СОГЛАСОВАНО
Первый заместитель начальника Центра защиты информации и спец. связи ФНС России
_____ / Кузьмин А.С. /
«___» _____ 20___ г.

УТВЕРЖДАЮ
Заместитель руководителя ФНС России
_____ / Потрунин /
«___» _____ 20___ г.

Федеральная налоговая служба Российской Федерации

Модель угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных

от 06.07.2015 № ЧГ-7006/ИБ/3/2/2-1045

Начальник отдела ИБ УИТ ФНС России
_____ / Соловьев /
«___» _____ 20___ г.

СОГЛАСОВАНО
И.о. начальника УИТ ФНС России
_____ / Юрьев /
«___» _____ 20___ г.

Москва 2015

Содержание

1. Общие положения

1.1 Назначение Модели угроз

Применение контрольно-кассовой техники с передачей данных, техническая эффективность которой была подтверждена в эксперименте по применению контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт, обеспечивающей передачу налоговым органам в электронном виде информации о таких расчетах, на территории Республики Татарстан, Калужской области, Московской области и г. Москвы с 1 августа 2014 г. до 1 февраля 2015 г., открывает ряд качественно новых возможностей для снижения нагрузки на бизнес, повышения качества и эффективности контрольной работы налоговых органов, собираемости налогов, сбора статистики и анализа макроэкономических показателей.

Настоящая Модель угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных (далее по тексту – Модель угроз) предназначена для постановки задач и разработки требований по информационной безопасности фискальных данных (ФД), технических средств обработки фискальных данных, прежде всего контрольно-кассовой техники (ККТ), автоматизированных систем, обеспечивающих электронную регистрацию ККТ, сбор фискальных данных и взаимодействие с информационными ресурсами налоговых органов.

1.2 Правовые и методические основы Модели угроз

Настоящая Модель угроз разработана на основе требований действующей Концепции информационной безопасности Федеральной налоговой службы Российской Федерации [1], учитывает и развивает требования действующего на период разработки Модели угроз законодательства [2], подзаконных актов [3,4], методических документов ФСБ России [5,6,7,8], ФСТЭК России [9,10,11,12] и ряда

других отечественных и зарубежных методических, научно-технических и научно-исследовательских документов, полный перечень которых приведен в Приложении 1 «Источники разработки».

1.3 Цели разработки Модели угроз

Разработка настоящей Модели угроз выполнена с целями, установленными в Концепции ИБ ФНС России [1] для разработки требований по информационной безопасности и защите информации применительно к ФД, программно-техническим средствам их обработки (включая ККТ и средства обеспечения некорректируемой регистрации ФД), автоматизированным системам, обеспечивающим сбор, обработку и хранение ФД, электронную регистрацию ККТ. В соответствии с [1], основными целями разработки Модели угроз являются:

- Глубокое изучение состава объектов защиты, угроз информационной безопасности, возможностей нарушителей ИБ ФД.
- Определение уровня защищенности информационных систем налоговых органов и Оператора фискальных данных (ОФД), а также состав функций (механизмов) информационной безопасности, которые должны обеспечить компенсацию угроз (обработку риска) информационной безопасности ФД, программно-технических средств и автоматизированных систем их обработки.
- Оценка эффективности предлагаемых средств (мер, механизмов) информационной безопасности ФД, технических средств и автоматизированных систем их обработки.

В то же время, во избежание дублирования тезисов Концепции информационной безопасности ФНС России [1], в настоящей Модели угроз не рассматриваются вопросы, исчерпывающе проработанные в [1], а именно:

- Общие аспекты информации, как объекта права и защиты.

– Субъекты отношений, в том числе государство и государственные органы, не имеющие прямого касательства к процессам создания и обработки фискальных данных.

– Структура информационных ресурсов ФНС России, не связанных с процессами создания и обработки фискальных данных.

– Естественные природные и атипичные (присущие любым информационным ресурсам и любым автоматизированным системам) угрозы информационной безопасности.

– Общие архитектурные и организационные вопросы построения системы обеспечения информационной безопасности.

1.4 Объекты защиты

Объектами защиты, к которым адресована настоящая Модель угроз, являются:

– Фискальные данные во всех возможных их представлениях на всех этапах их жизненного цикла.

– Средства формирования фискальных данных – контрольно-кассовая техника, средства обеспечения некорректируемой регистрации фискальных данных.

– Автоматизированные системы сбора, обработки и хранения фискальных данных.

– Автоматизированные системы, обеспечивающие жизненный цикл средств обработки фискальных данных (осуществление электронной регистрации ККТ).

Развернутая характеристика перечисленных объектов защиты приводится ниже в соответствующих разделах Модели угроз.

1.5 Структура Модели угроз

Общие сведения об объектах защиты, практика обработки фискальных данных, обзор практик нарушения информационной

безопасности фискальных данных изложены в разделе «2. Базовая модель угроз безопасности фискальных данных».

Далее Модель угроз структурирована применительно к составу объектов защиты, описанному в предыдущем разделе:

- Модель угроз для ККТ (Раздел «3. Модель угроз средств обработки фискальных данных. Контрольно-кассовая техника»).
- Модель угроз для фискальных данных (Раздел «4. Модель угроз информационной безопасности фискальных данных, фиксируемых контрольно-кассовой техникой и переданных оператору фискальных данных»).
- Модели угроз для автоматизированных систем электронной регистрации ККТ (АС ЭР ККТ) и сбора фискальных данных (АС ОФД) (Рразделы «5. Модель угроз средств обработки фискальных данных. Автоматизированная система электронной регистрации контрольно-кассовой техники» и «6. Модель угроз средств обработки фискальных данных. Автоматизированная система Оператора фискальных данных»), соответственно.

Затем приводится описание угроз информационной безопасности применительно к каждому из видов объектов защиты детализировано до уровня атак и характеристик атак, реализующих эти угрозы (раздел «7. Анализ угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных»).

Для решения задачи выработки рекомендаций по выбору и применению средств защиты общая классификация средств защиты приведена в разделе «8.1 Описание мер противодействия угрозам ИБ ФД, ККТ, АС ЭР ККТ, АС ОФД».

Оценка эффективности мер защиты и оценка остаточных рисков применительно к рассматриваемому комплексу угроз производится в разделе «8. Анализ мер противодействия угрозам информационной безопасности фискальных данных, средств и систем обработки фискальных данных».

Раздел «8.2 Заключение об эффективности мер защиты фискальных данных, средств и систем обработки фискальных данных» содержит резюме по результатам анализа, выполненного при разработке Модели угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных.

1.6 Понятия и определения

Кассовый чек	- первичный учетный документ, отпечатанный на бумажном носителе или сформированный в виде электронного документа, выданный пользователем ККТ покупателю и подтверждающий факт осуществления наличного денежного расчета и (или) расчета с использованием платежных карт между пользователем и покупателем, содержащий установленный перечень сведений об этих расчетах.
Контрольно-кассовая техника	- контрольно-кассовые машины, оснащенные фискальной памятью, электронно-вычислительные машины, в том числе персональные, программно-технические комплексы [2].
Корпус	- аппаратное средство, без вскрытия или разрушения которого исключается возможность изменения или замены программно-аппаратных средств, содержащихся внутри него.
Марка-пломба	- защищенная от подделки полиграфическая продукция, позволяющая выявить факт вскрытия корпуса контрольно-кассовой техники.
Модель контрольно-	– контрольно-кассовая техника, имеющая индивидуальное наименование, присвоенное

кассовой техники	поставщиком.
Исправность	- соответствие экземпляра контрольно-кассовой техники, в том числе входящих в ее состав частей, техническим характеристикам и параметрам функционирования модели одобренного типа.
Техническая поддержка	- работы и услуги по вводу в эксплуатацию, проверке исправности, ремонту, техническому обслуживанию и выводу из эксплуатации контрольно-кассовой техники, замене программно-аппаратных средств, в том числе фискальной памяти, а также передаче налоговым органам сведений о контрольно-кассовой технике и введению в нее установленного перечня сведений при регистрации, перерегистрации и снятии с регистрации в налоговых органах.
Фискальные данные	- сведения о наличных денежных расчетах и (или) расчетах с использованием платежных карт, защищенные при помощи фискального признака.
Фискальная память	- комплекс программно-аппаратных средств в составе контрольно-кассовой техники, обеспечивающих некорректируемую ежесуточную (ежесменную) регистрацию и энергонезависимое долговременное хранение итоговой информации, необходимой для полного учета наличных денежных расчетов и (или) расчетов с использованием платежных карт, осуществляемых с применением контрольно-кассовой техники, в целях правильного исчисления налогов; [2].
Фискальный признак	- информация, сформированная с использованием средств формирования

фискального признака и ключа фискального признака, в результате криптографического преобразования установленного перечня сведений о контрольно-кассовой технике, о пользователе, о наличных денежных расчетах и (или) расчетах с использованием платежных карт, обеспечивающая возможность гарантированного выявления корректировки или фальсификации этих сведений.

1.7 Список аббревиатур

ИБ	Информационная безопасность.
ИР	Информационный ресурс.
ККТ	Контрольно-кассовая техника.
ЛВС	Локальная вычислительная сеть.
МФП	Модуль фискальной памяти.
НДВ	Недекларированные возможности.
НСД	Несанкционированный доступ.
ОР	Оператор регистрации.
ОФД	Оператор фискальных данных.
ПО	Программное обеспечение.
СЗИ	Средство защиты информации.
СКЗИ	Средство криптографической защиты информации.
СКЗФД	Средство криптографической защиты фискальных данных.
ФД	Фискальные данные.
ФП	Фискальный признак.
ФР	Фискальный регистратор.
ЭКЛЗ	Электронная контрольная лента защищенная.

2. Базовая модель угроз безопасности фискальных данных

2.1 Определение условий создания и использования фискальных данных

2.1.1 Описание форм представления фискальных данных

Фискальные данные формируются и фиксируются ККТ в ходе выполнения расчетных операций.

Фискальные данные в ККТ могут фиксироваться в следующих документах:

- кассовый чек;
- чек возврата платежей;
- контрольная лента;
- отчеты о содержимом фискальной памяти и применении ККТ, включая сменные.

Указанные документыимеют следующую структуру:

- Заголовок документа, который, содержит данные, позволяющие идентифицировать пользователя ККТ, ККТ и документ, а также определить дату и время формирования документа.
- Сведения о расчетах, которые могут включать, в том числе наименование товара, работ и услуг, по которым производился расчет, их количество и цену.
- Резюме документа, которое может включать сумму, полученную от покупателя (клиента), сумму товаров, работ и услуг, предоставленных покупателю (клиенту), сумму сдачи, выданной покупателю (клиенту), размеры скидок, виды и ставки налогов, а также в обязательном порядке фискальный признак документа.

Также фискальные данные фиксируются в следующих документах, на электронных носителях информации, в массивах и базах данных:

– В модулях фискальной памяти (фискальных накопителях).

– В документах бухгалтерского учета у пользователя ККТ.

– В документах и базах данных налоговых органов.

– В базах данных оператора фискальных данных.

При этом первичным источником фискальных данных является ККТ.

2.1.2 Описание информации, сопутствующей процессам создания и использования фискальных данных в ККТ

В процессе формирования, фиксации, проверки и обработки, фискальных данных используются следующие данные:

– Сведения о налогоплательщике, использующем ККТ.

– Сведения о ККТ, формирующей фискальные данные (документы).

– Сведения о товарах, ценах, суммах расчетов с использованием ККТ.

– Сведения о времени осуществления расчетов с использованием ККТ.

– Сведения о количестве покупателей (клиентов), с которыми осуществлялись расчеты, в том числе, о последовательности выдачи им кассовых чеков.

– Сведения о количестве наличных денежных средств, имеющихся у лица (кассира) в процессе осуществления наличных денежных расчетов с использованием ККТ.

В процессе создания, обработки, хранения и обеспечения информационной безопасности фискальных данных в ККТ используются:

– Средства контроля доступа к ККТ лиц, осуществляющих применение ККТ от имени налогоплательщика, в том числе информация, позволяющая их аутентифицировать, аппаратные средства для их аутентификации, включая электронные и механические ключи от ККТ для кассиров и администраторов.

– Средства идентификации ККТ, в том числе информация о ней, зафиксированная в ее паспорте и иной эксплуатационной документации, нанесенная на корпус ККТ, а также зафиксированная на ее электронных носителях.

– Средства идентификации программно-аппаратных средств, обеспечивающих некорректируемую регистрацию фискальных данных в ККТ, в том числе информация о ее программно-аппаратных средствах, зафиксированная в их паспортах, в паспорте ККТ и иной эксплуатационной документации ККТ, нанесенная на их корпус, а также зафиксированная на их электронных носителях.

– Средства идентификации иных программных и программно-аппаратных средств ККТ, в том числе информация о них, зафиксированная в их паспортах, в паспорте ККТ и иной эксплуатационной документации ККТ, а также зафиксированная на электронных носителях ККТ.

В соответствии с классификацией, введенной Федеральным законом [2], контрольно-кассовая техника классифицируется, как три класса технических средств, оснащенных фискальной памятью (рис. 1):

– Контрольно-кассовые машины.

– Электронно-вычислительные машины, в том числе персональные.

– Программно-технические комплексы.

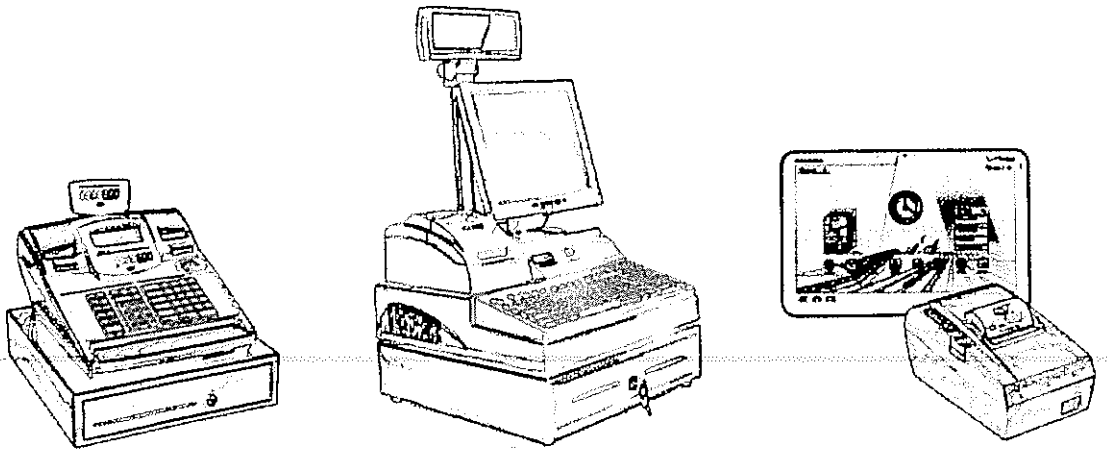

Рис. 1.

Вне зависимости от класса, ККТ состоит из следующих основных элементов:

- Информационный терминал ККТ (ИТ ККТ, POS). Имеет клавиатуру для формирования информации о расчетах, а также программно-аппаратные средства для ее обработки, предоставления на экране или дисплее кассиру и покупателю, передачи данных в модуль фискальной памяти и на принтер для печати кассового чека. Может размещаться в одном или нескольких корпусах. В программно-техническом комплексе в качестве информационного терминала может применяться мобильное устройство (смартфон, планшет), снабженное модулем фискальной памяти (данный модуль может быть встроен в фискальный регистратор, входящий в состав программно-технического комплекса).
- Принтер, имеющий программно-аппаратные средства для печати фискальных данных на бумаге в виде кассовых чеков и отчетов, а также программно-аппаратные средства для получения этих данных из информационного терминала. Может иметь свой корпус, в котором должен размещается модуль фискальной памяти. Принтер с корпусом и модулем фискальной памяти принято именовать фискальным регистратором.
- Модуль фискальной памяти (фискальный накопитель), включающий в свой состав комплекс программно-аппаратных средств, выполняющий функции фискальной памяти в соответствии с Федеральным законом [2]. Имеет свой корпус, ограничивающий доступ к его программно-аппаратным средствам и размещается только либо в фискальном регистраторе, либо в корпусе ККТ, содержащем принтер.

В соответствии с Федеральным законом [2] ККТ должна обеспечивать реализацию следующих процессов:

- Процесс проверки исправности ККТ и ее опломбирования для обеспечения защиты от несанкционированного доступа к программно-аппаратным средствам ККТ.

– Процесс регистрации исправной ККТ в налоговых органах, включая ввод в нее сведений о налогоплательщике, применяющем ККТ, и о регистрации ККТ в налоговом органе, а также перевод ККТ в фискальный режим в присутствии должностного лица налогового органа, завершающийся печатью первого кассового чека.

– Процесс ввода сведений о расчетах, формирования и обработки фискальных данных, включая их регистрацию в некорректируемом виде и долговременное хранение в накопителе фискальной памяти (модуле фискальной памяти).

– Процесс печати документов, содержащих фискальные данные, в том числе кассовых чеков, контрольных лент и отчетов.

Новый порядок применения контрольно-кассовой техники, предусматривает реализацию дополнительных процессов:

– Процесса электронной регистрации ККТ.

– Процесса передачи фискальных данных в электронном виде в налоговые органы.

2.1.3 Источник фискальных данных

С учётом [3], субъектом обработки фискальных данных является лицо, применяющее ККТ при осуществлении наличных денежных расчётов и (или) расчётов с использованием платёжных карт с покупателем (клиентом) при продаже товаров, выполнении работ или оказании услуг, получившее карточку регистрации ККТ.

2.1.4 Описание этапов жизненного цикла ККТ, влияющих на состояние информационной безопасности фискальных данных

Жизненный цикл ККТ включает следующие этапы:

– Разработка (проектирование) модели ККТ и ее программно-аппаратных средств, в том числе модуля фискальной памяти.

– Оценка соответствия разработанной модели ККТ и ее программно-аппаратных средств, в том числе модуля фискальной памяти, установленным требованиям.

- Производство ККТ и ее программно-аппаратных средств, в том числе модуля фискальной памяти.
- Реализация ККТ ее пользователю (налогоплательщику).
- Ввод ККТ в эксплуатацию, включая проверку ее исправности, опломбирование, перевод ККТ в фискальный режим.
- Регистрация (перерегистрация) ККТ в налоговых органах.
- Эксплуатация ККТ.
- Ремонт и техническое обслуживание ККТ, включая замену ее программно-аппаратных средств, в том числе модуля фискальной памяти.
- Снятие ККТ с регистрации в налоговых органах и утилизация ККТ.

Ввиду того, что в основе нарушения информационной безопасности фискальных данных очень часто лежит нарушение целостности программно-аппаратных средств ККТ (см. Дополнительно раздел «Обзор практик нарушений информационной безопасности фискальных данных»), важнейшей из задач информационной безопасности фискальных данных является обеспечение целостности ККТ и юридически доказуемого определения лица, виновного в нарушении целостности ККТ.

Нарушение целостности ККТ может иметь место на каждом из перечисленных выше этапов жизненного цикла ККТ. В то же время методы компенсации угроз информационной безопасности ККТ на различных этапах жизненного цикла ККТ различны. Поэтому в настоящей Модели угроз анализ угроз ведется там, где требуется учесть специфику отдельного этапа, в контексте отдельных этапов жизненного цикла ККТ. Производство контрольно-кассовой техники, в соответствии с действующим законодательством [2,3,4], является объектом технического регулирования. Объективная необходимость такого регулирования (формирование требований к ККТ, проверка соответствия требований к ККТ применительно к моделям, включаемым в реестр ККТ) сохраняется и в новом порядке применения

контрольно-кассовой техники. Однако для упрощения процедур технического обслуживания ККТ и снижения нагрузки на бизнес новый порядок применения предусматривает электронную регистрацию ККТ.

Для ККТ, включаемой в реестр, установлены технические требования, включающие, наряду с функциональными, требования безопасности. Проектирование ККТ должно осуществляться с учетом этих требований.

Вновь разработанная модель ККТ включается в реестр и допускается на рынок (к регистрации в налоговых органах) в случае, если она прошла оценку соответствия установленным требованиям.

Производство ККТ должно базироваться на использовании документации одобренных моделей ККТ. Производитель не имеет права модернизировать модель одобренного типа. По мере изготовления продукции на корпус ККТ должна наноситься саморазрушающаяся марка-пломба, препятствующая вскрытию корпуса ККТ и нарушению целостности ее программно-аппаратных составляющих.

Этап регистрации ККТ в установленном порядке начитается с подачи Налогоплательщиком заявления о регистрации в налоговые органы. Регистрация ККТ может осуществляться вручную, с предъявлением ККТ налогоплательщиком в налоговые органы или в результате автоматизированной процедуры, называемой электронной регистрацией ККТ.

На этапе электронной регистрации выполняются следующие операции:

- Проверка сведений об одобрении типа (модели) ККТ и ее модуля фискальной памяти, а также их наличия в реестре.
- Проверка целостности ККТ.
- Ввод и некорректируемая регистрация в модуле фискальной памяти сведений об образце ККТ и Налогоплательщике.

– Проверка целостности и исправности ККТ.

– Формирование нулевого кассового чека (отчета о фискализации ККТ) и проверка по нему целостности и исправности ККТ.

– Формирование учетных записей в системе регистрации налоговых органов и карточки регистрации ККТ.

Этап регистрации ККТ завершается переводом ККТ в фискальный режим и выдачей Налогоплательщику юридически значимого документа – карточки регистрации ККТ.

ФД при эксплуатации ККТ формируются, регистрируются в некорректируемом виде в модуле фискальной памяти, проверяются в ходе контрольной работы налоговых органов и, в новом порядке применения ККТ, передаются в налоговые органы в электронном виде при поддержке Оператора фискальных данных.

2.1.5 Функциональные элементы, выполняющие операции обработки фискальных данных

Обобщенная схема взаимодействия участников процесса создания и обработки фискальных данных представлена на рис. 2.

