требований по защите информации о денежных расчетах с населением, необходимой для правильного исчисления налогов и контроля налоговыми органами, а также испытательными лабораториями (центрами) при проведении сертификации данных устройств в Системе сертификации средств защиты информации по требованиям безопасности информации (РООС RU 0001.01БИ00).

Руководящий документ разработан в соответствии с Законами Российской Федерации «О применении контрольно-кассовых машин», «Об информации, информатизации и защите информации» и в соответствии с Указом Президента Российской Федерации от 16 февраля 1993 года №224 «Об обязательном применении контрольно-кассовых машин предприятиями, учреждениями и организациями всех форм собственности при осуществлении расчетов с населением».

Документ учитывает технические требования (в части защиты информации) к электронным ККМ различных моделей и сфер применения, включенных в Государственный реестр Российской Федерации, технические требования к фискальной памяти электронных ККМ и пакетам прикладных программ.

Принятые сокращения:

ККМ - контрольно-кассовая машина;

АКС - автоматизированная кассовая система;

СВТ - средство вычислительной техники;

ЗУ - запоминающее устройство;

ПЗУ - постоянное запоминающее устройство;

НСД - несанкционированный доступ;

ФД - фискальные данные;

ФП - фискальная память;

ППП - пакеты прикладных программ;

ЯЗ - ядро защиты.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Установленные термины обязательны для применения во всех видах документации по защите информации. Для каждого понятия установлен один термин. Применение синонимов термина не допускается. Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Контрольно-кассовая машина (ККМ) - устройство, предназначенное для автоматизации и механизации учета, контроля и первичной обработки информации кассовых операций и регистрации ее на печатаемых документах в соответствии с принятыми нормативными и правовыми документами.

Автоматизированная кассовая система (АКС) - система, состоящая из персонала и ККМ на основе средств вычислительной техники, реализующая технологию обработки информации кассовых операций.

Фискальные данные (ФД) - информация о денежных расчетах с населением, проведенных на ККМ, необходимая для правильного исчисления налогов и контроля со стороны налоговых органов, подлежащая ежесуточной (ежесменной) регистрации и долговременному хранению.

Фискальные функции (операции с ФД):

формирование и накопление ФД в суточных (сменных) счетчиках и регистрах с оформлением и печатью финансовых документов;

запись (регистрация) ФД в фискальную память с оформлением и печатью финансовых документов;

хранение ФД в фискальной памяти;

чтение ФД из фискальной памяти с оформлением и печатью документов.

Фискальная память ККМ (ФП) - комплекс программно-аппаратных средств в составе ККМ, обеспечивающий некорректируемую, ежесуточную (ежесменную) регистрацию и энергонезависимое долговременное хранение итоговой информации о денежных расчетах с населением, проведенных на ККМ, необходимой для правильного исчисления налогов.

Защита фискальных данных - предотвращение несанкционированного доступа к ФД с целью их корректировки (умышленного искажения), модификации или уничтожения вследствие неисправности технических средств, ошибки программного обеспечения, преднамеренных и непреднамеренных действий человека.

Пакеты прикладных программ (ППП) - комплекс прикладных программ ККМ, предназначенный для решения взаимоувязанных задач реализации фискальных функций.

Системные данные - параметры системы, используемые при загрузке и определяющие конфигурацию средств вычислительной техники.

Фискализация - включение фискального режима ККМ.

Ядро защиты (ЯЗ) - технические, программные и микропрограммные элементы комплекса средств защиты фискальных данных, реализующие функцию управления доступом к фискальной памяти.

2. КЛАССИФИКАЦИЯ ККМ

2.1. Классификация распространяется на все действующие и проектируемые ККМ зарубежного и отечественного производства.

2.2. Деление контрольно-кассовых машин и средств вычислительной техники, входящих в состав АКС на соответствующие группы по их конструктивным и функциональным особенностям с точки зрения защиты информации, подлежащей контролю налоговыми органами, проводится

для выработки и применения обоснованных мер по достижению требуемого уровня защищенности фискальных данных.

2.3. Дифференциация подходов к выбору методов, средств защиты и принципов построения ядра защиты определяется различием контрольно-кассовых машин по своему составу, функциональным и конструктивным особенностям, способам хранения фискальных данных.

2.4. Устанавливаются две группы ККМ, согласно которым к ККМ предъявляются требования по защите информации, хранимой в ФП. Каждая группа характеризуется определенной совокупностью требований по защите информации.

2.5. Первая группа ККМ включает устройства, имеющие закрытую архитектуру.

Признаки закрытой архитектуры:

наличие программного обеспечения, находящегося в ПЗУ и его исполнение путем прямого считывания команд из ПЗУ;

невозможность выполнения прикладного программного обеспечения, находящегося во внешней памяти.

2.6. Вторая группа ККМ включает устройства, имеющие открытую архитектуру.

Признаки открытой архитектуры:

наличие устройства, выполненного на базе универсальных средств вычислительной техники;

прикладное программное обеспечение в виде ППП загружается в оперативную память;

наличие стандартных интерфейсов ввода/вывода с возможностью подключения периферийных устройств;

модульное конструктивное исполнение.

2.7. В пределах каждой группы ККМ классифицируются по масштабам возможных материальных потерь вследствие уклонения от налогообложения. К первому классу относятся устройства, использование

которых связано с обработкой информации о денежных оборотах на сумму до 700 минимальных размеров оплаты труда в сутки, а ко второму классу – устройства, связанные с обработкой информации о денежных оборотах на сумму свыше 700 минимальных размеров оплаты труда в сутки.

3. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ХРАНИМОЙ В ФИСКАЛЬНОЙ ПАМЯТИ, ОТ НСД

3.1. ФП должна исключать возможность потери информации за счет физического старения носителя фискальных данных в период их хранения или под влиянием окружающей среды (световых и электромагнитных излучений, температуры и пр.) в соответствии с техническими требованиями, оговоренными в действующих нормативных документах, регламентирующих вопросы эксплуатации, хранения и транспортировки ККМ.

3.2. В качестве ФП запрещается использовать:

устройства, информация в которых сохраняется менее 6 лет с момента фискализации ККМ;

микросхемы памяти, требующие электро-, термо- тренировки для записи информации;

устройства, требующие технического обслуживания в период хранения фискальных данных;

устройства, допускающие стирание информации под воздействием внешних источников (ультрафиолетового излучения, электрических сигналов и т.п.).

3.3. ФП не должна иметь прямой электрической связи с системной магистралью процессора обработки данных.

3.4. Адреса ФП не должны находится в области адресного пространства процессора обработки данных ККМ.

3.5. Комплекс средств защиты ФП должен обеспечивать:

защиту фискальных данных от сбоев по питанию;

защиту фискальных данных от несанкционированного изменения;

защиту от стирания (очистки) фискальных данных;

защиту от использования очищенной ФП без предварительной инициализации;

защиту от несанкционированной замены ФП;

защиту от несанкционированного отключения фискального режима;

контроль правильности записи в ФП фискальных данных;

сравнение даты записи фискальных данных с датой предыдущей записи в ФП и блокировку записи в случае, если дата осуществляемой записи более ранняя, чем дата предыдущей записи;

контроль целостности всех фискальных данных, содержащихся в ФП, при записи суточного (сменного) итога в ФП;

контроль правильности читаемых фискальных данных при снятии отчета ФП и выдачу сообщения при чтении (печати) испорченных фискальных данных.

3.6. Средства защиты должны обеспечивать следующие блокировки:

блокировку всех операций кроме чтения ФП, при обнаружении испорченных фискальных данных в ФП;

блокировку попыток изменения местоположения десятичной точки до операции перерегистрации;

блокировку всех операций кроме чтения ФП, при переполнении ФП;

блокировку всех операций при неисправности ФП;

блокировку всех операций при отсутствии ФП;

блокировку попыток подбора пароля доступа к фискальным данным;

блокировку попыток выполнения любых действий с ФП до записи заводского номера;

блокировку повторной записи заводского номера;

блокировку попыток выполнения любых действий с ФП, кроме чтения и записи заводского номера, до проведения фискализации;

блокировку попыток выполнения более 4-х перерегистраций;

блокировку попыток выполнения любых действий с использованием пароля доступа к ФП, до записи суточного (сменного) итога в ФП.

3.7. Программы управления работой ФП должны быть защищены от изменения.

4. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ В ККМ И АКС

4.1. Средства защиты ККМ первой группы устройств должны обеспечивать:

защиту системных данных от сбоев по питанию;

защиту от несанкционированной замены или изменения программного обеспечения в ПЗУ ККМ*;*

защиту фискальных данных от НСД не ниже 6 класса защищенности для ККМ 1 класса и не ниже 5 класса защищенности для ККМ 2 класса (согласно РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»).

4.2. Средства защиты ККМ второй группы устройств должны обеспечивать:

запись и хранение системных данных в энергонезависимой памяти;

защиту системных данных от сбоев по питанию;

защиту системных данных от несанкционированного изменения;

защиту от загрузки операционной системы с внешнего устройства;

защиту от замены или изменения незагружаемого программного обеспечения;

защиту от замены или изменения загружаемого программного обеспечения;

блокировку попыток записи двух суточных (сменных) итогов подряд, без промежуточного оформления платежных документов;

защиту фискальных данных от НСД не ниже 5 класса защищенности для ККМ 1 класса и не ниже 4 класса защищенности для ККМ 2 класса (согласно РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»);

защиту фискальных данных от НСД не ниже класса защищенности 1Г для ККМ 1 класса, объединенных в АКС и не ниже класса защищенности 1В для ККМ 2 класса, объединенных в АКС (согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»).

5. ПОРЯДОК ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ ККМ и АКС

5.1. Сертификация ККМ, АКС и ППП для ККМ и АКС по требованиям защиты информации производится в соответствии с требованиями «Положения о сертификации средств защиты информации по требованиям безопасности информации», «Типовыми методиками сертификации ППП по требованиям безопасности информации», «Типовыми методиками проведения сертификационных испытаний средств защиты от НСД к информации в ККМ и АКС».

5.2. Сертификация ККМ и АКС отечественного производства производится с последующей аттестацией производства по выпуску сертифицированной продукции и выдачей сертификационной лицензии на право применения знака соответствия.

5.3. Сертификация партии устройств производится по репрезентативной выборке из партии с последующей выдачей сертификата на всю партию. Действие сертификата соответствия распространяется на аналогичные устройства последующих партий при условии проведения дополнительной проверки выборки из последующих партий.

5.4. Сертификация единичных образцов ККМ и АКС проводится по схеме испытаний единичного образца с последующей выдачей сертификата на единичный образец с указанием заводского номера (уникального кода идентификации).