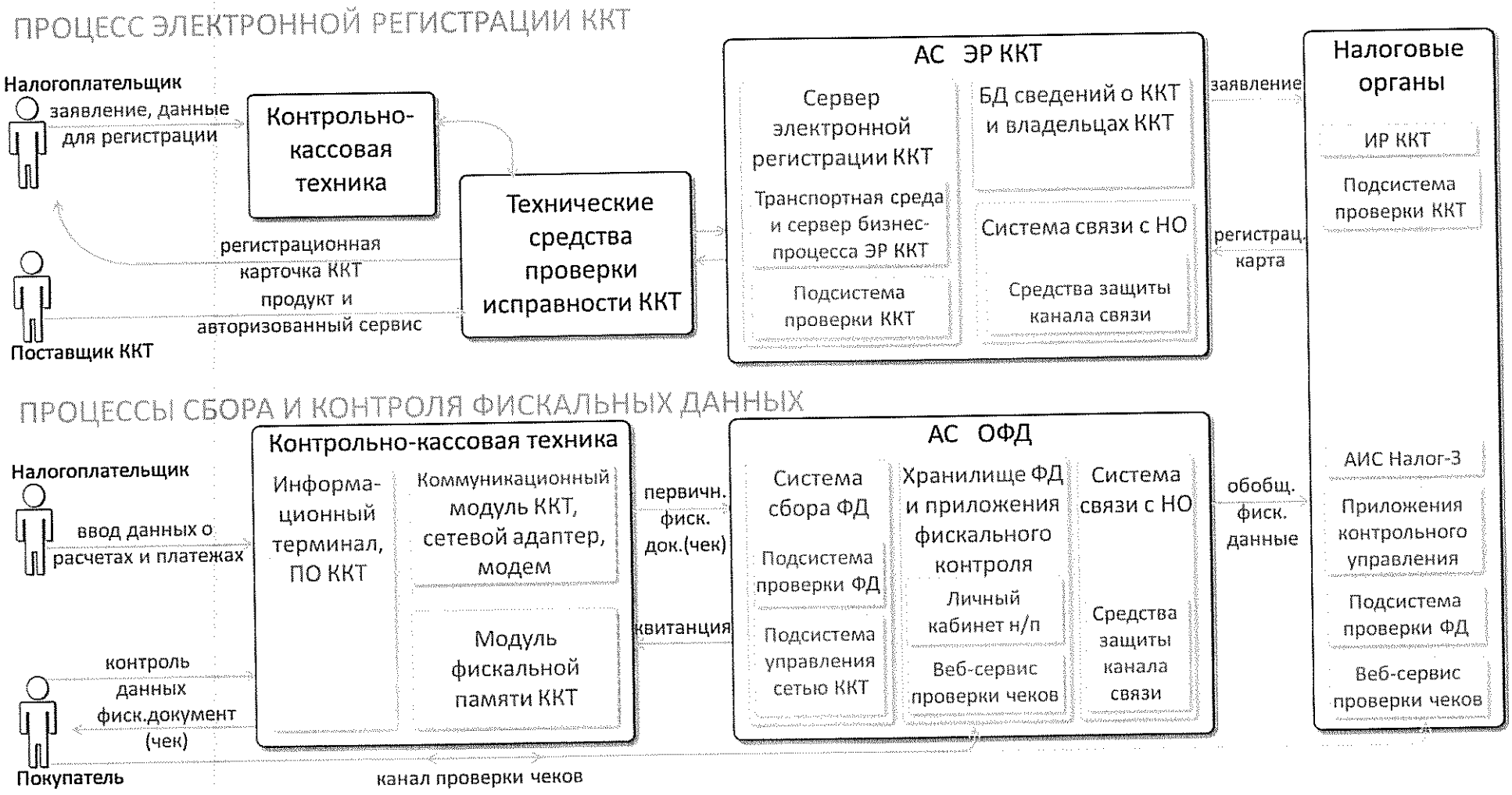
ПРОЦЕСС ЭЛЕКТРОННОЙ РЕГИСТРАЦИИ ККТ
Налогоплательщик
заявление, данные для регистрации
Контрольно-кассовая техника
Технические средства проверки исправности ККТ
регистрационная карточка ККТ
продукт и авторизованный сервис
Поставщик ККТ
АС ЭР ККТ
Сервер электронной регистрации ККТ
БД сведений о ККТ и владельцах ККТ
Транспортная среда и сервер бизнес-процесса ЭР ККТ
Система связи с НО
Подсистема проверки ККТ
Средства защиты канала связи
заявление
регистрац. карта
Налоговые органы
ИР ККТ
Подсистема проверки ККТ
ПРОЦЕССЫ СБОРА И КОНТРОЛЯ ФИСКАЛЬНЫХ ДАННЫХ
Налогоплательщик
ввод данных о расчетах и платежах
Контрольно-кассовая техника
Информа-ционный терминал, ПО ККТ
Коммуникационный модуль ККТ, сетевой адаптер, модем
Модуль фискальной памяти ККТ
первичн. фиск. док.(чек)
квитанция
АС ОФД
Система сбора ФД
Подсистема проверки ФД
Подсистема управления сетью ККТ
Хранилище ФД и приложения фискального контроля
Личный кабинет н/п
Веб-сервис проверки чеков
Система связи с НО
Средства защиты канала связи
обобщ. фиск. данные
АИС Налог-3
Приложения контрольного управления
Подсистема проверки ФД
Веб-сервис проверки чеков
контроль данных фиск.документ (чек)
Покупатель
канал проверки чеков

Рис. 2

С точки зрения информационной безопасности ФД, средств и систем обработки ФД, значение имеют:

- Собственно ФД в формате различных фискальных документов, а также в машинном представлении при их создании, обработке и хранении в составе ККТ и автоматизированных систем.
- Контрольно-кассовая техника всех типов.
- Автоматизированная система электронной регистрации ККТ.
- Автоматизированная система сбора и контроля фискальных данных.

Контрольно-кассовая техника.

Функционально технические средства ККТ включают информационный терминал и/или программный модуль, формирующий исходные данные для создания первичного фискального документа (кассового чека), модуль фискальной памяти и коммуникационный модуль.

Основное требование к информационному терминалу (программному модулю формирования исходных данных) – создавать достоверные исходные данные и не допускать избирательности (исключения из обработки) части сформированных данных.

Модуль фискальной памяти отвечает за некорректируемую регистрацию данных о расчетах и за создание фискального признака для фискального документа .

Коммуникационный модуль ККТ отвечает за передачу информации в налоговые органы с соблюдением требований информационной безопасности. При этом коммуникационный модуль ККТ может быть выполнен в виде отдельного устройства или интегрирован с модулем фискальной памяти.

Поставщик контрольно-кассовой техники должен обеспечивать сервис проверки исправности (программной и аппаратной целостности) ККТ, который может обеспечивать поддержку функции электронной регистрации ККТ.

Автоматизированная система электронной регистрации ККТ (АС ЭР ККТ на рис. 2).

Сервер электронной регистрации ККТ должен выполнять функции автоматизации процесса регистрации (прием заявления налогоплательщика о регистрации ККТ и его аутентификацию, проверку исправности ККТ, проверки сведений о ККТ, формирования запроса в налоговые органы, получения от налоговых органов карты регистрации ККТ в электронном виде, проверку перевода ККТ в фискальный режим, выдачи карты регистрации контрольно-кассовой техники в электронном виде) пользователю ККТ.

Существенными с точки зрения информационной безопасности фискальных данных элементами этого сервера являются:

- Транспортная среда, обеспечивающая защищенное от посторонних воздействий соединение с ККТ на местах и аутентификацию (авторизацию) операторов, выполняющих технологические операции по регистрации ККТ.
- Подсистема проверки исправности ККТ, подтверждающая при помощи технических средств поставщика ККТ исправность (в т.ч. аппаратную и программную целостность ККТ и ее способность формировать корректный фискальный признак).

База данных о ККТ и владельцах ККТ содержит сведения о моделях ККТ одобренного типа, технические параметры для проверки их исправности, сведения о парке зарегистрированной ККТ и о налогоплательщиках, владеющих этой техникой, учетные данные поэкземплярного учета средств криптографической защиты в составе ККТ и ККТ, в которую установлены эти средства.

В состав АС ЭР ККТ должна также входить защищённая система связи с налоговыми органами.

Автоматизированная система Оператора фискальных данных (АС ОФД, рис. 2).

В состав АС ОФД должен входить функциональный модуль (система) сбора фискальных данных. Функции безопасности, которые должны выполнять ее подсистемы, это:

- Проверка целостности (подлинности) фискальных данных (документов). Эта проверка должна производиться с использованием тех же криптографических механизмов, которые применялись в модулях фискальной памяти ККТ при формировании фискальных признаков.
- Управление системой сбора информации (включая управление средствами защиты связи с ККТ, формирование сеансовых ключей, мониторинг и диагностику состояния каналов связи).

Кроме системы сбора фискальных данных в составе АС ОФД должно находиться хранилище собранных фискальных данных. Функция безопасности этого элемента – хранение фискальных данных в некорректируемом виде с возможностью их использованияя налоговыми органами в соответствии с действующим законодательством.

Система связи с налоговыми органами в составе АС ОФД должна выполнять те же функции, что и в составе АС ЭР ККТ.

Личные кабинеты налогоплательщиков могут выполнять функции дополнительных услуг для граждан (вопросы обоснования и безопасности такого рода дополнительных услуг в настоящей Модели угроз не рассматриваются). Веб-услуги проверки чеков должны обеспечивать гражданам возможность проверки подлинности выданных им чеков.

2.2 Процесс разработки и производства ККТ и модулей фискальной памяти

Производство ККТ выполняется в следующем порядке:

1. Поставщик ККТ и/или поставщик модуля фискальной памяти (МФП) разрабатывает и сертифицирует модель МФП ККТ в

соответствии с установленным порядком разработки шифровальных (криптографических) средств [5].

2. Разработанная модель МФП ККТ включается ФСБ России в перечень сертифицированных средств криптографической защиты.
3. Модули фискальной памяти в установленном для СКЗИ порядке поэкземплярно регистрируются поставщиком МФП ККТ.
4. Поставщик ККТ получает МФП и встраивает их в модель ККТ, в установленном порядке производит тематические исследования ККТ на предмет отсутствия негативных влияний программно-аппаратных средств разработанной модели ККТ на МФП.
5. При положительном результате тематических исследований ККТ Поставщик ККТ включает сведения о разработанной модели ККТ в реестр ККТ.
6. Поставщик ККТ производит ККТ, осуществляет их поэкземплярный учет, в том числе указывая номера МФП, установленных в ККТ.

Описанный процесс выполняется единым порядком для ККТ типов «контрольно-кассовая машина», «ЭВМ, в т.ч. персональная» и «программно-технический комплекс». При этом для ККТ типа «программно-технический комплекс» в качестве объекта разработки и тематического исследования выступает программное обеспечение, выполняющее функции обработки фискальных данных (ПО ККТ) и взаимодействия с модулем фискальной памяти. Разработчик ПО ККТ выполняет роль поставщика ККТ. В качестве «модели ККТ» принимается версия этого программного обеспечения, в качестве «заводского номера ККТ» принимается уникальный номер лицензии программного обеспечения. Предметом тематического исследования является данное программное обеспечение, программный интерфейс взаимодействия ПО ККТ с МФП, операционная среда (платформа), в которой работает ПО ККТ.

2.3 Процесс технической поддержки ККТ

Для технической поддержки поставщик ККТ использует сеть технической поддержки из уполномоченных представителей поставщика ККТ.

Представители поставщика ККТ выполняют все операции по технической поддержке ККТ на местах эксплуатации, включая:

- Техническую поддержку регистрации (перерегистрации, снятия с регистрации) ККТ.
- Замену накопителей (модулей) фискальной памяти.
- Сервисное обслуживание, ремонт – в установленном порядке, включающем, по завершении ремонта, проверку исправности ККТ и установку средств защиты корпуса ККТ.

В процессе технической поддержки для ККТ типа «программно-технический комплекс» в качестве объекта технического обслуживания выступает ПО ККТ. Аппаратная часть программно-технического комплекса может ремонтироваться и обслуживаться у ее производителя с соблюдением требований соответствия аппаратной платформы заявленным характеристикам. Прошивка ПО ККТ и проверка целостности программной среды при этом лежат в области ответственности представителя поставщика ККТ (ПО ККТ).

2.4 Источники угроз информационной безопасности фискальных данных

2.4.1 Мотивация непосредственных нарушителей безопасности фискальных данных

Первичные фискальные данные, как объект атаки представляют прямой интерес для следующих субъектов:

1. Для налогоплательщика, заинтересованного в сокрытии части выручки, фактически полученной от покупателей (клиентов) в ходе расчетных операций и от налоговых органов с целью уклонения от уплаты налогов.

2. Для сотрудника налогоплательщика, заинтересованного в сокрытии от налогоплательщика части выручки, фактически полученной им в ходе расчетных операций, для присвоения им этой части выручки.
3. Для внешнего нарушителя, заинтересованного в несанкционированном доступе к информации, путем перехвата фискальных данных, коммерческой тайны продавца, коммерческой или личной тайны покупателя, дискредитации налогоплательщика перед покупателями, контрагентами, налоговыми органами, дискредитации поставщика ККТ перед его потенциальными покупателями.

2.4.2 Вторичные мотивы и вторичные субъекты налоговых правонарушений

Доминирующий мотив нарушений информационной безопасности первичных фискальных данных, представленный в российском (и в мировом) обществе в массовом порядке - налоговое правонарушение – создает среди потенциальных нарушителей спрос на технические средства поддержки налогового правонарушения. Этот спрос удовлетворяется тремя социальными группами вторичных нарушителей безопасности фискальных данных или пособников налогового правонарушения:

1. Недобросовестный производитель ККТ и ПО для ККТ, который позиционирует уязвимость системы защиты ККТ, как «конкурентное преимущество» своей продукции. Такой производитель либо прямо размещает в ККТ свою закладку, либо закладывает в конструкции ККТ возможность для применения закладки, поставляемой в дальнейшем.
2. Производитель закладки для ККТ. При этом закладка может исполняться в виде программного или программно-аппаратного модуля, устанавливаемого в ККТ в дополнение к ее программным или программно-аппаратным средствам, либо вместо ее штатных программных или программно-аппаратных средств, в том числе в

виде контрафактного процессора ККТ или контрафактного модуля фискальной памяти, в виде несанкционированной модификации ПО ККТ.

3. Недобросовестный сотрудник службы технического обслуживания ККТ, производящий незаконную модернизацию ККТ или бездействующий при выявлении незаконной модернизации ККТ.

2.4.3 Обзор практик нарушений информационной безопасности фискальных данных

Для уточнения постановки задачи в модели угроз верхнего уровня приведем краткий обзор практик нарушения информационной безопасности фискальных данных в соответствии с результатами научно-исследовательской работы [14].

Правоприменительная практика показывает, что невыдача кассового чека (в том числе пробитие чека на меньшую сумму или пустого чека) — одно из самых массовых нарушений в торговле.

При этом невыдача чека относительно редко применяется в явном виде – при полном отсутствии ККТ в предприятии торговли. Чаще налоговое правонарушение осуществляется «…с использованием чекопечатающих устройств, не соответствующих требованиям Закона №54-ФЗ к ККТ, в частности: не включенных в Государственный реестр ККТ, не зарегистрированных в налоговых органах, не использующих в своем составе фискальную память, не обеспечивающих печать кассовых чеков, содержащих некорректируемые данные о проведенных денежных расчетах».

«Значительное количество налоговых мошенничеств производится путем нетехнических манипуляций с кассами в нарушение требований по их эксплуатации, особенно использование «второй» («черной», «установленной под столом») кассы. Установка «второй» кассы заключается в том, что основная регистрационная нагрузка возлагается на незаконно установленное незарегистрированное кассовое устройство. Покупатели получают распечатанные этим устройством фальшивые чеки с достоверным

внешним видом и содержанием. Далее учет по этим чекам не производится, а вся налоговая выручка со «второй» кассы уводится из-под налогообложения. Зарегистрированная касса при этом также используется, однако только с целью изображения видимости легитимной торговли для органов налогового контроля.».

«… большей популярностью пользуется «скручивание» памяти ККТ «умельцами», работающими в специализированных мастерских. По различной информации, «скрутка» обычно стоит 15–20% от выведенной из-под налогов суммы».

«Возможные действия злоумышленников с целью искажения (занижения) денежных сумм, регистрируемых в ФП ККТ, выполнимы при получении доступа к программно-аппаратным средствам ККТ, который может быть осуществлен:

– Либо путем нарушения целостности корпуса ККТ.

– Либо без её нарушения.

Доступ к программно-аппаратным средствам ККТ при нарушении целостности корпуса ККТ может достигаться:

– Путем снятия марки-пломбы (с последующей установкой прежней марки-пломбы, снятой с применением неразрушающего метода, либо поддельной марки-пломбы).

– Либо без снятия марки-пломбы путем проникновения к элементам программно-аппаратных средств ККТ через незащищенные (или недостаточно защищенные) технологические отверстия в корпусе ККТ, либо через специально создаваемые отверстия в корпусе ККТ с последующей их «маскировкой»».

«… действия злоумышленников с целью искажения (занижения) денежных сумм, регистрируемых в ФП [фискальной памяти] ККТ … могут быть направлены на подмену [штатных] программных, аппаратных и программно-аппаратных средств ККТ … на программные, аппаратные и программно-аппаратные средства, позволяющие нарушать режим функционирования ККТ,

обеспечивающий некорректируемую регистрацию информации о проведенных платежах…».

В качестве средств взлома применяются «Программно-аппаратные средства, имитирующие функционирование штатных средств ККТ, но позволяющие при записи в постоянный накопитель ФП ККТ (ПНФП) данных об итоговых денежных суммах, зарегистрированных в ККТ в течение смены (или суток), корректировать (занижать) эти данные.

Такими средствами могут быть эмуляторы ЭКЛЗ и различные микросхемы.

Эмуляторы используют для формирования фискального признака (КПК), печатаемого на кассовом чеке, генератор случайных чисел, при этом значение КПК формируется случайным образом. Такие эмуляторы имеют полное сходство внешнего вида, атрибутов, указанных на корпусе, и регистрационных номеров с реально существующими ЭКЛЗ».

«Организационные и технические способы противодействия реализации мер обеспечения полноты учета выручки в целях налогообложения, как правило, взаимосвязаны и их классификацию можно привести совместно, выделив по объединяющим их признакам:

1) применение ККТ, не соответствующей:

- Образцам, представленным при внесении сведений о модели ККТ в Государственный реестр;
- Требованиям, определяемым Правительством РФ, в том числе: отсутствие на ККТ средства визуального контроля; отсутствие на ККТ марки-пломбы или повреждении марки-пломбы; отсутствие заключенного договора с центром технического обслуживания; отсутствие на кассовом чеке обязательных реквизитов (ИНН юридического лица или предпринимателя, наименования организации и др.); несоответствие времени проведения платежа, указанного на кассовом чеке, фактическому времени;

– Требованию по применению ККТ, обеспечивающей надлежащий учет денежных средств при проведении расчетов, в том числе использование чекопечатающих устройств, не соответствующих требованиям ФЗ-54 к ККТ, в частности: не включенных в Государственный реестр ККТ, не зарегистрированных в налоговых органах, не использующих в своем составе фискальную память, не обеспечивающих печать кассовых чеков, содержащих некорректируемые данные о проведенных денежных расчетах. Данный способ может быть реализован в двух видах:

– Злоумышленник для проведения денежных расчетов с клиентами использует только указанное устройство;

– Злоумышленник для проведения денежных расчетов с клиентами наряду с указанным устройством использует в ряде случаев ККТ, соответствующую установленным требованиям, с целью подтверждения информации об объемах выручки, предъявляемой в налоговые органы (использование «второй», «черной», «установленной под столом» ККТ);

– Требованию по применению исправной ККТ;

2) фактическое неиспользование контрольно-кассового аппарата, в том числе:

– Физическое отсутствие ККТ;

– Применение контрольно-кассовой техники не в составе платежного терминала, а в составе используемой системы приема платежей, в том числе когда:

– Клиентам выдается квитанция о проведенном платеже, однако сам платеж в ККТ не регистрируется (и подлинный кассовый чек не распечатывается), а в квитанции печатается фальшивый (недостоверный) фискальный признак (КПК);

– Клиентам разных ПТ, осуществляющих в течение одного дня оплату однотипных услуг на одинаковую сумму, выдаются квитанции, содержащие копии реквизитов кассового чека о зарегистрированном

в ККТ платеже за аналогичные услуги и на такую же сумму, но в указанных квитанциях указывается место осуществления платежа в соответствии с реальным местом расположения ПТ. В этом случае количество незарегистрированных в ККТ платежей будет в прямой зависимости от количества ПТ в сети;

- Злоумышленник может воспользоваться возникающими возможностями в связи с фальсификацией документов, оформляемых в случае отказа клиента от услуги по приему платежа через ПТ. Учитывая, что подлинные кассовые чеки клиентам не выдаются, а остаются у злоумышленника, последний может оформить возврат кассовых чеков от клиентов и возврат клиентам внесенных ими денежных средств при проведенной ими оплате услуг через ПТ;

3) невыдача кассового чека, в том числе:

- Неполучение кассового чека покупателем: в том числе передача кассового чека не в руки, а размещение его рядом с ККТ либо в какой-либо емкости или в ином месте, что создает предпосылки для неполучения кассового чека покупателем; выдача квитанции, похожей на кассовый чек с фальшивым фискальным признаком; выдача покупателю использованных чеков;
- Пробитие недостоверного кассового чека, в т.ч. чека на меньшую сумму, не с фактическим временем и с иными недостоверными данными;
- Пробитие пустого кассового чека;
- Невыдача части кассового чека;

4) несанкционированное вмешательство в работу программного обеспечения контрольно-кассовой техники («скрутка данных»):

А) по способам осуществления:

- Путем снятия марки-пломбы:

– Несанкционированной (с последующей установкой прежней марки-пломбы, снятой с применением неразрушающего метода, либо поддельной марки-пломбы);

– Санкционированной при осуществлении сервисного обслуживания;

– Без снятия марки-пломбы путем проникновения к элементам программно-аппаратных средств ККТ ещё на этапе производства ККТ (в том числе внесение в Государственный реестр ККТ моделей, в которых штатные программно-аппаратные средства позволяют реализовывать недекларируемые функции) либо через незащищенные (или недостаточно защищенные) технологические отверстия в корпусе ККТ, либо через специально создаваемые отверстия в корпусе ККТ с последующей их «маскировкой»;

Б) по функциональным особенностям:

– Программно-аппаратные средства, имитирующие функционирование штатных средств ККТ, но позволяющие при записи в постоянный накопитель ФП ККТ (ПНФП) данных об итоговых денежных суммах, зарегистрированных в ККТ в течение смены (или суток), корректировать (занижать) эти данные, в частности:

– Эмуляторы ЭКЛЗ, которые внешне практически идентичны легальным средствам и используют для формирования фискального признака (КПК), печатаемого на кассовом чеке, генератор случайных чисел, при этом значение КПК формируется случайным образом;

– Микросхемы, выполняющие функции управляющих устройств в ККТ (процессоры управления), отличающиеся от штатных микросхем ККТ по функциональным возможностям, но имеющие маркировку, совпадающую с маркировкой штатных микросхем <...>

– Программа, позволяющая злоумышленнику отключить применение ЭКЛЗ в начале смены;

– Программа, позволяющая злоумышленнику отключить применение ЭКЛЗ в ККТ в конце смены;

– Программные средства - специальные компьютерные программы, устанавливаемые в штатные аппаратные средства ККТ вместо штатного (эталонного) программного обеспечения и предназначенные для постоянного или кратковременного исключения ЭКЛЗ из процесса регистрации в ККТ денежных платежей;

5) невыдача бланков строгой отчетности либо выдача БСО, несоответствующих установленным требованиям».

Таким образом:

1. В настоящее время, при отсутствии удаленного доступа к программно-аппаратным средствам ККТ, доминирующим мотивом нарушения безопасности фискальных данных является замысел на налоговое правонарушение. Инициатива нарушения безопасности при этом принадлежит налогоплательщику.
2. Значительная часть налоговых правонарушений осуществляется нетехническими методами. Прежде всего – это невыдача чека покупателю и/или выдача чекового суррогата, не выдерживающего проверки.
3. Возможность нарушения безопасности фискальных данных с использованием нетехнических махинаций не дает оснований для признания этого способа махинаций основным и пренебрежения угрозы совершения махинаций с использованием технических средств, а также противодействия этим угрозам с использованием технических средств защиты фискальных данных.
4. Следует признать, что техническое обеспечение нарушений информационной безопасности фискальных данных весьма развито, изобретательно, изощренно и составляет отдельный, сформировавшийся и вполне объемный рынок продукции и услуг, предназначенных для технического обеспечения налоговых правонарушений.

5. Фокус технической атаки при этом направлен на целостность потока фискальных данных. Простым, эффективным и одновременно технически наиболее сложно детектируемым способом уклонения от налогообложения является изъятие части первичных фискальных документов из оборота – невыдача чека по факту его формирования или отложенное формирование чеков и «переучет» выручки с изъятием части выручки из обращения, например, по результатам смены или истечения срока давности привлечения к административной ответственности за выдачу недостоверного кассового чека.
6. Вторым по распространенности видом атаки является нарушение целостности непосредственно фискального документа. Это - выдача правдоподобно выглядящего, иногда даже – дающего положительный результат проверки КПК чека (путем, например, дублирования чеков или фальсификации данных на входе системы фискальной регистрации). Эта атака, как правило, реализуется путем нарушения целостности ККТ, которая, будучи проверенной, включенной в реестр контрольно-кассовой техники, правильно зарегистрированной и эксплуатируемой, должна противостоять такого рода атакам.
7. Далее, наряду с нарушением целостности фискальных документов (путем, возможно, сопутствующего нарушения целостности ККТ), широчайшим образом применяется нарушение систем идентификации и аутентификации ККТ. К распространенным атакам данного вида относится нарушение системы аутентификации, позволяющее осуществить клонирование ККТ («вторая касса», «черная касса», «касса под столом»), когда один зарегистрированный образец ККТ, несущий умеренную нагрузку по выручке, «прикрывает» собой один или несколько образцов ККТ, выдающих неучтенные фискальные документы и скрывающих свою выручку от налогообложения. Нарушения идентификации ККТ выполняются путем регистрации ККТ на некоторую фирму-однодневку (не платящую и не собирающуюся никогда платить

налоги) и подстановка этой кассы в торговый зал другой, фактически выполняющей продажи, организации. Как определенный класс мошенничеств с нарушением аутентификации следует выделить также выдачу фискальных документов от имени другой организации, вполне легитимной, зарегистрированной и платящей налоги (мошенничество «перекладывание налогов на соседа»).

8. Важнейшим объектом атаки и соответственно, важным объектом защиты фискальных данных являются часы ККТ. Время выдачи фискального документа фальсифицируется в ряде атак, связанных как с целостностью фискальных данных (например, путем «переучета» и сокрытия части чеков при отложенной фискальной регистрации выручки), в мошенничествах с многократным оборотом однажды выданного легитимного чека, а также атак, связанных с идентификацией и аутентификацией ККТ, когда мошенник выдает свои чеки «под прикрытием» ранее выданных другой, легитимной организацией, чеков.

9. Далее, потенциально значительный ущерб взиманию налогов наносит оборот неучтенных копий, клонов и повторно используемых средств регистрации фискальных данных и ключевых документов. По данной зоне мошенничеств отсутствует собранная до конца и доведенная до следственного результата и судебного взыскания практика. Однако о таких нарушениях убедительно свидетельствуют два факта: появление чеков с «правильным» КПК, выдаваемых вне налогового учета клонами зарегистрированной техники и существенный дисбаланс между числом официально проданных и фактически эксплуатируемых образцов нелегитимных (несертифицированных ФСБ России) средств защиты фискальных данных. Хотя инициатором и исполнителем налогового правонарушения в данном случае, как и ранее, является недобросовестный налогоплательщик, данное нарушение, как и вывод на рынок ряда уязвимостей ККТ и

закладок в ККТ, выполняется при активном содействии недобросовестного производителя ККТ и недобросовестных производителей нелегитимных средств регистрации фискальных данных и ключевых документов. В налоговое правонарушение при этом вовлекаются, как правило, и операторы «серого» рынка контрафактной ККТ, а также производители средств взлома ККТ.

2.4.4 Вновь появляющиеся угрозы информационной безопасности фискальных данных

Перечисленные в предыдущем разделе условия и обстоятельства совершения налоговых правонарушений относятся к более чем десятилетнему историческому периоду эксплуатации автономной контрольно-кассовой техники с применением в качестве средства защиты криптографического модуля фискальной памяти ЭКЛЗ.

На сегодня этот опыт требует переосмысления в связи с появлением новых технологий и изменениями структуры рынка.

2.4.5 Сетевая информационная безопасность ККТ

Применение техники с передачей данных создает ряд принципиально новых угроз информационной безопасности фискальных данных. Контрольно-кассовая техника подключается к сетям передачи данных общего пользования и, в этом отношении, подвергается всем тем сетевым угрозам, которым подвержены подключенные к сети Интернет компьютеры.

2.5 Модель угроз верхнего уровня

Обобщенный (для формирования модели угроз верхнего уровня) состав угроз для перечисленных в предыдущем разделе практик нарушений безопасности ФД выглядит следующим образом:

1. Эксплуатация недобросовестным налогоплательщиком уязвимостей, недокументированных возможностей ККТ, в т.ч. закладок

производителя (атаки на целостность фискальных данных при их создании и обработке).

2. Внедрение недобросовестным налогоплательщиком или лицами, находящимися в сговоре с ним, закладок в ККТ. Несанкционированная модернизация, разрушение, порча, нарушение целостности ККТ, установка контрафактного МФП, закладки, несанкционированная «перепрошивка» ПО кассы (атаки на целостность фискальных данных при их создании и обработке).
3. Нарушение недобросовестным налогоплательщиком или лицами, находящимися в сговоре с ним, маркировки, системы идентификации ККТ (в т.ч. электронной), подмена ККТ, клонирование ККТ, средств регистрации фискальных данных и ключевых документов (атаки на целостность фискальных данных при их создании и обработке или манипуляции с несанкционированными образцами ККТ).
4. Блокирование недобросовестным налогоплательщиком или лицами, находящимися в сговоре с ним, или третьими лицами, фискальных данных (в т.ч. при их передаче Оператору фискальных данных или в налоговые органы).
5. Нарушение недобросовестным налогоплательщиком или лицами, находящимися в сговоре с ним, или третьими лицами, целостности фискальных данных при их передаче Оператору фискальных данных или в налоговые органы (атаки перехвата, искажения, издания от чужого имени фискальных данных).
6. Нарушение третьими лицами конфиденциальности фискальных данных при их передаче Оператору фискальных данных или в налоговые органы (перехват, разглашение коммерческой тайны владельца ККТ).
7. Нарушение недобросовестным налогоплательщиком или лицами, находящимися в сговоре с ним, или третьими лицами, целостности первичных фискальных документов при их использовании и

обработке в электронном виде (искажение, фальсификация юридически значимого документа).

2.6 Модель нарушителя информационной безопасности фискальных данных технических средств и автоматизированных систем обработки фискальных данных

2.6.1 Классификация нарушителей информационной безопасности

В соответствии классификацией нарушителя, принятой компетентными федеральными органами исполнительной власти в сфере обеспечения информационной безопасности, в частности, [8], в настоящем документе принята классификация нарушителей по признаку прав доступа к информации:

- Н1 –нарушитель, не имеющий доступа в зону эксплуатации[1] ККТ, где расположены ФД и средства их обработки;
- Н2 – нарушитель, имеющий физический доступ к средствам (системам) обработки ФД, но не имеющий прав пользователя этих средств (систем).
- Н3 – нарушитель, имеющий права пользователя средств (систем) обработки фискальных данных, но не имеющий прав администрирования и конфигурирования этих средств (систем).

К пользователям средств (систем) обработки ФД с более высокими правами доступа (администраторам систем, аудиторам органов фискального контроля) в настоящей Модели угроз постулируется доверие и требования по защите от нарушителей этих классов не устанавливаются.

---

[1] Термин «зона эксплуатации ККТ» используется как синоним общепринятого в литературе по информационной безопасности понятия «контролируемая зона». Необходимость применения нового термина была вызвана тем, что торговая точка, в которой эксплуатируется ККТ, в большинстве случаев открыта для публичного доступа. Однако в любой торговой точке всегда существуют организационные и технические ограничения на прямой физический доступ покупателя к контрольно-кассовой технике. Область действия этих ограничений именуется по тексту Модели угроз «зоной эксплуатации ККТ».

Возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi (0 < i <4).

2.6.2 H1: нарушитель, не имеющий доступа к системам обработки фискальных данных

В классе H1, с точки зрения атаки на фискальные данные, значимостью обладают две группы нарушителей:

- Производители ККТ, встраивающие технические закладки в свои продукты. Производители закладок. Злоумышленники из числа сотрудников системы технического обслуживания ККТ. Эту группу нарушителей далее по тексту именуется H1z.
- Хакеры, пытающиеся получить несанкционированный доступ к ФД, ККТ или другим системам обработки ФД по сети. Эту группу нарушителей далее по тексту именуется H1i.

Мотивы нарушения.

Нарушитель H1z мотивирован корыстными интересами, не связанными непосредственно с компрометацией фискальных данных, но связанных с коммерческой прибылью, получаемой им от встраивания в ККТ закладки. При этом производитель ККТ получает такую прибыль косвенно, путем стимулирования сбыта своей контрольно-кассовой техники заинтересованным в проведении налоговых мошенничеств покупателям, а производитель закладок продает их тому же контингенту как самостоятельный товар. Следует отметить, что мотивы для самостоятельной атаки на системы обработки фискальных данных у нарушителя H1z отсутствуют, за исключением случаев необходимости поиска уязвимостей в системах обеспечения информационной безопасности фискальных данных для совершенствования закладок и способов их встраивания в ККТ.

Нарушитель H1i может быть мотивирован любыми, как корыстными, так и бескорыстными, вандальными или хакерскими, интересами.

Знания о системе защиты фискальных данных.

Нарушители H1z обладают всей полнотой знаний о ККТ в достаточном объеме для реализации атак.

Нарушители H1i могут обладать достаточными и практически полными знаниями об отдельных образцах ККТ.

Технические средства реализации угроз.

Технические средства реализации угроз у нарушителя H1z представлены в виде производимых им закладок.

Нарушитель H1i вооружен средствами для осуществления сетевых атак (средства перехвата трафика на отдельных звеньях его передачи, средствами разведки топологии сети и сканирования портов, анализаторами протоколов и т.п.). Кроме того, в распоряжении нарушителя H1i могут находиться средства для проведения примитивного криптоанализа на ограниченных вычислительных мощностях.

2.6.3 H2: субъект в зоне эксплуатации ККТ

Мотивы нарушения.

Субъект H2, допущенный в зону эксплуатации ККТ, но не имеющий прав доступа к ФД, может физически атаковать ККТ, руководствоваться мотивами хулиганства, вандализма, компрометации кассира или пользователя ККТ. Наличие у нарушителя H2 мотивов атаки на фискальные данные менее вероятно. Однако такой мотив нельзя исключить полностью, поскольку нарушитель H2 может действовать в сговоре или по поручению лица, заинтересованного в совершении налогового правонарушения или в провокации, имитирующей налоговое правонарушение. В этом случае можно ожидать от нарушителя H2 установки закладки в ККТ и попытки ее использования.

Знания о системе защиты фискальных данных.

В среднем – невысоки. Но целесообразно предположить, что технические знания нарушителя H2 равны знаниям нарушителя H1z и H1i.

Технические средства реализации угроз.

Нарушитель Н2 может владеть механическими и электронными инструментами, а также закладками для компрометации ФД.

2.6.4 Н3: нарушитель с правами пользователя ККТ

Мотивы нарушения.

Корыстные мотивы, замысел на налоговое мошенничество, связанное с компрометацией фискальных данных.

В ряде случаев нарушитель класса Н3 (владелец ККТ) вступает в сговор с сотрудником служб технического обслуживания ККТ. Права доступа нарушителя Н3 при этом значительно не увеличиваются, однако существенно расширяются технические возможности для осуществления атаки. Такого нарушителя по тексту будем обозначать индексом Н3s.

Знания о системе защиты фискальных данных.

Предполагается, что нарушитель Н3 обладает:

- Знаниями нарушителя Н2.
- Отдельными фрагментами знаний о ККТ и системе обработки фискальных данных, в частности:
- Сведениями об идентификаторах некоторых легитимных пользователей.
- Сведениями об используемых в системе приложениях и об инфраструктуре системы (IP-адреса, порты, версии операционных систем серверов и в ПО).
- Знаниями об уязвимостях используемой ККТ, вычислительной техники и сетевого оборудования.

В определенных обстоятельствах нарушитель Н3 может действовать в сговоре с нарушителем Н1z, а также нарушителем Н1i или привлекать их к соучастию в организации атаки на ККТ.

Технические средства реализации угроз.

Следует предполагать, что нарушитель Н3 располагает:

- Программными и программно-аппаратными закладками для компрометации фискальных данных.
- Возможностью делать попытки применения имеющихся программных и программно-аппаратных закладок.
- Возможностями перехвата и модификации трафика в локальной сети.
- Техническими средствами для эксплуатации уязвимостей ККТ и автоматизированной системы обработки фискальных данных. Возможностью делать попытки эксплуатации уязвимостей ККТ и автоматизированной системы обработки фискальных данных.

3. Модель угроз средств обработки фискальных данных. Контрольно-кассовая техника

3.1 Состав угроз целостности контрольно-кассовой техники на этапах ее проектирования, одобрения типа и производства

На этапах проектирования, одобрения типа ККТ и производства ККТ могут реализоваться следующие виды угроз:

1. Ошибка проектирования, приводящая к появлению уязвимости ККТ.
2. Разработка третьим лицом (нарушитель H1z) специализированного для применения в данной модели ККИ средства атаки на первичные фискальные данные (аппаратной или программной закладки).
3. Установка закладки в процессе производства, хранения, транспортировки ККТ (путем модернизации аппаратной части ККТ, ПО ККТ или того и другого). Данная атака может производиться недобросовестным разработчиком, недобросовестным сотрудником производителя ККТ, третьим лицом, участвующим в процессе складского хранения или поставки готовой продукции ККТ.

3.2 Состав угроз контрольно-кассовой технике на этапе регистрации (перерегистрации) ККТ

На этапах регистрации или перерегистрации ККТ могут реализоваться следующие угрозы информационной безопасности первичных фискальных данных:

1. Установка закладки в процессе приобретения, ввода в эксплуатацию, перевода ККТ в фискальный режим. Разновидностью данной атаки является блокирование средств криптографической защиты фискальных данных в составе ККТ и установка имитатора СКЗФД, некорректно выполняющего функции защиты первичных фискальных данных, либо нелегитимного СКЗФД, заведомо имеющего дубликаты или клоны, позволяющие имитировать применение СКЗФД и не

осуществлять регистрацию, передачу и долговременное хранение фискальных данных.

2. Регистрация в качестве ККТ техники, не прошедшей одобрение типа.
3. Нарушение правил проверки целостности и исправности ККТ при регистрации ККТ. (В частности, применение неаттестованного оборудования для регистрации ККТ, не производящего полную проверку целостности, неустановка или ненадлежащая установка марки-пломбы и т.п.).

Целями этой группы атак могут являться мошенничества по схемам «вторая касса», «платеж в однодневку» и подобных. Данные атаки могут производиться недобросовестным налогоплательщиком, возможно – с привлечением технического специалиста или в сговоре с недобросовестным сотрудником службы технической поддержки продукции ККТ.

3.3 Угрозы целостности ККТ и отдельных элементов ККТ на этапе эксплуатации ККТ

Угрозы целостности ККТ могут быть адресованы к устройству ККТ в целом, а также к отдельным его элементам. При этом риски в этой группе угроз не исчерпываются стоимостью ККТ или отдельного элемента ККТ. Нарушение целостности ККТ практически всегда имеет целью приобретение нарушителем возможности для атаки на фискальные данные с целью уклонения от налогообложения в размерах, существенно превышающих стоимость ККТ и ее отдельных элементов. Таким образом, величина риска в этой группе угроз определяется не ценностью кассы или отдельного ее модуля, а уровнем ущерба, который может быть нанесен налоговым сборам при помощи скомпрометированного устройства ККТ.

Угрозы целостности ККТ могут быть реализованы посредством следующего набора атак:

1. Нарушение целостности программно-аппаратных средств ККТ (размещение программной или аппаратной закладки, нарушение целостности штатного ПО).
2. Нарушение целостности модуля фискальной памяти ККТ. Нарушение средств идентификации МФП ККТ. Клонирование/компрометация модуля фискальной памяти ККТ.
3. Применение в составе ККТ контрафактных модулей фискальной памяти.
4. Клонирование ККТ. Применение, наряду с легально зарегистрированной, «теневой» контрольно-кассовой техники, на которую выводится регистрация скрываемой от налогообложения выручки.

3.4 Сетевые угрозы целостности ККТ

Нарушение целостности программного обеспечения ККТ может осуществляться путем атак из открытых сетей передачи данных. Целостности ККТ могут угрожать:

1. Поиск уязвимостей ККТ методами сетевого доступа и/или эксплуатация известных уязвимостей ККТ по отношению к сетевым атакам. Захват прав доступа администратора и модернизация прошивки (установка закладки) в ККТ.
2. Атаки на ККТ, выполняемые путем распространения опасного мобильного кода (вирусопоражение, установка spyware и т.п.) из открытых сетей общего пользования и ЛВС налогоплательщика.
3. Перехват каналов сетевого управления (конфигурирования) ККТ. Нарушение конфигурации ККТ.

4. Модель угроз информационной безопасности фискальных данных, фиксируемых контрольно-кассовой техникой и переданных оператору фискальных данных

4.1 Состав угроз ИБ ФД на этапе эксплуатации ККТ

Состав угроз информационной безопасности первичных фискальных данных и средств обработки фискальных данных показан на рис. 3.

Рис. 3

4.1.1 Угрозы целостности фискальных данных при вводе первичной информации и выдаче распечатки фискального документа

Угрозы целостности фискальных данных при вводе первичной информации и выдаче распечатки фискального документа в соответствии с результатами исследования [14], представляют собой группу угроз, которую на сегодняшний день реализует подавляющее большинство налоговых злоумышленников.

Защита от этих угроз реализуется, преимущественно, следующими методами:

- Проверка полноты учета выручки в ККТ, отсутствие возможности провести платежную операцию и корректно сформировать все реквизиты кассового чека без обращения к фискальной памяти. Эта проверка особенно актуальна для ККТ из класса «программно-технический комплекс».
- Контроль безопасности контрольно-кассовой техники на этапах одобрения ее типа, регистрации в налоговых органах и перевода ККТ в фискальный режим. Ведение Государственного реестра контрольно-кассовой техники, допущенной к выполнению платежных операций и обработке фискальных данных.
- Периодически осуществляемый контроль за эксплуатацией контрольно-кассовой техники, плановые и внеплановые проверки налогоплательщиков.
- Предоставление покупателю канала проверки подлинности фискальных данных. Оперативное расследование сигналов покупателей о невыдаче фискальных документов или выдаче фальшивых фискальных документов.

4.1.2 Угрозы фискальным данным в процессе их формирования и обработки

В процессе создания, обработки, передачи первичные фискальные данные могут подвергаться следующим атакам:

1. Манипуляции с чеками при их создании (блокирование регистрации ФД и невыдача чека, дублирование чеков или подмена номера/идентификатора чека).
2. Фальсификация содержания чека (блокирование учета части данных при формировании фискального документа, нарушение целостности фискальных данных путем изъятия или фальсификации части товарных позиций, путем фальсификации данных о владельце ККТ или регистрационных атрибутов ККТ).
3. Фальсификация фискального признака чека.
4. Отложенное формирование или ревизия отчетности с изъятием полного состава (или части) фискальных данных.
5. Фальсификация электронного фискального документа (в случае, если фискальные документы предполагается формировать в электронном виде).

4.1.3 Сетевые угрозы информационной безопасности фискальных данных

В процессе создания, обработки, передачи первичные фискальные данные могут подвергаться следующим атакам из сетей передачи данных:

1. Любое нарушение целостности фискальных данных произвольным нарушителем из сети.
2. Изъятие из потока (блокировка) или нарушение целостности фискальных данных недобросовестным налогоплательщиком на этапе их передачи от ККТ к ОФД.
3. Перехват (нарушение конфиденциальности) фискальных данных на этапе их передачи от ККТ к ОФД.
4. Атаки на систему аутентификации участников сетевого взаимодействия. Атака с посредником. Имперсонация ККТ.
5. Подавление сетевой активности ККТ (атака «отказ в обслуживании», направленная на кассу).

5. Модель угроз средств обработки фискальных данных. Автоматизированная система электронной регистрации контрольно-кассовой техники

5.1 Порядок выполнения электронной регистрации контрольно-кассовой техники

При разработке модели угроз информационной безопасности технических средств и автоматизированных систем, выполняющих государственную услугу электронной регистрации контрольно-кассовой техники, были приняты во внимание процедуры, представленные в разделах 47-91 действующего Административного регламента регистрации ККТ [15]. При этом общий состав и последовательность операций, выполняемых в ходе государственной услуги, остаются без изменений.

В случае исполнения процедуры электронной регистрации ККТ в ходе электронного взаимодействия удаленных сторон требуются следующие меры (по перечню процедур из Административного регламента [15]):

а) Прием и регистрация заявления и прилагаемых документов.

Требуется удостовериться, что заявление и пакет документов подает именно тот налогоплательщик, от имени которого выполняется операция.

б) Рассмотрение заявления и документов, прилагаемых к заявлению.

Требуется проверка подлинности заявления и прилагаемых документов. Эту проверку можно провести на шаге (б) процедуры регистрации, однако, в случае применения средств автоматизации, целесообразно, во избежание избыточных операций и затрат, провести проверку подлинности документов при их приемке на шаге (а).

Поскольку процедура приема и регистрации заявления о регистрации ККТ и прилагаемых документов завершается проставлением штампа территориального налогового органа с

указанием даты регистрации и заверения его подписью специалиста территориального налогового органа, ответственного за прием документов, на этапе электронной приемки документов целесообразно предусмотреть транзакцию в направлении от налоговых органов к налогоплательщику, подтверждающую прием документов.

в) Осмотр контрольно-кассовой техники.

Осмотр контрольно-кассовой техники преследует цели проверки:

- соответствия образца ККТ модели одобренного типа, включенной в Государственный реестр контрольно-кассовой техники;
- регистрационных знаков и заводских номеров;
- целостности корпуса ККТ;
- исправности ККТ.

Для выполнения в дистанционном режиме проверок подлинности заводских номеров ККТ целесообразно предусмотреть процедуру предварительной регистрации заводских номеров выпускаемой продукции контрольно-кассовой техники.

Процедура ввода регистрационных данных в ККТ должна выполняться в защищенном режиме и исключать возможность их фальсификации. Эта операция должна выполняться либо как защищенная транзакция между Оператором регистрации и ККТ, либо контролироваться уполномоченным ответственным специалистом Оператора регистрации.

Часть перечисленных целей (проверка исправности ККТ) может быть выполнена дистанционно при наличии соответствующей поддержки (поставки технических средств проверки исправности) со стороны поставщика ККТ, в то время как другая, не поддающаяся автоматизации часть операций, прежде всего – проверка модели ККТ и осмотр средств защиты корпуса ККТ, должна выполняться ответственным сотрудником технической поддержки.

г) Регистрация контрольно-кассовой техники с одновременной выдачей заявителю карточки регистрации.

Регистрация контрольно-кассовой техники должна производиться на основании положительного результате проверок, выполняемых на шаге (в). Результаты проверок, выполняемых в дистанционном режиме, должны оформляться в виде электронных документов, заверенных электронной подписью уполномоченного специалиста (представителя поставщика ККТ и/иди Оператора регистрации), выполнившего операцию регистрации.

Перевод ККТ в фискальный режим и разблокировка функции контрольно-кассовой техники по учету платежных операций должны выполняться на финальном этапе регистрации ККТ или по завершении этого этапа.

Карточка регистрации, выдаваемая налогоплательщику в виде электронного документа, должна снабжаться электронной подписью уполномоченного специалиста налоговых органов.

д) Перерегистрация контрольно-кассовой техники с выдачей заявителю карточки регистрации.

Перерегистрация контрольно-кассовой техники должна производиться с выполнением основных требований, изложенных в разделе (г).

е) Снятие с регистрации контрольно-кассовой техники.

Снятие контрольно-кассовой техники с регистрации должно производиться с выполнением основных требований, изложенных в разделе (г) с тем дополнением, что ККТ должна выводиться из фискального режима и должны предприниматься меры для блокировки функции регистрации сведений о платежах и расчетах при помощи снятой с регистрации контрольно-кассовой техники. Меры блокировки снятой с регистрации техники целесообразно выполнять как на стороне ККТ, так и у Оператора регистрации, Оператора фискальных данных и в составе информационных ресурсов налоговых органов.

ж) Уведомление заявителя об отказе в предоставлении государственной услуги.

Уведомление заявителя об отказе в регистрации контрольно-кассовой техники должно быть обосновано. Основания для отказа в регистрации ККТ, обнаруженные в ходе электронной регистрации, должны иметь доказательную силу. Документ об отказе в регистрации ККТ должен быть заверен электронной подписью уполномоченного специалиста налоговых органов.

Дополнительно к перечисленным предположениям относительно процедуры электронной регистрации может быть выдвинуто дополнительное требование налогоплательщика о конфиденциальности состоявшихся электронных обменов, поскольку факты изменения статуса регистрации ККТ могут рассматриваться им, как коммерческая тайна. Требования конфиденциальности обменов информации, по усмотрению налоговых органов, могут устанавливаться как общие, типовые, так и выполняться избирательно для отдельно взятых налогоплательщиков.

5.2 Назначение и функции АС ЭР ККТ

Перспективная автоматизированная система электронной регистрации (АС ЭР) ККТ предназначена для решения задач, перечисленный в предыдущем разделе.

В состав АС ЭР ККТ должны входить как серверные компоненты (сервер электронной регистрации ККТ, базы данных сведений о ККТ и владельцах ККТ, система связи с налоговыми органами, рис.3), так и технические средства, обеспечивающие взаимодействие представителя поставщика ККТ или Оператора регистрации непосредственно с контрольно-кассовой техникой и средствами проверки ее исправности. Для краткости этот комплекс клиентского программно-технического обеспечения далее по тексту будет именоваться, как автоматизированное рабочее место (АРМ) АС ЭР ККТ.

Оператором может выступать как ОФД, так и третье лицо, для определенности – Оператор регистрации (ОР) ККТ.

При необходимости АС ЭР может использоваться для решения других задач технического обслуживания парка ККТ.

5.3 Классификация угроз информационной безопасности АС ЭР ККТ

Общий состав угроз информационной безопасности АС ЭР ККТ показан на рис. 3:

- Угрозы со стороны поставщика ККТ.
- Угрозы нарушения технического регламента регистрации ККТ.
- Угрозы целостности регистрационных данных.
- Угрозы техническим средствам дистанционной проверки исправности ККТ.
- Сетевые угрозы информационной безопасности АС ЭР ККТ.
- Юридические риски Оператора регистрации.
- Внутренние угрозы информационной безопасности ККТ.

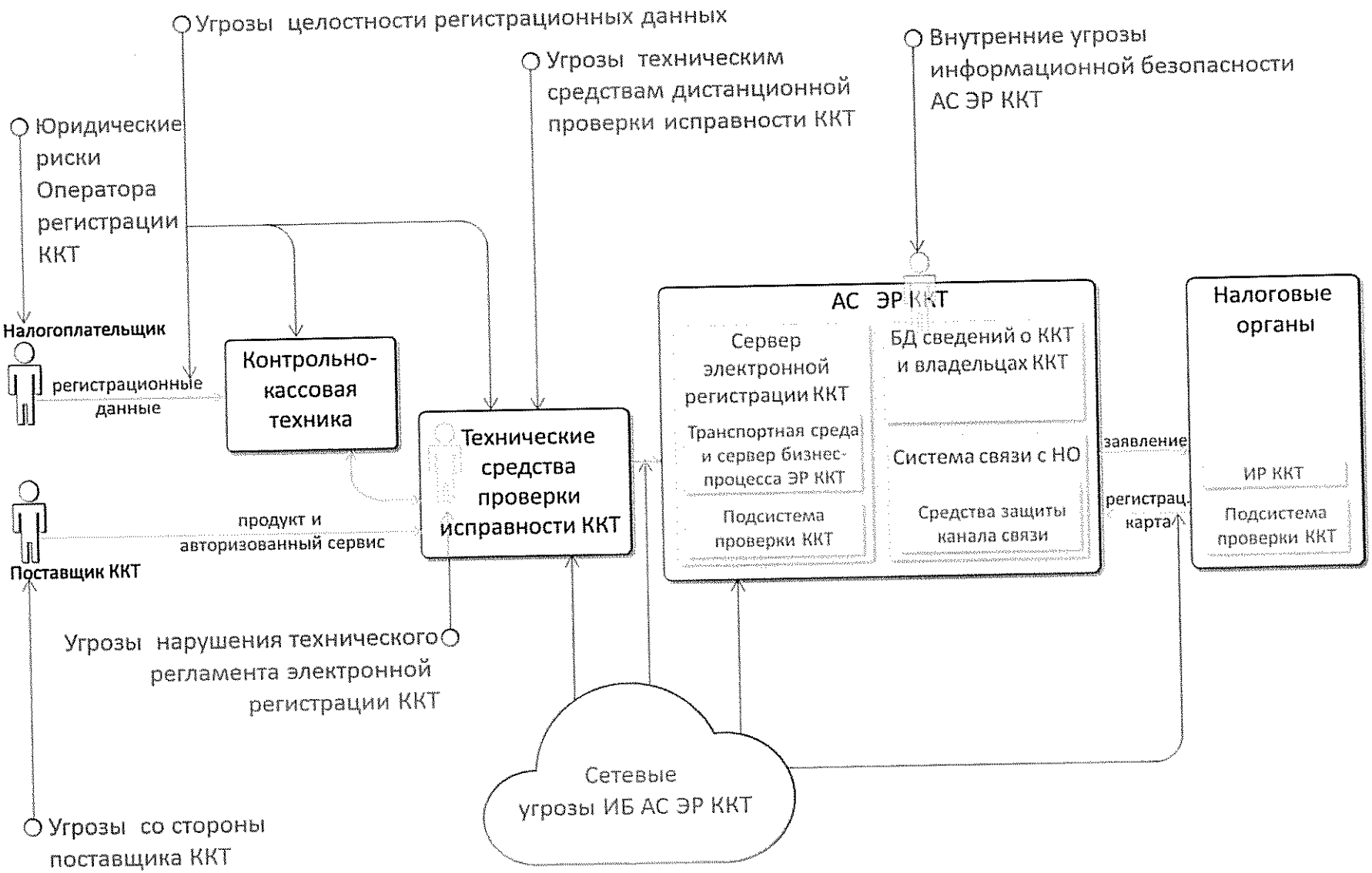
Угрозы целостности регистрационных данных
Угрозы техническим средствам дистанционной проверки исправности ККТ
Внутренние угрозы информационной безопасности АС ЭР ККТ
Юридические риски Оператора регистрации ККТ
Налогоплательщик
регистрационные данные
Контрольно-кассовая техника
Технические средства проверки исправности ККТ
АС ЭР ККТ
Сервер электронной регистрации ККТ
БД сведений о ККТ и владельцах ККТ
Транспортная среда и сервер бизнес-процесса ЭР ККТ
Система связи с НО
Подсистема проверки ККТ
Средства защиты канала связи
заявление
регистрац. карта
Налоговые органы
ИР ККТ
Подсистема проверки ККТ
продукт и авторизованный сервис
Поставщик ККТ
Угрозы нарушения технического регламента электронной регистрации ККТ
Сетевые угрозы ИБ АС ЭР ККТ
Угрозы со стороны поставщика ККТ

Рис. 3

5.3.1 Угрозы со стороны поставщика ККТ

Поставщик ККТ, руководствуясь, прежде всего, мотивами недобросовестной конкуренции и получения дополнительной (незаконной, не учтенной) прибыли, может реализовывать следующие угрозы информационной безопасности ККТ и фискальных данных:

1. Выпуск незарегистрированной продукции. Дублирование заводских номеров контрольно-кассовой техники. (Целью угрозы является последующая эксплуатация незарегистрированной техники с уклонением от налогообложения расчетных операций).
2. Выпуск контрольно-кассовой техники, не соответствующей образцу модели, прошедшей одобрение типа. Выпуск ККТ, содержащей программный или аппаратные закладки. Выпуск ККТ, содержащей уязвимости для установок программных или аппаратных закладок.
3. Применение несертифицированных средств криптографической защиты фискальных данных.

Применительно к автоматизированной системе электронной регистрации ККТ данная группа угроз может приводить к регистрации (или к попыткам регистрации, или к эксплуатации незарегистрированной) контрольно-кассовой техники, не соответствующей установленным требованиям и способствующей уклонению от учета расчетных операций и налоговым правонарушениям.

5.3.2 Угрозы нарушения технического регламента регистрации ККТ

В процессе регистрации (перерегистрации) ККТ в результате нарушения технического регламента регистрации ККТ могут возникать следующие угрозы информационной безопасности ККТ и фискальных данных:

1. Регистрация (легитимизация) образца контрольно-кассовой техники, модель которой не включена в Государственный реестр.

2. Регистрация неисправной, не выполняющей или некорректно выполняющей функции регистрации информации контрольно-кассовой техники.
3. Регистрация техники без уведомления налоговых органов. При эксплуатации такой техники правонарушитель может пытаться обеспечить корректный результат проверки контрольного проверочного кода для чеков, выведенных из-под налогообложения.
4. Нарушение целостности корпуса ККТ или ненадлежащее использование защиты корпуса ККТ.
5. Нарушение правил проверки целостности и регистрации ККТ. Неприменение или ненадлежащее применение технических средств проверки исправности ККТ. Перевод в фискальный режим и ввод в эксплуатацию неисправной (содержащей закладки, не выполняющей функции регистрации информации) контрольно-кассовой техники. (В частности, применение неаттестованного оборудования для регистрации ККТ, не производящего полную проверку целостности, неустановка или ненадлежащая установка марки-пломбы и т.п.).
6. Оформление ложных регистрационных документов или ложных свидетельств об исполнении этапов процедуры регистрации ККТ (осмотра, проверки соответствия модели, проверки исправности ККТ).

5.3.3 Угрозы целостности регистрационных данных

В процессе регистрации (перерегистрации) ККТ могут возникать угрозы информационной безопасности регистрационных данных:

1. Подача налогоплательщиком Оператору регистрации неверных сведений для регистрации ККТ.
2. Ввод в ККТ недостоверной регистрационной информации.
3. Нарушение целостности содержания регистрационной информации при ее вводе в ККТ и/или нарушение функции средств проверки целостности регистрационной информации.

5.3.4 Угрозы техническим средствам дистанционной проверки исправности ККТ

В процессе регистрации (перерегистрации) ККТ требуется выполнить проверку целостности (исправности) ККТ. Неприменение, ненадлежащее применение или нарушение целостности технических средств проверки исправности ККТ могут вести к возникновению угроз информационной безопасности ККТ, регистрационных данных ККТ или фискальных данных.

Целями угроз, перечисленных в разделах 5.3.2-5.3.4 могут являться мошенничества по схемам «вторая касса», «платеж в однодневку» и подобных. Данные атаки могут производиться недобросовестным налогоплательщиком, возможно – с привлечением технического специалиста или в сговоре с недобросовестным сотрудником службы технической поддержки продукции ККТ.

5.3.5 Сетевые угрозы информационной безопасности АС ЭР ККТ

В процессе регистрации (перерегистрации) ККТ могут возникать следующие угрозы информационной безопасности ККТ и фискальных данных, выполняемые методами сетевого доступа и/или перехвата передаваемой по сети информации:

1. Перехват, нарушение конфиденциальности регистрационных данных и/или результатов проверки сведений и проверки исправности ККТ.
2. Перехват, нарушение целостности (фальсификация) регистрационных данных и/или результатов проверки сведений и проверки исправности ККТ.
3. Фальсификация регистрационной сессии. Подмена сетевого узла, регистрирующего ККТ.
4. Фальсификация регистрационной сессии. Подмена сетевого сервера АС ЭР ККТ (фишинг).

5. Нарушение целостности АРМ АС ЭР ККТ, вирусопоражение, установка закладки в АРМ АС ЭР ККТ из сети в процессе регистрации ККТ.
6. Несанкционированный доступ из сети, нарушение целостности, вирусопоражение АС ЭР ККТ, установка закладки из сети в АС ЭР ККТ.
7. Перехват, нарушение конфиденциальности и целостности данных, передаваемый между Оператором регистрации и налоговыми органами.
8. Подавление услуги АС ЭР ККТ избыточным количеством сетевых соединений, подлинных (включая атаку перехвата и повторной передачи пакета или сообщения) или ложных запросов на регистрацию.
9. Выпуск незарегистрированной и/или не соответствующей образцу модели, прошедшей одобрение типа контрольно-кассовой техники с одновременным предоставлением фальсифицированных (фишинг) средств регистрации ККТ.

5.3.6 Юридические риски Оператора регистрации

В процессе регистрации (перерегистрации) ККТ могут возникать следующие угрозы информационной безопасности ККТ и фискальных данных:

1. Отказ участником процесса регистрации ККТ от факта выполнения действия (операции). Перераспределение ответственности за неправомерные действия.
2. Непризнание налогоплательщиком причин (фактов) отказа в регистрации ККТ.
3. Оформление ложных документов о регистрации ККТ.

5.3.7 Внутренние угрозы информационной безопасности АС ЭР ККТ

Модель внутренних, возникающих внутри контролируемой зоны АС ЭР ККТ, угроз целесообразно выстраивать в соответствии с основным положениями Концепции безопасности ФНС России [1].

В соответствии с положениями этого документа:

- Внутренний нарушитель информационной безопасности, согласно рекомендациям раздела «5.2. Базовая модель нарушителя безопасности информации ФНС России», «... более всего приближен к типу Н3. Этот тип нарушителя определяется как внутренний, самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки».
- В качестве модели внутренних угроз информационной безопасности АС ЭР ККТ следует использовать Приложение №3 к Концепции информационной безопасности Федеральной налоговой службы [1] «Перечень актуальных угроз для объектов ФНС России» и Приложение №4 «Общая классификация методов реализации угроз ИБ в ФНС России».
- Для АС ЭР ККТ целесообразно рекомендовать сегментирование системы и контроль доступа на границах сегментов. Согласно [1], «Сегменты могут группироваться по степени конфиденциальности, по функциональной потребности, по территориальному размещению средств обработки информации и самих ИР». Применительно к АК ЭР ККТ целесообразно выделить сегмент защищенной сети удаленного доступа для регистрации ККТ, сегмент взаимодействия с налоговыми органами, сегмент обработки и хранения сведений о продукции, регистрационных данных ККТ (сегмент серверов и баз данных), сегмент управления и мониторинга, сегмент управления криптографическими ключами и ключевыми документами.

- Общие задачи организации защиты информации от внутренних угроз в АС ЭР ККТ целесообразно привести в соответствие с требованиями разделов «6.3. Архитектура системы обеспечения информационной безопасности ФНС России», [1].
- Общие требования сетевой информационной безопасности АС ЭР ККТ должны соответствовать положениям раздела «8.1. Обеспечение безопасности информации при использовании международных информационно-телекоммуникационных сетей общего пользования, включая сеть Интернет» [1].
- В случае применения в составе АС ЭР ККТ средств криптографической защиты, их эксплуатацию следует организовать в соответствии с требованиями раздела «7.2.5. Дополнительные требования использования криптографических средств» [1]. Дополнительно для обработки фискальных данных и сохранения целостности ключевого пространства (см. дополнительно описания атаки 13.3, Таблица 1), следует использовать средства криптографической защиты фискальных данных, совместимые с применяемыми в ККТ..
- Систему управления и мониторинга ИБ АС ЭР ККТ целесообразно разрабатывать с учетом требований раздела «IX. Мониторинг и контроль состояния безопасности информации» документа [1].
- В случае, если в качестве Оператора регистрации выступает внешняя, не входящая в состав налоговых органов, организация, требования к этой организации должны определяться в соответствии с разделом «8.2.1. Требования, учитываемые при заключении контракта с поставщиком услуг» документа [1]. Дополнительно для Оператора регистрации следует рекомендовать наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации и лицензии ФСБ России на виды деятельности 12, 13, 14, 17, 20, 21, 25, 26, 27 [16].

Использование цитированных выше методических источников и применение практик, рекомендованных в Концепции информационной

безопасности ФНС России, исчерпывает постановку задачи защиты АС ЭР ККТ от внутренних угроз и далее в настоящем документе эти вопросы не рассматриваются.

6. Модель угроз средств обработки фискальных данных. Автоматизированная система Оператора фискальных данных

6.1 Предположения о порядке сбора фискальных данных Оператором фискальных данных

В настоящее время сбор и контроль фискальных данных не регламентируется никакими нормативно-правовыми актами или техническими регламентами. Поэтому предположения о порядке сбора фискальных данных сделаны на основе результатов эксперимента ФНС России, проведенного в 2014-2015 гг. на основе Доклада Правительству Российской Федерации по результатам эксперимента ФНС России [17].

Данные о расчетах формировались ККТ и передавались в АС ОФД, осуществлявшего передачу этих сведений в неизменном виде в налоговые органы, а также их обработку и хранение в принадлежащих этому ОФД средствах вычислительной техники.

При подключении ККТ в рамках эксперимента, использовались как проводные (Ethernet, оптоволокно, ADSL), так и беспроводные (3G, 4G, gprs, edge, WiMax)каналы связи.

Распечатанный (сформированный в электронном виде) чек, переданный покупателю, снабжался фискальным признаком, сформированным с применением СКЗИ.

При отсутствии технической возможности передачи данных (отсутствие связи в зоне эксплуатации ККТ) в ККТ предлагается использовать механизм выгрузки данных по проведенным расчётам за отчетный период. При этом отчет должен формироваться с применением криптографических методов для защиты от чтения и корректировки данных и направляться ОФД по окончанию отчетного периода.

Для проверки кассовых чеков были разработаны мобильные приложения на платформах iOS и Android, которые были размещены в соответствующих магазинах приложений.

6.2 Назначение и функции АС ОФД

В соответствии с [17] основные функции АС ОФД:

- Подключение ККТ к сети сбора фискальных данных.
- Прием (сбор) фискальных данных и проверка (контроль) их достоверности.
- Обработка и хранение фискальных данных.
- Передача фискальных данных в налоговые органы, в т.ч. по заданному расписанию и по запросу из налоговых органов.

6.3 Классификация угроз информационной безопасности АС ОФД

Угрозы информационной безопасности фискальных данных, возникающие на этапах их формирования, сбора и контроля описаны в разделе «4. Модель угроз информационной безопасности фискальных данных, фиксируемых контрольно-кассовой техникой и переданных оператору фискальных данных». Общий состав угроз информационной безопасности АС ОФД, за исключением упомянутых угроз безопасности фискальных данных, показан на рис. 4:

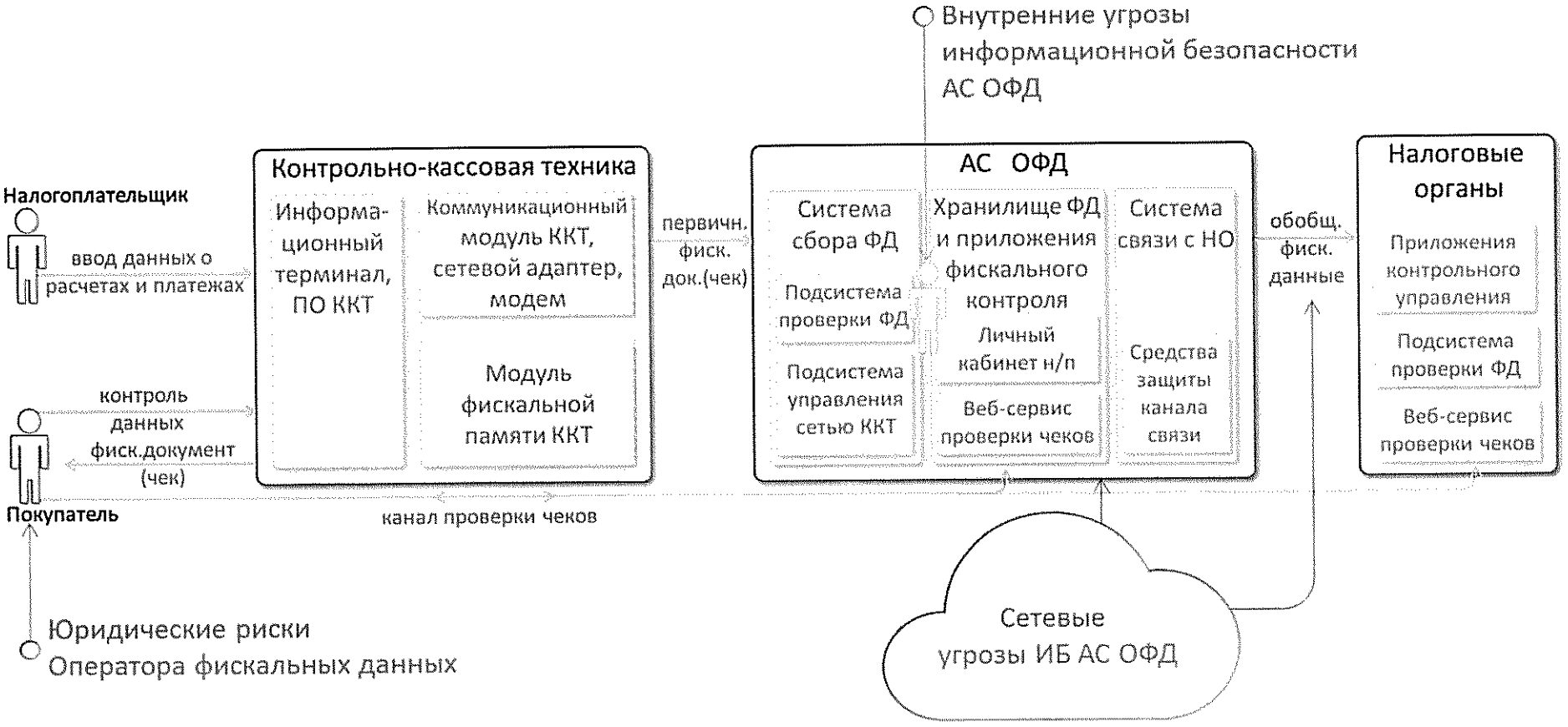
Внутренние угрозы информационной безопасности АС ОФД
Налогоплательщик
ввод данных о расчетах и платежах
Контрольно-кассовая техника
Информа-ционный терминал, ПО ККТ
Коммуникационный модуль ККТ, сетевой адаптер, модем
Модуль фискальной памяти ККТ
первичн. фиск. док.(чек)
АС ОФД
Система сбора ФД
Подсистема проверки ФД
Подсистема управления сетью ККТ
Хранилище ФД и приложения фискального контроля
Личный кабинет н/п
Веб-сервис проверки чеков
Система связи с НО
Средства защиты канала связи
обобщ. фиск. данные
Налоговые органы
Приложения контрольного управления
Подсистема проверки ФД
Веб-сервис проверки чеков
контроль данных фиск.документ (чек)
Покупатель
канал проверки чеков
Сетевые угрозы ИБ АС ОФД
Юридические риски Оператора фискальных данных

Рис. 4

6.4 Сетевые угрозы информационной безопасности АС ОФД

Состав угроз информационной безопасности АС ОФД в целом совпадает с перечисленными в разделах «4.1.3 Сетевые угрозы информационной безопасности фискальных данных» и «5.3.5 Сетевые угрозы информационной безопасности АС ЭР ККТ» с дополнениями:

- Сетевые угрозы целостности фискальных данных могут реализоваться путем атак на целостность фискальных данных. Загрузка закладки в ККТ из сети может производиться динамически. Закладка может временно использоваться на этапе совершения налогового правонарушения, после чего автоматически или по команде злоумышленника устраняться из ККТ. В этом случае следы и доказательная база налогового правонарушения могут уничтожаться на момент проведения проверки специалистами налоговых органов.
- Устранение следов налогового правонарушения еще более эффективно, если агент блокировки/модернизации фискальных данных располагается вне зоны эксплуатации ККТ. В этом случае доказательно установить, что установленная на внешнем по отношению к ККТ оборудовании закладка связана с действиями налогового правонарушителя будет чрезвычайно сложно или невозможно.
- Особое значение сетевые угрозы имеют при использовании в качестве ККТ программно-технических комплексов на основе мобильных гаджетов. Техника этого класса характеризуется тем, что (а) не контролируема – высшие права доступа в ОС мобильного гаджета обычно оставляет за собой производитель, передавая пользователю ограниченные права доступа и (б) ее программная среда не замкнута – компонентный состав операционной системы, обновление ПО, обмены данными с серверами производителя гаджета и серверами обновлений программного обеспечения не документированы, могут выполняться скрытно и без управления со стороны пользователя.

- АС ОФД работает с высокой нагрузкой. Общее количество чеков, обрабатываемых автоматизированной системой в день, может превышать несколько миллионов. Одновременно АС ОФД должна оперативно управлять процессом сбора фискальных документов, как минимум, оперативно производя проверку принимаемых данных и распространяя подтверждения их приема. Оба эти обстоятельства делают АС ОФД чрезвычайно уязвимой по отношению к атакам отказа в обслуживании.
- В распределенной среде особое значение приобретает целостность пространства доверия, в котором работают ККТ и АС ОФД. В случае, если это пространство доверия может быть сегментировано, производитель контрафактных средств защиты может создать пару: «нелегитимное средство защиты + нелегитимный сервис проверки». Далее, на фальсифицированном чеке достаточно указать ссылку на сервис «проверки» фальсифицированных чеков. В этом случае покупатель будет получать чек от фальсифицированной контрольно-кассовой техники и проверять подлинность чека на фальсифицированном же сервере проверки чека (его интернет-адрес для автоматической проверки чека может печататься непосредственно на чеке). В этом выделенном «кластере доверия», включающем парный фальсификат средств защиты ФД и средств проверки подлинности ФД, созданном с целями налогового правонарушения, покупатель никогда не сможет установить факт получения им фальсифицированного, не учтенного в налоговых органах, чека.

С учетом перечисленных особенностей сетевой информационной безопасности АС ОФД, целесообразно рассмотреть следующие дополнительные угрозы:

1. Подавление услуги АС ОФД (атака «отказ в обслуживании»). Перехват и повторная передача ранее переданных легитимных фискальных данных (может иметь как самостоятельные деструктивные последствия, так и использоваться для усиления эффекта атаки «отказ в обслуживании»).

2. Создание ложного сервера АС ОФД (имперсонация АС ОФД, «фишинг»). Блокировка/фальсификация каналов квитирования приема фискальных документов.
3. Создание ложного канала проверки фискального признака (в пакете с выдачей ложного чека).

6.5 Юридические риски Оператора фискальных данных, связанные с качеством фискальных данных

Деятельность Оператора фискальных данных связана с возможной ответственностью по ряду юридических рисков, связанных с процессами сбора и обработки фискальных данных:

1. Перенаправление к Оператору фискальных данных претензий покупателей в случае отказа владельца ККТ от фискального документа.
2. Претензия налогоплательщика в случае легализации Оператором фискальных данных фальшивого фискального документа или при обнаружении чека, изданного третьим лицом от имени налогоплательщика.

6.6 Внутренние угрозы информационной безопасности АС ОФД

Внутренние угрозы информационной безопасности АС ОФД в совокупности имеют те же состав и природу, что и описанные в разделе «5.3.7 Внутренние угрозы информационной безопасности ККТ». Эти внутренние угрозы должны нейтрализовываться в соответствии с рекомендациями, изложенными в [1] и далее в настоящем документе не рассматриваются.

7. Анализ угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных

Угрозы информационной безопасности реализуются путем различного рода атак.

Атака – метод осуществления заданной угрозы информационной безопасности, определенным способом, реализованный нарушителем заданного класса. В рамках настоящего документа атаки характеризуются следующим набором данных:

- Субъект, осуществляющий атаку. Далее по тексту, если не оговорено иное –это нарушитель типа Н3, обладающий всеми доступными ему техническими средствами.
- Объект (цель) атаки. В конечном счете, целью всякой атаки является нарушение той или иной характеристики безопасности фискальных данных из числа перечисленных в разделе «Общие цели и механизмы защиты фискальных данных». Это целостность (Ц), доступность (Д), аутентичность (А), подотчетность (П), конфиденциальность (К) фискальных данных.
- Канал(ы) осуществления атаки.

Угрозы, реализуемые при помощи тех или иных атак, характеризуются различным уровнем риска реализации угрозы. Риск зависит от вероятности того, что состоится угрожающее событие, и размера ущерба, который будет нанесен системе в случае реализации угрожающего события [18]. В настоящем документе будет принят следующий метод качественного анализа.

Применительно к определенной атаке, риск, вероятность и ущерб будут описываться тремя качественными значениями – высокий (В), средний (С), низкий (Н). В случае, когда остаточный риск будет характеризоваться исчезающе малыми значениями (например, риск компрометации стойкого криптографического ключа методом прямого

перебора), будет применяться дополнительно характеристика «пренебрежимо малый» (П).

Меры защиты от угроз (обработки риска) классифицируются как организационные (О) и технические (Т), среди которых, как особый класс технических мер, выделим криптографические (К). По отношению ко времени совершения угрожающего события, меры обработки риска различают как проактивные (профилактические), применяемые для устранения причин возникновения риска, активные, оказывающие непосредственное противодействие угрожающим факторам, и реактивные (апостериорные), применяемые после реализации угрожающего события.

Детальное описание угроз информационной безопасности приведено в Таблице 1. При описании атак использованы обозначения нарушителей, приведенные в разделе «2.6 Модель нарушителя информационной безопасности фискальных данных, технических средств и автоматизированных систем обработки фискальных данных» и обозначения объектов атак, принятые в разделе «2.7 Методика детализированного анализа угроз информационной безопасности».

Таблица 1

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
1	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ НА ЭТАПАХ ПРОЕКТИРОВАНИЯ, ОДОБРЕНИЯ ТИПА И ПРОИЗВОДСТВА					
1.1	Ошибка проектирования, приводящая к появлению уязвимости ККТ	H1z	ККТ, МФП (Ц)	Ошибка при разработке архитектуры, проектной документации, цикла испытаний контрольно-кассовой техники	H	Предполагается, что разработчик ККТ обладает квалификацией, обеспечивающей разумно низкий риск появления ошибки, имеющей последствия в области безопасности фискальных данных. Для ККТ в виде программно-технических комплексов этот риск следует считать более высоким, поскольку разработчик ПО ККТ не имеет прямого влияния на модель и состояние аппаратной и операционной платформы
1.2	Преднамеренное внесение закладки или создание условий для ее успешного внесения недобросовестным разработчиком ККТ	H1z	ККТ, МФП (Ц)	Преднамеренное внесение уязвимости или организация интерфейса (возможности) для последующего внесения уязвимости при разработке архитектуры, проектной документации модели ККТ	H(C)	Этот риск принят равным для всех производителей, поскольку нет оснований для того, чтобы утверждать, что криминальные мотивы доминируют у производителей выделенного класса техники

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
1.3	Разработка закладки третьим лицом	H1z	ККТ, МФП (Ц)	Разработка программной или программно-аппаратной закладки, предназначенной для нарушения процесса регистрации фискальных данных	В	Разработка закладок, способствующих нарушению процесса регистрации фискальных данных, является отдельным направлением криминального бизнеса. Установлен факт, что уязвимость ККТ является конкурентным преимуществом на рынке контрольно-кассовой техники. Поэтому наличие уязвимости ККТ является вероятным, а эксплуатация уязвимости – массовой. Такие закладки разрабатываются в массовом порядке,. Вероятность разработки закладки практически для всякого распространенного образца ККТ близка к единице. Вероятность разработки программной закладки

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						для применения в программно-технических комплексах ККТ следует считать повышенной, поскольку цена разработки такой закладки в 5-20 раз ниже, чем стоимость закладки, ориентированной на конкретную аппаратную модель ККМ
1.4	Установка закладки в процессе производства, хранения, транспортировки продукции ККТ	H2	ККТ, МФП (Ц)	Закладка, разработанная нарушителем H1z в составе атаки 1.3, устанавливается в продукцию до ее поставки покупателю	H	до продажи ККТ конкретному покупателю отсутствует возможность избирательного подхода: априорно не ясно, проявит ли потенциальный покупатель ККТ интерес к наличию в ее составе закладки
2	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ НА ЭТАПЕ РЕГИСТРАЦИИ ККТ					
2.1	Установка закладки в процессе приобретения, ввода в эксплуатацию, перевода ККТ в фискальный режим	H3, H3s	ККТ, МФП (Ц)	Совместные действия пользователя ККТ и сотрудника технической поддержки с целями блокировки функции модуля фискальной памяти,	B	Статистически это один из наиболее часто реализующихся на практике рисков

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				установки контрафактного модуля фискальной памяти или установки в ККТ закладки, подобной разработанной нарушителем H1z в составе атаки 1.3		
2.2	Регистрация в качестве ККТ техники, не прошедшей одобрение типа	H3, H3s	ККТ, МФП (Ц)	Совместные действия пользователя ККТ и сотрудника технической поддержки с целями регистрации в качестве ККТ постороннего программно-технического средства, не выполняющего (частично блокирующего) функции регистрации расчетных операций. По существу атака 2.2 отличается от атаки 2.1 лишь тем, что каналом атаки 2.1 является модернизация прошедшей одобрение типа ККТ, а в результате атаки 2.2 используется произвольное программно-техническое средство	В	См. 2.1
2.3	Нарушение правил проверки целостности и исправности ККТ при	H3, H3s	ККТ, МФП (Ц)	При электронной регистрации ККТ должны использоваться те или иные	В	См. 2.1.

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	регистрации ККТ			технические средства проверки исправности ККТ. Пользователь ККТ, действуя в сговоре с сотрудником технической поддержки, могут отказаться от штатного использования, блокировать или фальсифицировать результаты работы технических средств проверки ККТ с целями регистрации образца ККТ, не исполняющего надлежащим образом функции регистрации информации о расчетах		
3	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ И ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ ККТ НА ЭТАПЕ ЭКСПЛУАТАЦИИ ККТ					
3.1	Нарушение целостности ККТ	Н3 [+Н1z, +Н3s]	ККТ, МФП (Ц)	Владелец ККТ, самостоятельно или в сговоре с сотрудником службы технической поддержки ККТ, производит нарушение целостности ККТ. Непосредственной угрозы для фискальных данных атака не представляет, однако является первым этапом для атак 3.2-3.4,	В	нарушение корпуса или марок-пломб ККТ носит распространенный характер. Нарушение сдерживается мерами контроля налоговых органов над парком ККТ и центрами технического обслуживания, однако выявление нарушения требует проверки на месте

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				характеризующихся высоким риском		эксплуатации ККТ и по этой причине является дорогостоящим мероприятием
3.2	Нарушение целостности программно-аппаратных средств ККТ	Н3 [+Н1z, +Н3s]	ККТ, МФП (Ц)	Владелец ККТ, самостоятельно или в сговоре с сотрудником службы технической поддержки ККТ, возможно, с применением инструментария, разработанного для взлома ККТ и/или с эксплуатацией уязвимостей, умышленно или не умышленно допущенных производителем ККТ, выполняет установку аппаратной закладки и/или перепрошивку штатного программного обеспечения ККТ с целями: (1) блокировки ФД или фальсификации состава регистрируемых ФД (Ц, Д ФД) (2) нарушения данных о времени регистрируемых событий (Ц ККТ, Ц ФД) (3) изменения	В	Атака отличается от 2.1 только тем, что выполняется на другом, нежели регистрация ККТ, этапе жизненного цикла ККТ. Особенность этой атаки для программно-технических комплексов ККТ на основе гаджетов состоит в том, что для касс этого типа на сегодня нет разработанной и апробированной практики технического обслуживания

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				регистрационных реквизитов ККТ и/или данных о налогоплательщике (Ц ККТ, А ФД)		
3.3	Нарушение целостности модуля фискальной памяти ККТ и применение нелегально восстановленного модуля фискальной памяти	Н3 [+H1z, +H3s]	ККТ, МФП (Ц,А)	Владелец ККТ, самостоятельно или в сговоре с сотрудником службы технической поддержки ККТ, производит установку в ККТ модуля фискальной памяти, имеющего созданный нарушителем H1z канал для блокировки/модернизации фискальных данных. Эта атака отличается от предыдущих способом исполнения (объектом и каналом атаки)	С	Атака носит распространенный характер. По практике эксплуатации ЭКЛЗ, существует ряд мастерских, выполняющих реверс-инжиниринг МФП и модернизирующих его. Уровень риска установлен как «средний» потому, что выявление злоумышленника при контроле выполняется достаточно эффективно (имеется явная улика), а суммарная мощность производства «восстановленных» МФП этим способом ограничена
3.4	Применение в составе ККТ контрафактных и клонированных модулей	Н3 [+H1z, +H3s]	ККТ, МФП (Ц,А)	Владелец ККТ, умышленно или по неведению, производит установку в ККТ	С	Атака имеет широкое распространение у производителей МФП, не

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	фискальной памяти			модуля фискальной памяти, созданного с нарушением технологии и с повторно использованными атрибутами регистрации и криптографическими ключами. Ввиду того, что ККТ имеет в своем составе конфиденциальный криптографический ключ, а дизайн МФП представляется достаточно защищенным, компрометация ключа и атрибутов аутентификации МФП может быть осуществлена исключительно на площадке производителя МФП		прошедших сертификационную оценку своей продукции. Атака может осуществляться путем: (1) выпуска продукции, не прошедшей оценку соответствия (2) нарушения порядка производства ККТ в части отсутствия тематического исследования по результатам встраивания МФП (3) путем повторного использования уникальных ключей и регистрационных данных производителем МФП. Изготовление «клонов МФП» с идентичными регистрационными данными позволяет заполнять фискальными данными один экземпляр «клона МФП» и после его заполнения заменять в ККТ на новый чистый

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						экземпляр «клона МФП». В случае если добросовестный владелец ККТ был не в курсе того, что в его ККТ установлен «клон МФП», такой «клон МФП» мог не использоваться им непосредственно для уклонения от уплаты налогов. В тоже время такой пользователь ККТ мог косвенно и сознательно вовлекаться в расширение сбыта «клонов МФП» путем их покупки по более привлекательным ценам и создания эффекта массовости их применения, в результате чего для налоговых органов становится затруднительно реализовать мероприятия по выявлению пользователей ККТ умышленно

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						применяющих «клонов МФП» в целях уклонения от уплаты налогов.
3.5	Клонирование ККТ	Н3, Н3s	ККТ, МФП (Ц,А)	Атака осуществляется путем регистрации легитимной кассы и создания под прикрытием легитимной кассы ее «клонов», т.е. незарегистрированных касс с аналогичными регистрационными атрибутами	В	За данной атакой стоит распространенное налоговое мошенничество по схеме «вторая» («черная») касса. Эта мошенническая схема получает широкое распространение, поскольку обеспечивает довольно высокий уровень безопасности для налогового правонарушителя, который при проверке со стороны налоговых органов предъявляет легитимную кассу и эффективно отказывается от операций с «черной» кассой
4	СЕТЕВЫЕ УГРОЗЫ ЦЕЛОСТНОСТИ ККТ					
4.1	Взлом ККТ методами сетевого доступа	Н1i (Н3)	ККТ, МФП	Канал атаки (идентификация платформы ККТ, поиск	С	Установка закладки в ККТ по сети нарушителем

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
			(А, Ц, К)	уязвимостей, несанкционированный доступ из сети, захват прав доступа в операционной системе образца ККТ и т.д.). Объекты и субъекты атаки совпадают с описанными в атаке 3.2		H1i представляется относительно маловероятной. Также у налогового злоумышленника Н3 есть более простые и более эффективные каналы установки закладки. Однако установка самому себе сетевой закладки для коррекции чеков и маскировка закладки под вирус технически проста и удобна для нарушителя Н3 с точки зрения ухода от ответственности за налоговое правонарушение. При установке корректирующей закладки вне ККТ при проверке налогоплательщика налоговыми органами практически невозможно как найти закладку, так и доказать связь между недобросовестным

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						налогоплательщиком и закладкой. Удобные для мошенника возможности дают также варианты удаленного управления сетевой закладкой: доверенное лицо налогоплательщика без уведомления кассира изымает из учета или модернизирует чеки путем, например, мобильного приложения не смартфоне, никак не связанном с ККТ. В связи с тем, что атаки подобного типа были выявлены в ККТ, объединенных в закрытые сети связи налогоплательщиков, и реализовывались даже в ККТ без передачи данных, такие атаки требуют присвоения им уровня риска не ниже, чем «средний»
4.2	Атаки на ККТ,	H1i	ККТ,	Атака отличается от	H	Вероятность поражения

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	выполняемые путем распространения опасного мобильного кода		МФП (А, Ц, К,Д)	предыдущей только каналом (вирусопоражение, передача опасного мобильного кода, установка spyware) и субъектом: мало вероятно, что владелец ККТ, нарушитель Н3, станет использовать столь сложный инструмент, как сетевой вирус для поражения находящейся в его распоряжении техники		неадресной сетевой атакой представляется маловероятной для техники класса ККТ, более вероятна для техники класса ЭВМ и относительно высоко вероятна для ККТ типа «программно-технический комплекс»
4.3	Перехват каналов сетевого управления (конфигурирования) ККТ	H1i [+H3, +H1z, +H3s]	ККТ, МФП (Ц,К,Д, А)	Каналом атаки является перехват (блокирование, вмешательство в поток данных, искажение данных) управления ККТ с целями изменения режимов функционирования ККТ, раскрытия ККТ для атаки 4.1, перенаправление трафика ККТ на ложный узел приема фискальных данных и т.п.	В(С)	Риск представляется высоким или средним при условии, что канал управления открыт для перехвата
5	УГРОЗЫ ФИСКАЛЬНЫМ ДАННЫМ В ПРОЦЕССЕ ИХ ФОРМИРОВАНИЯ И ОБРАБОТКИ					
5.1	Манипуляции с чеками при их создании	Н3	ФД	Пользователь ККТ не выдает покупателю чек или выдает документ, не являющийся чеком, или повторно выдает	В	Риски атак этого типа чрезвычайно высоки. В то же время атаки этого типа не контролируются

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				ранее сформированный, не востребованный предыдущим покупателем чек и т.п. Чек не формируется, сумма чека не регистрируется и выводится из-под налогообложения		техническими средствами и не могут быть предотвращены техническими мерами
5.2	Фальсификация содержания чека	НЗ	ФД (Ц,А)	Атака выполняется владельцем ККТ или лицом, имеющим права доступа пользователя ККТ и действующим по поручению владельца ККТ. Цель атаки – изъятие из фискального документа всех или части позиций расчёта для снижения зарегистрированной суммы и уклонения от уплаты налогов. Как канал атаки может использоваться, управляемое оператором кассы в реальном времени, средство атаки (закладка) в составе ККТ. Канал атаки может использовать закладку в ККТ, внедренную в результате атак 1.1-1.4, 2.1-2.3, 3.2-3.4, 4.1	В	Риск атаки установлен, как «высокий» на основе анализа практики технических нарушений целостности фискальных данных

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				или 4.2. Механизм применения закладки – модернизация регистрируемых фискальных данных. При выполнении атаки фискальный признак может устанавливаться произвольно в расчете на то, что фискальный признак чека не будет проверен		
5.3	Фальсификация фискального признака чека	НЗ	ФД	Атака в целом аналогична атаке 5.2, где, наряду с чеком, формируется суррогат фискального признака, но отличается деталями подделки фискального признака. Существует ряд способов полной или частичной защиты фальсифицированного чека от раскрытия фальсификации при проверке: 1) повторное использование реквизитов, суммы и фискального признака для выписки «нового» чека (обычно на ту же сумму при торговле однотипными	В	Риск оценен как «высокий», поскольку контроль за допуском к эксплуатации ККТ и МФП одобренного типа был в течение длительного периода времени ослаблен, и в настоящее время на рынке функционируют сотни тысяч единиц нелегитимной продукции ККТ и МФП

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				товарами) 2) формирование чека с частично корректной информацией 3) создание сервиса для поверки фискального признака нелегитимных чеков		
5.4	Отложенное формирование или ревизия отчетности с изъятием полного состава (или части) фискальных данных	НЗ	ФД (Ц,А)	Атаки с отложенным формированием фискального признака могут применяться по нескольким сценариям: 1) откладывание регистрации чека до момента, когда оператор ККТ убедится, что чек востребован покупателем (востребованные чеки при этом регистрируются, невостребованные – нет) 2) выдача покупателю чековых суррогатов и «учет» (включающий регистрацию в МФП) части «удобных» или «опасных» чеков в конце смены 3) выдача покупателю чековых суррогатов и регистрация корректных	В(С)	Мошенничества, связанные с искажением времени регистрации чека имеют широкое распространение. Риски уклонения от налогообложения по этим схемам следует признать высокими (или средними, в силу более сложной, чем, например, атаки 5.1-5.3 схемы атаки)

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				чеков постфактум, только в случае проверки (при этом сформированный постфактум чек полностью воспроизводит ранее фальсифицированный, фальсифицированный чек владельцем ККТ не признается, а отложенная регистрация чека, «прикрывающего» фальсификацию производится с перестановкой времени ККТ на время выписки фальшивого чека)		
5.5	Фальсификация электронного фискального документа[2]	Н3	ФД (Ц,А)	Электронный фискальный документ может быть модифицирован, причем следы изменения могут полностью отсутствовать	В	Риск признан высоким по причине простоты и отсутствия следов модификации данных в вычислительной системе
6	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИСКАЛЬНЫХ ДАННЫХ					
6.1	Любое нарушение целостности фискальных данных произвольным	Н1i	ФД (Ц,А)	Перехват, блокировка, уничтожение, дуплицирование,	Н	Вероятность поражения данных в незащищенном виде высока. Риск

[2] В настоящее время практика применения фискального документа только в электронной (без печати бумажной копии) форме отсутствует. Однако данная атака включена в Модель угроз, поскольку вопрос о необходимости применения чека в электронной форме активно обсуждается и следует предвидеть появление фискальных документов в чисто электронной форме.

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	нарушителем из сети			модернизация, создание фальсифицированных фискальных данных сетевым хакером		признан низким, поскольку субъект атаки, не имеющий конкретных корыстных интересов, с крайне малой вероятностью сможет нанести существенный ущерб процессам сбора налогов и фискального контроля
6.2	Изъятие из потока (блокировка) или нарушение целостности фискальных данных недобросовестным налогоплательщиком на этапе их передачи от ККТ к ОФД	НЗ	ФД (Ц)	Атака по сценариям, мотивам и результатам подобна результатам действия закладок в составе ККТ (см. атаки 1.2, 1.4, 2.1, 3.2, 4.1) с той разницей, что средство атаки на фискальные данные располагается за пределами ККИ и контролируемой зоны владельца ККТ. Применение закладки вне ККТ позволяет производить любые технические операции с фискальными данными (блокировка, нарушение целостности ФД в части даты, суммы, регистрационных данных о	В	Оценка риска соответствует оценке для соответствующих несетевых атак

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				владельце ККТ, фискального признака) без улик, прямо указывающих на действительного злоумышленника		
6.3	Перехват (нарушение конфиденциальности) ФД на этапе их передачи от ККТ к ОФД	H1i	ФД (К)	Цель атаки – раскрытие личной или коммерческой тайны налогоплательщика и/или покупателя	С	Единичная атака наносит практически очень малый ущерб (за исключением достаточно редких покупок, компрометирующих продавца или покупателя). Более значимо систематическое наблюдение за трафиком. Организация такого наблюдения – деятельность, близкая по характеру к промышленному шпионажу, но ущерб в отдельных случаях может быть очень значителен. Риск оценен как «средний»
6.4	Атаки на систему аутентификации участников сетевого	H1i, H3	ФД (А,Ц,К)	Атаки с посредником, атаки на системы управления сетевыми адресами и	В	Риск этих атак по отношению к незащищенным

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	взаимодействия			именами, атаки на домены аутентификации, имперсонация ОФД или ККТ. В основе атак лежит «обман» системы аутентификации, в результате которого производится замена одного из участников взаимодействия на нарушителя или включение нарушителя в канал защищенного взаимодействия с последующей компрометацией защиты канала. Целями атаки могут быть: нарушение целостности и конфиденциальности фискальных данных. Для атаки могут также использоваться скомпрометированные инфраструктуры типа системы именования DNS, веб-инфраструктуры ОФД и т.п. Атаку может осуществлять произвольный сетевой хакер		фискальным данным, в силу распространенности подобных атак в сети, следует признать высоким

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				(H1i) или нарушитель-налогоплательщик Н3. Как и во всех прочих сетевых атаках, поиск сетевой закладки и доказательство уличающей связи закладки с нарушителем Н3 весьма затруднительны		
6.5	Подавление сетевой активности ККТ	H1i	ККТ, ФД (Д)	Атака, выполняемая сетевым хакером по мотивам вандализма, шантажа или с целями нанесения ущерба конкуренту, механизм которой заключается в адресации к ККТ структурированного или не структурированного трафика высокой интенсивности с целями вывода ККТ из строя, блокирования ее сетевых взаимодействий, блокирования операций по передаче данных	Н	Риск принят низким по причине, что временное подавление сетевой активности единичного образца контрольно-кассовой техники в целом не может нанести значительный ущерб системе регистрации сведений о расчетах и платежах в целом. Предусматривается, что ККТ должна иметь возможность в некорректируемом виде хранить информацию в случае временного отсутствия канала связи с ОФД
7	УГРОЗЫ АС ЭР ККТ СО СТОРОНЫ ПОСТАВЩИКА ККТ					

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
7.1	Выпуск незарегистрированной продукции	Н1	БД АС ЭР ККТ (Ц,А)	Поставщик ККТ выпускает продукцию без ее регистрации и поэкземплярного учета СКЗФД в базах данных АС ЭР ККТ. Мотивом может служить выгода от продажи контрафактной, предназначенной для организации уклонения от налогообложения, ККТ	В	Риск признан высоким по причине широко распространенной практики использования контрафактной продукции ККТ и МФП
7.2	Выпуск ККТ, не соответствующей образцу модели, прошедшей одобрение типа	Н1	БД АС ЭР ККТ (Ц,А)	Атака отличается от 7.1 каналом: продукция, также подготовленная для поддержки налогового правонарушения, регистрируется как полностью легитимная	В	Риск признан высоким по причине широко распространенной практики использования контрафактной продукции ККТ и МФП
7.3	Применение несертифицированных средств криптографической защиты фискальных данных	Н1	БД АС ЭР ККТ (Ц,А)	Атака отличается от 7.1 каналом: в составе полностью соответствующей образцу модели из Госреестра ККТ применяется фискальная память, функции безопасности которой не прошли оценку в установленном порядке,	В	Риск признан высоким по причине широко распространенной практики использования контрафактной продукции ККТ и МФП
8	УГРОЗЫ НАРУШЕНИЯ ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕГИСТРАЦИИ ККТ В АС ЭР ККТ					

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
8.1	Регистрация ККТ, не включенной в Государственный реестр	Н3, Н3s	АС ЭР ККТ (Ц,А)	Представитель Оператора регистрации, находясь в сговоре с налогоплательщиком, не производит проверку регистрируемой техники на предмет одобрения типа (включения модели ККТ в Госреестр) с целью последующего ненадлежащего применения ККТ	С	Риск оценен как «средний»,при этом . оценка требует уточнения по мере внедрения АС ЭР ККТ
8.2	Регистрация неисправной контрольно-кассовой техники	Н3, Н3s	АС ЭР ККТ (Ц,А)	Атака отличается от 8.1 каналом: представитель Оператора регистрации, находясь в сговоре с налогоплательщиком, пренебрегает проверкой исправности ККТ или фальсифицирует результат проверки	С	Риск оценен, как «средний», при этом оценка требует уточнения по мере внедрения АС ЭР ККТ
8.3	Псевдорегистрация ККТ без уведомления налоговых органов	Н3, Н3s	АС ЭР ККТ (А)	Владелец ККТ, самостоятельно или в сговоре с сотрудником службы технической поддержки ККТ, производит псевдорегистрацию образца техники без уведомления	С	Риск оценен как «средний», на основе анализа существующих практик налоговых правонарушений

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				налоговых органов. При использовании легитимно выпущенной продукции, такая контрольно-кассовая техника может давать положительные результаты проверки фискального признака и, тем самым, не возбуждать подозрений покупателя. Одновременно, выручка, зарегистрированная такой ККТ, может выводиться из-под налогообложения		
8.4	Нарушение целостности корпуса ККТ при регистрации ККТ	Н3, Н3s	ККТ, АС ЭР ККТ (Ц,А)	Владелец ККТ, самостоятельно или в сговоре с сотрудником службы технической поддержки ККТ, производит регистрацию образца техники, нарушая целостность корпуса ККТ или оставляя возможность такого нарушения целостности на будущее с целями реализации атак, подобных 1.2, 1.4, 2.1, 3.2, 4.1	С	Риск оценен, как «средний», на основе анализа существующих практик налоговых правонарушений
8.5	Нарушение правил проверки целостности и	Н3, Н3s	ККТ, АРМ	Атака имеет те же цели, что и атаки 8.1, 8.2, 8.4, но	С	Риск оценен, как «средний», при этом

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
	регистрации ККТ		АС ККТ, АС ЭР ККТ (Ц,А)	выполняется по другому каналу: неисполнение установленной процедуры регистрации, неиспользование, ненадлежащее использованием или порча технических средств (АРМ АС ЭР ККТ)		оценка требует уточнения по мере внедрения АС ЭР ККТ
8.6	Оформление ложных регистрационных документов	Н3, Н3s	АС ЭР ККТ (Ц,А)	В процедуре электронной регистрации ККТ ряд документов (заявление о регистрации, карточка регистрации ККТ, свидетельства соответствия и технических проверок) могут быть представлены в виде электронных документов	Н	Риск оценен как «низкий» по той причине, что оформление недостоверных документов не оказывает прямого влияния на собираемость налогов, однако проблема защиты электронных документов требует решения, поскольку ложные документы могут использоваться для сокрытия следов нарушений правил регистрации ККТ (атака 8.4) и прикрытия налоговых правонарушений

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
9	УГРОЗЫ ЦЕЛОСТНОСТИ РЕГИСТРАЦИОННЫХ ДАННЫХ ККТ					
9.1	Подача налогоплательщиком Оператору регистрации неверных сведений для регистрации ККТ	Н3	ККТ, ФД, АС ЭР ККТ (Ц)	Владелец ККТ указывает в заявлении на регистрацию ККТ ложные сведения о своей организации, о контрольно-кассовой технике с целью уклонения от налогообложения	В	Риск оценен, как «высокий» по причине распространенности правонарушений, основанных на искажении регистрационных данных (мошенничества «платеж в однодневку», «перекладывание налогов на соседа»)
9.2	Ввод в ККТ недостоверной регистрационной информации	Н3, Н3s	ККТ, ФД, АС ЭР ККТ (Ц,А)	Владелец ККТ, вероятно – в сговоре с сотрудником службы технической поддержки ККТ, вводит в АС ККТ неверные регистрационные данные	В	Риск оценен как «высокий» по причине распространенности правонарушений, основанных на искажении регистрационных данных
9.3	Нарушение целостности регистрационной информации при ее вводе в ККТ	Н3, Н3s	ККТ, ФД, АС ЭР ККТ (Ц,А)	Атака 9.3 полностью аналогична атаке 9.2 (и может выполняться одновременно с атакой 9.2), но отличается от атаки 9.2 объектом воздействия: в атаке 9.2 ложные данные вводятся в автоматизированную систему, а в атаке 9.3 – в ККТ	В	Риск оценен как «высокий» по причине распространенности правонарушений, основанных на искажении регистрационных данных
10	УГРОЗЫ ТЕХНИЧЕСКИМ СРЕДСТВАМ ДИСТАНЦИОННОЙ ПРОВЕРКИ ИСПРАВНОСТИ ККТ					

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
10.1	Нарушение целостности, неисправность технических средств проверки ККТ	H1i, H3, H3s	АРМ АС ЭР ККТ (Ц,А)	Технические средства проверки исправности ККТ (АРМ АС ЭР ККТ) могут быть выведены из строя, что приведет к невозможности проверки исправности ККТ, к регистрации неисправной ККТ или к регистрации ККТ без проверки исправности. Атака может осуществляться: 1) хакером из сетей общего пользования (H1i) 2) Специалистом оператора регистрации H3s, возможно, находящимся в сговоре с налогоплательщиком. Целью атаки может быть регистрация неисправной или содержащей закладку ККТ (с осуществлением впоследствии атак 1.1-1.4, 2.1-2.3, 3.2-3.4, 4.1 или 4.2)	С	Риск оценен как «средний», при этом оценка требует уточнения по мере внедрения АС ЭР ККТ
11	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЭР ККТ					
11.1	Перехват, нарушение конфиденциальности регистрационных данных	H1i	ККТ, АС ЭР ККТ (К)	Атака 11.1 аналогична атаке 6.3 с той разницей, что в качестве объекта атаки выступает трафик системы регистрации	С	Риск «средний» установлен условно. Реальный уровень риска определяется владельцем контрольно-кассовой

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						техники
11.2	Перехват, нарушение целостности (фальсификация) регистрационных данных	H1i, H3	ККТ, АС ЭР ККТ (Ц,А)	Применение сетевого перехватчика для модернизации регистрационных данных «на лету»	H	Риск «низкий» установлен условно. Сетевой перехват единичного сеанса перехвата сеанса регистрации ККТ данных с целями их модернизации представляется трудоемким и поэтому мало вероятным. Реальный уровень риска определяется владельцем контрольно-кассовой техники
11.3	Фальсификация регистрационной сессии. Подмена сетевого узла, регистрирующего ККТ	H1i, H3, H3s	ККТ, АС ЭР ККТ (Ц,А)	1) Перехват сеанса регистрации, применение «подставного» узла регистрации ККТ сетевым хакером H1i представляется мало вероятным за отсутствием мотива. 2) Подмена узла регистрации ККТ может осуществляться находящимися в сговоре нарушителями H3 и H3s с целями регистрации нелегитимной техники или	C	Риск оценен как «средний», при этом оценка требует уточнения по мере внедрения АС ЭР ККТ

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				внедрения закладки в ККТ. 3) Атака 11.3 может выполняться в комбинации с атакой 11.4, как сеанс «регистрации» техники с несертифицированным образцом модуля фискальной памяти		
11.4	Фальсификация регистрационной сессии. Подмена сетевого сервера АС ЭР ККТ (фишинг)	H1i, H3, H3s	ККТ, АС ЭР ККТ (Ц,А)	Подмена сервера в сеансе регистрации ККТ может выполняться по двум каналам: 1) для перехвата данных аутентификации клиента (атака «фишинг», выполняется хакером H1i) 2) для создания «параллельной» системы регистрации контрафактной ККТ или контрафактных МФП, выполняется налогоплательщиком H3, действующим в сговоре с представителем техобслуживания контрафактных продуктов (H3s), возможно – во взаимодействии с	С	Риск оценен как «средний», при этом оценка требует уточнения по мере внедрения АС ЭР ККТ

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				производителем контрафактных продуктов H1z		
11.5	Нарушение целостности АРМ АС ЭР ККТ, установка закладки из сети в процессе регистрации ККТ	H1i	АРМ АС ЭР ККТ (Ц,А)	Атака может осуществляться по ряду широко распространенных сценариев сетевой атаки на клиентское рабочее место. Меры защиты рассмотрены в разделе 7	H	Риск «низкий» установлен условно по причине, что атакуется единичное рабочее место. Оценка требует уточнения по мере внедрения АС ЭР ККТ
11.6	Несанкционированный доступ из сети, нарушение целостности, вирусопоражение АС ЭР ККТ, установка закладки из сети в АС ЭР ККТ	H1i	АС ЭР ККТ (Ц,А)	Атака может осуществляться по ряду широко распространенных сценариев сетевой атаки на информационные системы. Меры защиты рассмотрены в разделе 7	C	Риск оценен как «средний» на основе существующих практик эксплуатации крупных автоматизированных (информационных) систем. Оценка требует уточнения по мере внедрения АС ЭР ККТ
11.7	Перехват, нарушение конфиденциальности и целостности данных, передаваемый между Оператором регистрации и налоговыми органами	H1i	АС ЭР ККТ, ИР НО (Ц,А,К,Д)	Атака по своей природе аналогична атакам 11.1 и 11.2 с той разницей, что объектом атаки является сетевой трафик на звене передачи из АС ЭР ККТ в налоговые органы	B	Риск оценен как «высокий» на основе существующих практик эксплуатации крупных автоматизированных (информационных) систем. Оценка требует уточнения по мере внедрения АС ЭР ККТ

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
11.8	Подавление услуги АС ЭР ККТ	H1i	АС ЭР ККТ (Ц,Д)	Атака, выполняемая сетевым хакером по мотивам вандализма, шантажа, конкуренции с Оператором регистрации или с целями нанесения ущерба процессу регистрации контрольно-кассовой техники с целями вывода АС ЭР ККТ из строя, блокирования ее операций и сетевых взаимодействий	В	Риск оценен как «высокий» на том основании, что блокирование функции АС ЭР ККТ наносит ущерб одновременно крупной автоматизированной системе Оператора регистрации и большому количеству налогоплательщиков. Оценка требует уточнения по мере внедрения АС ЭР ККТ
11.9	Выпуск незарегистрированной и/или не соответствующей образцу модели, прошедшей одобрение типа, контрольно-кассовой техники с одновременным предоставлением фальсифицированных (фишинг) средств регистрации ККТ	H1z, H3s	ККТ, АС ЭР ККТ (Ц,Д)	Создание «собственной» системы регистрации для контрафактной продукции ККТ/МФП	В	Риск оценен как «высокий» на том основании, что в современной практике производства контрафактной продукции имеют место прецеденты создания инфраструктур «проверки» ее «подлинности. Следует предполагать, что производители массовой контрафактной продукции

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						позаботятся об «инфраструктуре» ее легализации. Оценка требует уточнения по мере внедрения АС ЭР ККТ
12	ЮРИДИЧЕСКИЕ РИСКИ ОПЕРАТОРА РЕГИСТРАЦИИ					
12.1	Отказ участником процесса регистрации ККТ от факта выполнения действия (операции)	Н1, Н3, Н3s	АС ЭР ККТ (Ц,А)	В ходе регистрации ККТ может использоваться значительное количество документов в электронной форме. В случае, если эти документы фальсифицируются налогоплательщиком, представителем техобслуживания или третьим лицом, юридическая ответственность за результат регистрации ККТ на основе недостоверных документов может быть адресована к АС ЭР ККТ (Оператору регистрации)	С	Риск оценен как «средний». Оценка требует уточнения по мере внедрения АС ЭР ККТ
12.2	Непризнание налогоплательщиком причин (фактов) отказа в регистрации ККТ	Н1, Н3, Н3s	АС ЭР ККТ (Ц,А)	Атака 12.2 отличается от 12.1 только формой юридической претензии (оспаривается не факт регистрации, а факт	Н	Риск оценен как «низкий» на том основании, что вероятность необоснованного отказа в

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
				отказа в регистрации)		регистрации ККТ представляется небольшой. Оценка требует уточнения по мере внедрения АС ЭР ККТ
13	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ОФД					
13.1	Подавление услуги АС ОФД	H1i	АС ОФД (Д)	Атака, выполняемая сетевым хакером по мотивам вандализма, шантажа, конкуренции с Оператором фискальных данных или с целями нанесения ущерба процессам фискального контроля	B	Риск оценен как «высокий» на том основании, что блокирование функции АС ОФД наносит ущерб одновременно государству и огромному числу покупателей и налогоплательщиков
13.2	Создание ложного сервера АС ОФД	H1z, H3s	АС ОФД (Ц,А)	Создание «частного» АС ОФД с целями создания иллюзии легализации работы с контрафактной техникой	C	Риск оценен как «средний». Оценка требует уточнения по мере внедрения АС ОФД
13.3	Создание ложного канала проверки фискального признака	H1z, H3s	АС ОФД (Ц,А)	Создание «частного» канала для проверки фискального признака контрафактной продукции с целями создания иллюзии легализации работы с контрафактной техникой	B	Риск оценен как «высокий» на основании существующей практики создания «частных» каналов проверки КПК для не сертифицированных моделей ЭКЛЗ. Оценка

№	Способ реализации угрозы (атака)	Субъект	Объект	Канал	Риск	Обоснование
						требует уточнения по мере внедрения АС ОФД
14	ЮРИДИЧЕСКИЕ РИСКИ ОПЕРАТОРА ФИСКАЛЬНЫХ ДАННЫХ					
14.1	Перенаправление к ОФД претензий покупателей в случае отказа владельца ККТ от фискального документа	Н1	АС ОФД (Ц,А)	В случае создания нелегитимного фискального документа Оператор фискальных данных, мнимо или в действительности причастный к его созданию, подпадает под претензию потерпевшего покупателя	В	Риск оценен как «высокий» на том основании, что претензии могут носить массовый характер. Оценка требует уточнения по мере внедрения АС ОФД
14.2	Претензия налогоплательщика в случае легализации ОФД фальшивого фискального документа	Н3	АС ОФД (Ц,А)	Атака 14.2 отличается от 14.1 1) субъектом (налогоплательщик вместо покупателя) 2) мотивом - претензиями могут являться не только ущербы, связанные с содержанием фискальных документов, но и факты необоснованных проверок, административных мер, штрафов, сопутствующих ущербов репутации и бизнесу налогоплательщика	В	Риск оценен как «высокий» на том основании, что претензии могут носить массовый характер. Оценка требует уточнения по мере внедрения АС ОФД

8. Анализ мер противодействия угрозам информационной безопасности фискальных данных, средств и систем обработки фискальных данных

8.1 Описание мер противодействия угрозам ИБ ФД, ККТ, АС ЭР ККТ, АС ОФД

Меры защиты от угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных целесообразно классифицировать

- по объекту защиты;
- по способу применения мер защиты;
- по отношению ко времени совершения угрожающего события.

Состав объектов защиты в настоящей Модели гроз представлен в разделе «1.4 Объекты защиты».

По способу применение меры защиты (методы обработки риска) классифицируются как организационные, включая правовые (О), организационно-технические, сочетающие организационные мероприятия с применением технических средств (ОТ) и технические (Т), среди которых необходимо выделить криптографические (К) меры защиты данных.

По отношению ко времени совершения угрожающего события среди мер обработки риска различают проактивные (предварительно выполняемые и профилактические), применяемые для устранения причин возникновения риска до начала эксплуатациииобъекта защиты, активные, оказывающие непосредственное противодействие угрожающим факторам, и реактивные, реализуемые после наступления угрожающего события.

В Таблице 2 приведены описания мер защиты фискальных данных, средств и систем обработки фискальных данных.

Таблица 2

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
	ПРОАКТИВНЫЕ МЕРЫ ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ			
П1	Требования к составу и структуре фискальных данных	О	Состав и структура фискальных документов должны быть регламентированы документами налоговых органов, имеющими силу норм прямого действия	Структура фискальных данных должна обеспечивать полную информационную базу для решения задач сбора налогов и задач расследования налоговых правонарушений
П2	Требования по учету/ идентификации фискальных данных	О	Каждый фискальный документ должен позволять идентифицировать: 1) документ и его номер; 2) владельца ККТ; 3) экземпляр ККТ. 4) экземпляр МФП. 5) дату и время составления документа. Для фискальных документов требования по идентификации, учету и хранению должны быть регламентированы в документах технического регулирования ККТ, имеющих силу норм прямого действия	Меры учета и идентификации фискальных данных должны обеспечивать 1) защиту от подмены фискальных документов и/или приписывания факта издания документа другому лицу 2) возможность идентификации программно-технического средства обработки фискальных данных, сформировавшего фискальный признак документа
П3	Требования безопасности ФД	О	Требования безопасности фискальных данных должны быть регламентированы документами технического регулирования для ККТ, имеющими силу норм прямого	Требования безопасности фискальных данных должны идентифицировать защищаемые данные, устанавливать для них нормы аутентификации, целостности, конфиденциальности и определять

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			действия	механизмы безопасности, применяемые для этих целей
П4	Нормативно-правовая база деятельности налогоплательщика	О	Должна определять правовое обеспечение организационно-технических мер регламента эксплуатации ККТ	Должна включать меры ответственности налогоплательщика за нарушения безопасности фискальных данных в зоне обработки ФД в ККТ налогоплательщика
П5	Нормативно-правовая база и меры стимулирования контроля подлинности фискальных документов со стороны покупателя	О	Должна определять правовое обеспечение мер контроля целостности фискальных документов со стороны покупателя	Должна включать меры стимулирования контроля со стороны покупателя и определять технические требования к услугам проверки фискальных документов
	ПРОАКТИВНЫЕ МЕРЫ ЗАЩИТЫ СРЕДСТВ ФОРМИРОВАНИЯ ФИСКАЛЬНЫХ ДАННЫХ (ККТ)			
П6	Требования к ККТ	О	Требования к ККТ должны быть регламентированы документами технического регулирования для ККТ, имеющими силу норм прямого действия	Требования к ККТ должны определять необходимый минимум функциональных, конструктивных, технических требований к ККТ, комплектующим ККТ, средствам печати и отображения информации, интерфейсам ввода-вывода, режимам функционирования и режимам хранения данных и других необходимых технических характеристик контрольно-кассовой техники
П7	Требования безопасности ККТ	О	Требования безопасности ККТ должны обеспечивать наличие в составе ККТ и у ОФД	Требования (критерии) безопасности являются неотъемлемым элементом всякой системы технического

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			необходимых средств активной защиты фискальных данных и механизмов, обеспечивающих применение реактивных мер защиты. Состав требований определяется ориентировочно перечнем активных мер защиты фискальных данных А1-А5, активной защиты ККТ А6-А11 и требованиями к обеспечению безопасности при регистрации ККТ А12-А18. Требования безопасности ККТ должны быть установлены нормативными правовыми актами. Требования безопасности ККТ должны быть опубликованы для сведения Поставщиков ККТ, Представителей Поставщиков ККТ, Операторов Регистрации ККТ и Операторов Фискальных Данных	регулирования в области информационной безопасности. Публикация требований безопасности ККТ является необходимой организационной мерой защиты фискальных данных. Опубликованные требования безопасности ККТ не могут гарантировать стойкость мер защиты в случае существенного возрастания какого-либо из рисков или появления новых рисков. В этом случае в требования безопасности ККТ должны вноситься необходимые изменения. Требования безопасности ККТ должны применяться в обязательном порядке всеми лицами, осуществляющими разработку и производство ККТ, а также оборудования, применяемого ОФД
П8	Требования безопасности МФП	ОТ	Требования безопасности МФП должны обеспечивать наличие у модуля фискальной памяти минимально необходимого	Требования (критерии) безопасности являются неотъемлемым элементом всякой системы технического регулирования в области

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			перечня функций, обеспечивающих техническую и криптографическую защиту информации. Состав требований определяется перечнем мер криптографической защиты фискальных данных А1-А5, требованиями к производству СКЗИ [5], требованиями к функциональности СКЗИ и СКЗФД [6,7]. Требования безопасности МФП должны быть установлены нормативными правовыми актами. Требования безопасности МФП могут являться составной частью требований безопасности ККТ. Требования безопасности МФП должны быть опубликованы для сведения Поставщиков ККТ, Поставщиков МФП, Операторов регистрации ККТ и Операторов фискальных данных	информационной безопасности. Публикация требований безопасности МФП является необходимой организационной мерой защиты фискальных данных. Опубликованные требования безопасности МФП не могут гарантировать стойкость мер защиты в случае существенного возрастания какого-либо из рисков или появления новых рисков. В этом случае в требования безопасности МФП должны вноситься необходимые изменения. Требования безопасности МФП должны применяться в обязательном порядке всеми лицами, осуществляющими разработку и производство МФП, ККТ, а также оборудования, применяемого ОФД.
П9	Система оценки соответствия ККТ требованиям безопасности	ОТ	Система оценки соответствия ККТ требованиям безопасности ККТ должна подтверждать	Система оценки соответствия ККТ требованиям безопасности ККТ должна выдавать заключение о

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
	ККТ (одобрения типа ККТ)		стойкость реализованных в модели ККТ механизмов защиты фискальных данных в соответствии с требованиями безопасности ККТ П7. Сведения о модели ККТ, соответствующей требованиям, должны быть опубликованы для сведения Пользователей ККТ от имени уполномоченного федерального органа исполнительной власти. Например, в виде сведений о ККТ, включенной в Государственный реестр контрольно-кассовой техники.	соответствии для каждой модели ККТ. Минимально необходимый механизм подтверждения соответствия ККТ – тематические исследование МФП в составе модели ККТ на отсутствие негативных влияний программно-аппаратных средств ККТ на МФП
П10	Система оценки соответствия МФП требованиям безопасности МФП	ОТ	Система оценки соответствия МФП требованиям безопасности МФП должна подтверждать стойкость реализованных в модели МФП механизмов защиты фискальных данных в соответствии с требованиями безопасности МФП П8. Сведения о модели МФП, соответствующей требованиям, должны быть опубликованы для сведения Поставщиков ККТ.	Система оценки соответствия МФП требованиям безопасности МФП должна выдавать заключение о соответствии для каждой модели МФП. Минимально необходимый механизм подтверждения соответствия МФП – тематические исследование МФП в порядке, установленном для СКЗФД

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			Например, помещены в перечень СКЗФД, на которые ФСБ России выдан сертификат соответствия.	
П11	Регламент эксплуатации ККТ	О	Правила эксплуатации ККТ должны предписывать пользователю ККТ минимально необходимый и обязательный перечень действий, которые обеспечивают безопасность фискальных данных, в том числе: - ид ентификацию ККТ и МФП, включая проверку наличия модели ККТ в Государственном реестре ККТ (П9) и модели МФП в перечне сведений о сертифицированных СКЗИ (П10); - проверку исправности ККТ и МФП, включая проверку наличия доступа к системам или ресурсам для проверки исправности ККТ и МФП; - регистрацию ККТ в налоговых органах и перевода ККТ в фискальный режим, включая проверку достоверности фискального признака и иных реквизитов, печатаемых ККТ на	Правила эксплуатации ККТ должны базироваться на требованиях действующего законодательства РФ и быть закреплены в нормативных правовых актах, регламентирующих применение ККТ (П4, П6-П8).

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			кассовом чеке; - правила формирования, обработки, хранения и передачи фискальных данных, включая проверку доступа к ресурсам ОФД	
П12	Регламент аудита безопасности ККТ	О	Система правил мониторинга и аудита безопасности, выполняемых ОФД и налоговыми органами с целями выявления нарушений целостности фискальных данных и налогового законодательства	Регламент аудита безопасности ККТ должен быть согласован с техническими мерами мониторинга аномальных активностей ККТ А20, А31, аудита безопасности ККТ Р1, Р3, Р5 и предусматривать периодическую публикацию налоговыми органами результатов аудита безопасности ККТ в целях профилактики массовых попыток подвергнуть сомнению действенность принятых мер по обеспечению безопасности фискальных данных
П13	Нормативно-правовая база деятельности поставщиков ККТ и комплектующих	О	Должна быть разработана в качестве правового обеспечения деятельности поставщиков продукции на рынок ККТ	Должна включать порядок допуска продукции на рынок и определять меры ответственности поставщика ККТ (комплектующих ККТ) и налогоплательщика за поставку (применение) контрафактной продукции
	ПРОАКТИВНЫЕ МЕРЫ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ			

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
П14	Требования к АС ЭР ККТ и АС ОФД	О	Требования к функциональности автоматизированных систем регистрации ККИ, сбора и обработки фискальных данных должны быть утверждены налоговыми органами	Требования к АС ЭР ККТ и АС ОФД должны определять необходимый минимум функциональных требований, требований к форматам данных, протоколам обмена данными, программным интерфейсам, режимам функционирования АС и других необходимых технических характеристик, обеспечивающих возможности разработки, системной интеграции, совместимости ККТ, АРС АС ЭР ККТ и серверных компонентов АС ЭР ККТ и АС ОФД
П15	Требования безопасности АС ЭР ККТ	О	Требования безопасности АС ЭР ККТ должны быть 1) регламентированы документами налоговых органов 2) отражены в системах одобрения типа ККТ (П9, П10) и регламентах эксплуатации (П11, П12, П17) в виде документов, имеющими силу норм прямого действия	Требования безопасности АС ЭР ККТ должны исключать возможность регистрации контрафактной ККТ, которая могла бы использоваться для совершения налоговых правонарушений путем выполнения атак на целостность и аутентификацию фискальных данных, на целостность ККТ и комплектующих ККТ. В силу того, что сведения о парке контрольно-кассовой техники являются государственным информационным ресурсом, АС ЭР

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
				ККТ, вне зависимости от принадлежности к органам государственной власти и формы собственности Оператора регистрации, требования безопасности АС ЭР ККТ должны включать, не ограничиваясь, полный состав требований, изложенных в Приказе ФСТЭК России [12]
П16	Требования безопасности АС ОФД	О	Требования безопасности АС ОФД должны быть 1) регламентированы документами налоговых органов 2) отражены в системах одобрения типа ККТ (П9, П10) и регламентах эксплуатации (П11, П12, П18) в виде документов, имеющими силу норм прямого действия	Требования безопасности АС ОФД должны исключать возможность фальсификации и изъятия фискальных данных из учета. В силу того, что фискальные данные используются в качестве исходных данных при формировании ряда государственных информационных ресурсов, АС ОФД, вне зависимости от принадлежности к органам государственной власти и формы собственности Оператора фискальных данных, требования безопасности АС ОФД должны включать, не ограничиваясь, полный состав требований, изложенных в Приказе ФСТЭК России [12]
П17	Регламент предоставления услуг Оператором	О	Система правил, в соответствии с которыми предоставляется	Регламент регистрации ККТ должен быть разработан с учетом требований

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
	Регистрации ККТ		услуга регистрации контрольно-кассовой техники. Регламент предоставления услуг ОР ККТ должен обеспечивать выполнение мер защиты парка ККТ от применения контрафактной продукции и включать организационно-технические меры, позволяющие выявить нарушения, а также и доказательно расследовать спорные вопросы во взаимоотношениях между налогоплательщиком, ОР и налоговыми органами	системы оценки соответствия ККТ требованиям безопасности ККТ (одобрения типа ККТ) П9 и системы оценки соответствия МФП требованиям безопасности МФП П10 и правил ведения Государственного реестра контрольно-кассовой техники
П18	Регламент предоставления услуг Оператором фискальных данных	О	Система правил, в соответствии с которыми предоставляются услуга сбора и контроля фискальных данных. Регламент предоставления услуг ОФД должен обеспечивать выполнение норм налоговых органов по собираемости налогов с учётом выполненных расчетов, осуществления налогового контроля и выявления налоговых правонарушений, а также	Правила регламента услуги ОФД должны базироваться на требованиях действующего законодательства РФ об осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			доказательно расследовать спорные вопросы во взаимоотношениях между покупателем, налогоплательщиком, ОФД и налоговыми органами	
П19	Мониторинг и аудит работы АС	ОТ	Составной частью требований безопасности автоматизированных систем должны быть технические требования на подсистемы мониторинга и аудита событий информационной безопасности при эксплуатации АС, позволяющие зарегистрировать событие, обеспечить реагирование на него (см. меры защиты А20, А31, А32, Р1, Р3, Р6, Р7) и провести расследование с возможностью определения персональной ответственности участников события	Для решения задач мониторинга и аудита событий безопасности должны использоваться: 1) системы идентификаторов и персональных учетных записей, уровень детализации которых позволяет персонализовать ответственность операторов и участников процессов 2) состав сведений, достаточный для расследования инцидентов информационной безопасности 3) юридически значимые документы в тех зонах, где производится документирование этапов технологического процесса
П20	Разделение прав доступа на пользование, администрирование, аудит	ОТ	Для организации персональной ответственности и защиты данных мониторинга и аудита информационной безопасности от несанкционированной модернизации, рекомендуется	Система контроля доступа АС должна препятствовать воздействию операторов каждой из перечисленных ролевых групп на информационные ресурсы, подчиненные другой ролевой группе

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			построение управления АС на принципах ролевого управления и разделение функций администратора (управление системой и ее ресурсами), оператора (исполнение целевых функций автоматизированной системы) и аудитора (управление системами и информационными ресурсами систем событийного протоколирования)	
П21	Нормативно-правовая база деятельности Операторов	О	Должна быть разработана в качестве правового обеспечения эксплуатации автоматизированных систем	Должна включать действенные меры ответственности нарушителей информационной безопасности фискальных данных, средств и систем обработки фискальных данных
	АКТИВНЫЕ МЕРЫ ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ			
А1	Присвоение ФП	Т	Присвоение фискального признака – основная мера аутентификации источника данных и защиты целостности фискального документа. В зону защиты ФП должны включаться все значимые поля фискального документа, включающие, как минимум: 1) сведения о расчетной	Меры защиты фискальных данных должны быть унифицированы и применяться для всех типов ККТ

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			операции; 2) сведения о владельце ККТ; 3) сведения об экземпляре ККТ (МФП), сформировавшем фискальный признак; 4) сведения о времени выполнения расчетной операции	
А2	Механизмы формирования ФП	ОТ	Для присвоения фискального признака могут применяться методы как симметричной, так и асимметричной криптографии,: - фискальный признак неотъемлем от защищаемого документа - фискальный признак должен непредсказуемо изменяться при минимальном (1 бит информации) изменения защищаемого документа - фискальных признак формируется при помощи секрета, известного только формирующему фискальный признак МФП и, при необходимости, серверу, обеспечивающему проверку ФП), тем самым обеспечивается аутентификация источника	Механизмы формирования и проверки фискального признака должны быть реализованы криптографическими механизмами, прошедшими оценку стойкости в соответствии с требованиями ФСБ России для средств защиты фискальных данных [6,7]

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			данных	
А3	Обеспечение целостности потока фискальных документов	Т	Помимо мер защиты единичных фискальных документов путем присвоения фискального признака (А1) должны применяться меры криптографической защиты потока фискальных данных, обеспечивающие: 1) невозможность изъятия одного или нескольких фискальных документов из целостного потока без обнаружения факта изъятия 2) невозможность помещения в поток одного или нескольких фискальных документов без обнаружения этого факта 3) невозможность повторной передачи ранее созданного документа, как нового элемента потока	Меры защиты фискальных данных должны быть унифицированы и применяться для всех типов ККТ
А4	Обеспечение конфиденциальности сообщений или канала передачи данных	Т	При передаче фискальных данных по сетям общего пользования должны применяться меры криптографической защиты, обеспечивающие, при	Меры защиты фискальных данных должны быть унифицированы и применяться для всех типов ККТ. Должен быть утвержден и опубликован протокол обмена фискальными данными между ККТ и

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			необходимости, конфиденциальность передаваемой информации (шифрование сообщений или потока данных), целостность передаваемой информации и аутентификацию участников сетевого взаимодействия	ОФД (налоговыми органами)
А5	Дополнительная защита электронного чека	Т	Для электронных фискальных документов в циклах обработки фискальных данных, исключающих формирование бумажного документа, помимо мер защиты А1-А4 должны применяться меры защиты, придающие электронному фискальному документу статус равнозначного документу на бумажном носителе с собственноручной подписью (квалифицированная электронная подпись) а также меры, позволяющие однозначно аутентифицировать получателя кассового чека как лица, с которым осуществлялся расчет	Мера защиты только для ККТ, формирующей электронный чек (в случае введения оборота фискальных документов в электронном виде без выдачи кассового чека на бумажном носителе)
	АКТИВНЫЕ МЕРЫ ЗАЩИТЫ СРЕДСТВ ФОРМИРОВАНИЯ ФИСКАЛЬНЫХ ДАННЫХ (ККТ)			
А6	Физическая защита ККТ	Т	Для ККТ типа «ККМ» или	Для ККТ типа «ЭВМ, в том числе

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			«ЭВМ, в том числе персональная», накопитель фискальной памяти и средства формирования фискального признака (МФП) должны находиться в едином корпусе, для которого должны предприниматься следующие меры защиты: 1) Корпус ККТ в исполнении, исключающем доступ к внутренним модулям ККТ без вскрытия марки-пломбы. 2) Марка-пломба	персональная» и «программно-технический корпус» допускается размещение устройства ККТ в нескольких автономных функциональных модулях. В этом случае требования защиты корпуса предъявляются только к модулю, в котором помещается модуль фискальной памяти с принтером
А7	Защита целостности программно-аппаратных средств ККТ	Т	Для ККТ всех типов должны предприниматься следующие меры защиты целостности программно-аппаратных средств: 1) Проверка одобрения типа модели ККТ при ее регистрации (А14, А15). 2) Контроль исправности при регистрации (А16). 3) Установка или проверка целостности физической защиты корпуса (при регистрации и периодически, (А17). 4) Самотестирование ,	В процессе эксплуатации ККТ должны обеспечиваться плановые и, при необходимости, оперативные меры контроля целостности программно - аппаратных средств ККТ. Защиту среды функционирования ПО ККТ (с выявлением и блокированием подозрительного программного кода, антивирус, анти-spyware) следует считать рекомендательной мерой для всех типов ККТ, однако, в зависимости от конструкции и условий эксплуатации ККТ,

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			статический контроль версии и проверка целостности ПО ККТ при включении ККТ и загрузке ПО ККТ. 5) Меры защиты от установки программной закладки во время работы ККТ (динамический контроль целостности ПО и среды функционирования ПО ККТ с выявлением и блокированием подозрительного программного кода, антивирус, анти-spyware) – опционально, с учетом конструкции ККТ и условий эксплуатации	допускается ослабление этих требований, если обеспечивается изоляция сетевой среды эксплуатации ККТ и/или применение внешних по отношению к ККТ средств защиты
А8	Защита целостности МФП	Т	Для ККТ всех типов должны предприниматься следующие меры защиты целостности МФП: 1) Проверка документов об одобрении типа МФП при регистрации ККТ (А15). 2) Контроль целостности корпуса МФП, маркировки, сроков эксплуатации (в составе проверки А17, если производится вскрытие корпуса ККТ). 3) Проверка исправности ККТ,	В процессе эксплуатации ККТ должны обеспечиваться плановые и, при необходимости, оперативные меры контроля наличия, исправности и целостности МФП в составе ККТ

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			включающая проверку фискального признака «нулевого» чека (А16). 4) Регулярная проверка фискального признака Оператором фискальных данных в ходе передачи фискальных данных (А19)	
А9	Защита регистрационных данных ККТ		Регистрационные данные ККТ должны вводиться в ККТ при переводе ККТ в фискальный режимЦелостность регистрационных данных должна обеспечиваться следующими мерами: 1) Регистрационные данные должны проверяться в ходе регистрации ККТ (А13). 2) Регистрационные данные ККТ должны храниться в МФП с применением криптографических мер обеспечения некорректируемости данных. 2) Регистрационные данные ККТ включаются в первичные фискальные документы и в зону защиты фискального признака	Регистрационные данные, подлежащие защите, должны включать (не ограничиваясь): 1) Сведения о налогоплательщике (ИНН). 2) Сведения о модели ККТ по идентификационному номеру в Госреестре ККТ. (Для ККТ типа «программно-технический комплекс» в качестве идентификатора модели должны учитываться наименование и номер версии ПО ККТ). 3) Заводской номер ККТ. (Для ККТ типа «программно-технический комплекс» в качестве заводского номера должен учитываться номер лицензии ПО ККТ). 4) Сведения об МФП. 5) Заводской номер МФП. 6) Дата и время регистрации.

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			(А1), поверяются при каждом акте передачи фискального документа (А19) к оператору фискальных данных (в налоговые органы)	7) Исполнитель (представитель поставщика ККТ или Оператора регистрации, выполнивший проверки)
А10	Защита регистрационных данных МФП	Т	Защита (целостность) регистрационных данных МФП должна обеспечиваться следующими мерами: 1) Регистрационные данные МФП должны храниться в МФП. 2) Регистрационные данные МФП должны однозначно соответствовать ключевому документу СКЗФД. Ключевой документ СКЗФД каждого МФП должен использоваться для аутентификации образца ККТ и проверки фискального признака (А19)	Меры защиты МФП должны применяться для всех типов ККТ
А11	Механизм защиты сведений о времени выполнения операции	Т	Сведения о времени, включаемые в фискальный документ, должны быть защищены криптографически (см. меру защиты А6, А11). Источником сведений о времени должны быть доверенные часы реального времени, работающие	Регистрация достоверного времени проведения расчетной операции является обязательным требованием для всех типов ККТ

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			в доверенной среде	
	АКТИВНЫЕ МЕРЫ ЗАЩИТЫ АС ЭР ККТ			
А12	Аутентификация АРМ АС ЭР ККТ	Т	Технические средства, обеспечивающие проверку исправности ККТ и техническую поддержку регистрации ККТ на местах (АРМ АС ЭР ККТ) должны: 1) аутентифицироваться при подключении к АС ЭР ККТ при помощи индивидуальных для данного рабочего места (оператора) атрибутов аутентификации; 2)производить самотестирование и проверку целостности в начале работы	Функции проверки исправности ККТ, ввода регистрационных данных и перевода ККТ в фискальный режим имеют критическое влияние на весь процесс эксплуатации ККТ. Процедура электронной регистрации должна быть унифицирована для всех видов ККТ. Функции безопасности АРМ АС ЭР ККТ должны пройти оценку стойкости (аттестацию, сертификацию) в установленном порядке
А13	Контроль сведений о пользователе ККТ и регистрационных данных ККТ	ОТ	При регистрации ККТ налогоплательщик должен предъявить представителю налоговых органов или уполномоченному ими Оператору регистрации документы, удостоверяющие его, как юридическое лицо или индивидуального предпринимателя. Представитель налоговых	Представитель налоговых органов или уполномоченный ими Оператор регистрации должны под личную ответственность удостовериться в подлинности документов и аутентичности пользователя ККТ. При несоответствии сведений, пользователь ККТ должен получать отказ в регистрации его ККТ в налоговых органах. При работе с электронными

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			органов или уполномоченный ими Оператор регистрации должен удостовериться, что сведения о налогоплательщике и иные регистрационные данные ККТ корректно введены в ККТ и в некорректируемом виде сохранены в МФП. В электронном процессе регистрации для контроля сведений о пользователе ККТ может производиться проверка квалифицированной электронной подписи пользователя на заявлении о регистрации ККТ	документами средства квалифицированной электронной подписи должны соответствовать требованиям [19] и быть сертифицированы в установленном порядке
A14	Контроль соответствия типа ККТ	ОТ	При регистрации и переводе ККТ в фискальный режим пользователь ККТ должен предъявить представителю налоговых органов или уполномоченному ими Оператору регистрации регистрируемый образец контрольно-кассовой техники и имеющиеся для него свидетельства об одобрении типа модели ККТ. Для документов,	Соответствие модели ККТ образцу, включенному в Государственный реестр ККТ должно проводиться: 1) по результатам чтения регистрационных данных ККТ в автоматическом режиме; 2) по результатам сверки сведений о выпущенной продукции (ККТ, МФП); 3) по результатам осмотра внешнего вида и регистрационных знаков на корпусе ККТ. ККТ, не имеющая подтверждения ее

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			свидетельствующих об одобрении типа регистрируемой модели ККТ, представленных в электронном виде, допускается в качестве процедуры контроля проведение проверки квалифицированной электронной подписи поставщика ККТ и/или его уполномоченного представителя	соответствия требованиям безопасности (не включенная в Государственный реестр ККТ), должна получать отказ в регистрации в налоговых органах. Проверка электронных документов должна производиться средствами, удовлетворяющими требованиям [19] и сертифицированными в установленном порядке
A15	Контроль соответствия типа МФП	ОТ	При регистрации и переводе ККТ в фискальный режим пользователь ККТ должен предъявить представителю налоговых органов или уполномоченному ими Оператору регистрации в составе эксплуатационной документации на регистрируемый образец ККТ входящие в состав этой документации свидетельства о соответствии МФП установленным требованиям	Соответствие МФП установленным требованиям должно устанавливаться: 1) по результатам сверки сведений о выпущенной и сертифицированной продукции СКЗФД (МФП); 2) по результатам проверки исправности МФП (A16); 3) по результатам проверки документов, выполняющих функцию свидетельств соответствия. ККТ с МФП, не имеющим подтверждения его соответствия требованиям безопасности, должна получать отказ в регистрации в налоговых органах
A16	Контроль исправности ККТ	Т	При регистрации и переводе ККТ в фискальный режим	ККТ, не прошедшая проверку исправности, должна получать отказ

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			представитель налоговых органов или уполномоченный ими Оператор регистрации ККТ должен провести проверку исправности ККТ в соответствии с эксплуатационной документацией. В состав проверки должны входить: 1) функция блокировки формирования фискальных данных без перевода ККТ в фискальный режим; 2) проверка корректности регистрационных данных ККТ, зарегистрированных в МФП и их отображение на печатном документе; 3) проверка корректности выполнения ККТ функций ввода, вывода, отображения данных; 4) проверка полноты регистрируемых данных и соответствия требованиям по форматам и семантике данных; 5) проверка корректности регистрации данных путем печати «нулевого чека» и проверки его фискального	в регистрации в налоговых органах. Причины неисправности ККТ подлежат расследованию и, при обнаружении нарушений требований безопасности, сопровождаться применением к нарушителю мер ответственности. В случае, если свидетельства проверки исправности ККТ оформляются в виде электронных документов, защита и проверка этих электронных документов должна производиться средствами, удовлетворяющими требованиям [19] и сертифицированными в установленном порядке

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			признака. В случае, если контрольно-кассовая техника предназначена для передачи данных, в состав проверки исправности ККТ должны входить операции подсоединения ККТ в АС ОФД и проверка передачи фискальных данных от ККТ в АС ОФД	
А17	Проверка (установка) физической защиты ККТ	ОТ	Процедура регистрации и перевода ККТ в фискальные режим должна завершаться установкой физической защиты на корпуса тех частей ККТ, которые содержат средства ограничения доступа к ПО ККТ, принтер и МФП	Указанная мера защиты должна применяться для всех типов ККТ. Допускается применение адаптированных к конкретной модели средств и конструктивов физической защиты ККТ в случае одобрения их при включении модели ККТ в Государственный реестр контрольно-кассовой техники. В случае, если свидетельства установки средств физической защиты ККТ оформляются в виде электронных документов, защита и проверка этих электронных документов должна производиться средствами, удовлетворяющими требованиям [19] и сертифицированными в установленном порядке

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
А18	Целостность пространства доверия в системе регистрации	ОТ	Для предотвращения атак, основанных на одновременном создании контрафактной продукции ККТ и/или МФП и средств проверки их исправности и регистрации, пространство доверия (совокупность криптографических ключей и ключевых документов) должно основываться на едином мастер-ключе	Средства создания, хранения, проверки ключевых документов в составе ККТ и в составе АС ЭР ККТ для достижения целей единства пространства доверия и для обеспечения совместимости должны соответствовать требованиями ФСБ России к СКЗИ и СКЗФД [6,7] и быть сертифицированы в установленном порядке
	АКТИВНЫЕ МЕРЫ ЗАЩИТЫ АС ОФД			
А19	Проверка фискального признака при приеме данных	Т	При приеме фискальных данных в автоматизированной системе Оператора фискальных данных после снятия криптографической защиты канала передачи данных должны применяться меры проверки целостности фискальных данных с использованием механизмов контроля, предусмотренных мерами защиты А1-А4. В случае, если перечисленные проверки дали отрицательный результат – должны быть выработаны критерии, по которым должна выявляться и	Мера защиты применяется для всех типов ККТ. Средства проверки фискального признака должны соответствовать требованиями ФСБ России к СКЗИ и СКЗФД [6,7] и быть сертифицированы в установленном порядке

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			регистрироваться аномальная активность в зоне ответственности заданного налогоплательщика	
А20	Мониторинг аномалий активности ККТ	Т	В автоматизированной системе Оператора фискальных данных должна существовать подсистема мониторинга аномальной активности ККТ, обеспечивающая: 1) выявление событий, которые могут свидетельствовать о нарушениях или попытках нарушения фискальных данных, регистрация таких событий и уведомление операторов безопасности информационной системы о событиях такого рода. 2) накопление доказательной базы для проведения внеплановой проверки владельца ККТ	Мера защиты применяется для всех типов ККТ и всех категорий налогоплательщиков. При формировании электронных документов доказательной базы возможного налогового правонарушения рекомендуется оформление этих электронных документов производить средствами, удовлетворяющими требованиям [19] и сертифицированными в установленном порядке
А21	Целостность пространства доверия в системе сбора фискальных данных	ОТ	Для предотвращения атак, основанных на одновременном создании контрафактной продукции ККТ и/или МФП, создающих фальсифицированный	Средства создания и проверки фискального признака в составе ККТ и в составе АС ОФД для достижения целей единства пространства доверия и для обеспечения совместимости должны соответствовать

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			фискальный признак и средств проверки фискального признака, скрывающих факт фальсификации, пространство доверия (совокупность криптографических ключей и ключевых документов) для создания и проверки фискального признака должно основываться на едином мастер-ключе	требованиями ФСБ России к СКЗИ и СКЗФД [6,7] и быть сертифицированы в установленном порядке
	АКТИВНЫЕ МЕРЫ ЗАЩИТЫ АС (ОБЪЕДИНЕННЫЕ ТРЕБОВАНИЯ К АС ЭР ККТ И АС ОФД)			
А22	Взаимная аутентификация партнеров по сетевому взаимодействию	Т	Сетевые взаимодействия между клиентским и серверным оборудованием, между компонентами распределенной автоматизированной системы, между АС Операторов и налоговыми органами должны устанавливаться только в результате взаимной аутентификации партнеров по взаимодействию	Аутентификация партнеров по взаимодействию должна производиться криптографическими методами. Средства аутентификации сетевых объектов должны соответствовать требованиям ФСБ России к СКЗИ [6], средства аутентификации субъектов обработки фискальных данных должны также соответствовать требованиями ФСБ России к СКЗФД [7]. Все средства аутентификации должны быть сертифицированы в установленном порядке
А23	Защита сообщений,	Т	Требования конфиденциальности	Средства шифрования должны

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
	каналов связи		данных при передаче данных по сетям связи общего пользования должны обеспечиваться возможностью шифрования данных	соответствовать требованиями ФСБ России к СКЗИ [6], для средств защиты фискальных данных - должны также соответствовать требованиями ФСБ России к СКЗФД [7]. Все средства шифрования данных должны быть сертифицированы в установленном порядке
А24	Защита от несанкционированного доступа из сетей связи общего пользования	Т	Для сетевых объектов, представляющих собой клиентское рабочее место (терминал, АРМ) рекомендуется режим работы, в котором исключаются любые незащищенные (не аутентифицированные, не шифрованные) сетевые взаимодействия (режим изоляции сетевого взаимодействия). Для сетевых объектов (ЛВС, серверных компонентов АС и т.п.) также рекомендуется режим изоляции сетевых взаимодействий. В тех случаях, когда применение режима изоляции невозможно,	Средства защиты от несанкционированного доступа из сетей связи общего пользования должны быть сертифицированы ФСТЭК России и/или ФСБ России. В случае, если осуществляется защита от несанкционированного доступа к среде функционирования СКЗИ или СКЗФД и к средствам управления криптографическими ключами и ключевыми документами, средства защиты должны обязательно обладать сертификатом ФСБ России

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			необходимо применять следующие меры защиты: 1) межсетевые экраны для контроля доступа из сетей общего пользования 2) средства обнаружения вторжений (IDS) и/или противодействия вторжениям (IPS), контролирующие, в том числе, качество фильтрации межсетевых экранов	
А25	Защита от опасного мобильного кода	ОТ	Защита от опасного мобильного кода (вирусов, червей, spyware и т.п.) должна осуществляться: 1) в точках взаимодействия компонентов АС с сетями связи общего пользования, в которых может распространяться опасный мобильный код; 2) на шлюзах взаимодействия с внешними организациями 3) внутри и на границах сегментов локальных сетей; 4) на рабочих местах пользователей (в первую очередь – при применении съемных носителей данных)	Защита от опасного мобильного кода должна осуществляться на основе отдельной политики безопасности, разработанной применительно к конкретному объекту защиты (автоматизированной систем в целом) с учетом всех точек контроля (поступления опасного мобильного кода в систему). В случае, если осуществляется защита среды функционирования СКЗИ или СКЗФД или средств управления криптографическими ключами и ключевыми документами, средства антивирусной защиты должны быть сертифицированы ФСБ России

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
А26	Защита от атак типа «отказ в обслуживании»	Т	Автоматизированные системы (в первую очередь АС ОФД, которая в совокупности должна обрабатывать несколько миллионов чеков в сутки, [14]) должны быть защищены от атак на подавление услуги (DoS, DDoS). В качестве мер защиты от атак этого типа рекомендуется: 1) применение на входе в АС из сетей общего пользования специализированных средств противодействия атакам на отказ в доступе; 2) дизайн протоколов доступа, относительно устойчивый к атакам отказа в доступе, для криптографических протоколов – для атак повторной передачи легитимного сообщения; 3) резервирование инфраструктуры АС, в том числе диверсификация точек обработки, каналов доступа, применение средств балансирования сетевой нагрузки	Меры защиты рекомендуется проработать в составе технического проекта АС и сопроводить нагрузочными испытаниями при проведении приемки системы

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			4) контракт с коммуникационным провайдером, подразумевающий сотрудничество по предотвращению атак на отказ в доступе	
A27	Защита каналов управления и мониторинга	T	Каналы управления и мониторинга для оконечного оборудования и компонентов АС должны быть защищены от несанкционированного доступа, перехвата, искажения данных. Для каналов мониторинга должен контролироваться также факт отказа канала	Для построения систем управления и мониторинга АС рекомендуется применение выделенной защищенной подсети. Защита должна строиться при помощи средств криптографической защиты данных. Для доступа к среде управления/мониторинга рекомендуется использование отдельных (усиленных) средств аутентификации администраторов и выделенной группы криптографических ключей. Средства защиты сетей управления и мониторинга должны соответствовать требованиям ФСБ России к СКЗИ [6], для управления средствами и системами защиты фискальных данных, должны также соответствовать требованиям ФСБ России к СКЗФД [7]. Все средства шифрования данных должны быть

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
				сертифицированы в установленном порядке
А28	Меры защиты от прерывания процесса предоставления услуги	ОТ	Поскольку АС ЭР ККТ и АС ОФД являются системами массового обслуживания, построение мер защиты от атаки на доступность систем А26 должно сопровождаться разработкой и реализацией плана непрерывности предоставления услуг АС, включающего: - анализ рисков непрерывности предоставления услуги; - разработку требований непрерывности услуги; - проектирование технических решений и процессов с заданными параметрами доступности; - испытания, включая процессы восстановления доступности АС после реализации угроз непрерывности предоставления услуги; - подготовку и организацию деятельности персонала в период эксплуатации систем.	Требования доступности услуги должны быть сформулированы в технических заданиях на разработку систем. План обеспечения непрерывности предоставления услуги должен быть разработан на стадии разработки технического проекта
А29	Защита от потерь данных	ОТ	Для накопителей, носителей и	Требования по обеспечению

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
	(обеспечение доступности данных при их хранении)		хранилищ данных должны быть рассмотрены меры их безопасности на случай аварии, отказа систем, порчи носителей и т.п., такие как - требования по эксплуатации и хранению носителей и накопителей информации; - распределенное хранение данных, репликация баз данных в резервных хранилищах; - процессы резервного копирования и восстановления данных	безопасности данных от стихийных и деструктивных воздействий, нормы эксплуатации и хранения данных, должны отражаться в технических заданиях на разработку систем, регламентах эксплуатации систем и в нормативно-правовой базе, предусматривающей ответственность владельца критичных данных за их доступность при хранении. Носители фискальных данных, дополнительно к перечисленным требованиям, должны отвечать требованиям по защите данных от деструктивных воздействий при их хранении, изложенные в [7]
A30	Применение катастрофоустойчивых архитектур АС	ОТ	В разделах требований по надежности, доступности услуги, доступности данных при их хранении для систем массового обслуживания федерального масштаба целесообразно рассмотреть требования катастрофоустойчивости центров обработки данных	Требования по обеспечению катастрофоустойчивости АС должны отражаться в технических заданиях на разработку систем и в нормативно-правовой базе, предусматривающей ответственность владельца АС за обеспечение катастрофоустойчивости АС
A31	Мониторинг и аудит безопасности АС в реальном времени	ОТ	Автоматизированные системы, в качестве отдельных подсистем, должны включать средства	Подсистемы мониторинга, событийного протоколирования и аудита информационной

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			мониторинга, событийного протоколирования и аудита информационной безопасности, обеспечивающие: - накопление сведений о событиях (инцидентах) информационной безопасности; - возможность поиска и анализа данных, формирования отчетов по выборкам; - возможность построения на основе данных мониторинга и аудита систем сигнализации и автоматического реагирования на угрозы информационной безопасности	безопасности должны строиться с учетом требований на меры защиты П19, П20, А20, А23, А24, А27. При этом рекомендуется применение сертифицированных средств защиты информации
А32	Контроль подлинности электронных документов	Т	При работе автоматизированных систем документы, получаемые в результате электронной процедуры, должны обладать юридической силой, равнозначной силе документа на бумаге с собственноручной подписью. Исключения из этого правила могут составлять документы, создаваемые и потребляемые одним и тем же юридическим лицом или те	При формировании электронных документов, которые могут использоваться в качестве доказательной базы при расследовании конфликта хозяйствующих субъектов или возможного правонарушения, рекомендуется оформление этих электронных документов производить средствами, удовлетворяющими требованиям [19] и сертифицированными в

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			документы, заключения по которым не составляют или с малой вероятностью составляют предмет конфликта сторон, участвующих в автоматизированном процессе	установленном порядке
А33	Защита от внутренних угроз	ОТ	При проектировании и вводе в эксплуатацию АС ЭР ККТ и АС ОФД должны быть решены задачи: - классификации информационных ресурсов и объектов защиты; - анализа угроз информационной безопасности для этих объектов и ресурсов от естественных, стихийных и субъективных угроз, а также угроз, возникающих со стороны персонала эксплуатации АС; - разработки требований безопасности и архитектуры системы обеспечение безопасности информации - построения систем управления СОБИ и процессов управления безопасностью в масштабах АС	Организация внутренних процессов эксплуатации АС и защита от угроз информационной безопасности, проистекающих от персонала, эксплуатирующего АС, детально проработана в Концепции безопасности ФНС России [1], положения которой следует рекомендовать или директивно внедрить при вводе в эксплуатацию автоматизированных систем Оператора регистрации и Оператора фискальных данных, действующих в интересах ФНС России и поставляющих данные для информационных ресурсов ФНС России
	РЕАКТИВНЫЕ МЕРЫ ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ			

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
Р1	Контрольная работа налоговых органов	ОТ	Данные АС ЭР ККТ и АС ЭР ОФД составляют информационную базу нового порядка контрольной работы налоговых органов. Инциденты информационной безопасности, такие как несоответствие фискального признака, нарушение целостности фискальных данных, наряду со сбором статистики о работе налогоплательщиков могут прямо указывать на потенциальные источники налоговых правонарушений и тем самым значительно увеличивать адресность и эффективность контрольной работы налоговых органов	Особый вклад в информационную базу контрольной работы ФНС России должны вносить инциденты безопасности, связанные с мерами защиты А1, А3, А4, А9-А11, А12-А16, А19-А21. Оформление результатов проверки и свидетельств налоговых правонарушений в виде электронных документов целесообразно производить с применением меры защиты А32
Р2	Проверка чека покупателем	ОТ	Внедрение средств автоматизации гражданского контроля, когда покупатель может проверить факт учета, аутентичности и целостности выданного ему кассового чека	Результаты таких проверок могут автоматически анализироваться и использоваться в системе сбора статистики и оценки рисков совершения правонарушений налогоплательщиком (Р3). Оформление свидетельств (жалоб) покупателей в электронном виде целесообразно производить с

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
				применением меры защиты А32
Р3	Аналитические приложения на основе данных АС ОФД	Т	В составе АС ОФД должен быть разработан функциональный модуль анализа и прогнозирования налоговых правонарушений, обеспечивающий сбор статистики эксплуатации ККТ, выявление аномальных режимов эксплуатации ККТ и формирование ориентировок на проведение контрольных мероприятий налоговых органов	Ориентировки модуля анализа и прогнозирования налоговых правонарушений не должны носить характер прямого свидетельства, не должны обладать силой документов, равнозначных бумажному с собственноручной подписью, и не нуждаются в мерах технической защиты
	РЕАКТИВНЫХ МЕРЫ ЗАЩИТЫ СРЕДСТВ ФОРМИРОВАНИЯ ФИСКАЛЬНЫХ ДАННЫХ (ККТ)			
Р4	Плановые и внеплановые проверки парка ККТ налоговыми органами	О	Проверка технического состояния парка ККТ представителем налоговых органов в сочетании с проверкой первичной и консолидированной налоговой отчетности	Должна сочетаться с нормативной базой эксплуатации ККТ (П5, П11-П13, П17, П18, П21), предусматривающей ответственность налогоплательщика за ее ненадлежащую эксплуатацию
Р5	Технический аудит ККТ	ОТ	Проверка технического состояния отдельных образцов ККТ (работоспособности, целостности, состава операций) с анализом состояния технических средств, параметров функционирования и данных систем защиты ККТ	Проверке подлежат документы одобрения типа образцов ККТ и МФП, физическая защита ККТ, технические средства ККТ, обеспечивающие (ориентировочно) меры защиты режима проверки ККТ А1-А4, А19, а также регистрационные и фискальные

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
				данные, сохраненные в модуле фискальной памяти. Дополнительно должна производиться сверка этих сведений с данными АС ЭР ККТ, АС ОФД, налоговых органов и содержанием налоговой отчетности налогоплательщика
	РЕАКТИВНЫЕ МЕРЫ ЗАЩИТЫ АС (ОБЪЕДИНЕННЫЕ ТРЕБОВАНИЯ К АС ЭР ККТ И АС ОФД)			
Р6	Анализ событий эксплуатации систем, сбор статистики	О	Системы событийного протоколирования АС должны использоваться в качестве дополнительной информационной базы для решения задач мониторинга и аудита информационной безопасности	Для построения систем событийного протоколирования общего назначения рекомендуется применять тот же комплекс мер безопасности, что и для систем мониторинга и аудита информационной безопасности А20, А31
Р7	Расследование инцидентов информационной безопасности фискальных данных, средств и систем обработки фискальных данных	О	Возникновение инцидентов безопасности и подозрительных событий, выявляемых с использованием мер защиты А19, А20, А31-А33 и реактивными мерами Р2, Р3, Р5 должно расследоваться с целями 1) выяснения природы явления – имеет место нарушение (попытка нарушения) информационной безопасности или событие порождено нейтральными с	Применение мер ответственности должно регулироваться действующим законодательством и нормативно-правовой базой эксплуатации систем. Результаты расследования инцидентов информационной безопасности фискальных данных, средств и систем обработки фискальных данных должны учитываться при обновлении политик информационной

№	Наименование меры защиты	Тип	Механизм	Оценка стойкости, зона применения
			точки зрения безопасности обстоятельствами; 2) выяснения причин инцидентов; 3) определения ответственного и мер ответственности	безопасности автоматизированных систем с целями устранения уязвимостей
Р8	Сопровождение и обновление политик безопасности АС	ОТ	Эксплуатация АС должна сопровождаться постоянным анализом актуальности политик безопасности систем и средств защиты информации, полноты и действенности регламентов эксплуатации систем. Выявление новых угроз, уязвимостей систем должно являться предметом постоянно действующего процесса анализа актуальности действующих политик безопасности и их своевременного обновления	Для решения этих задач целесообразно организовать выделенную группу специалистов эксплуатации АС, ответственных за состояние информационной безопасности систем

8.1 Оценка эффективности мер противодействия угрозам информационной безопасности

Оценка эффективности мер противодействия угрозам информационной безопасности фискальных данных, технических средств и средств автоматизации фискального контроля приведена в таблице 3.

Таблица 3

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
1	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ НА ЭТАПАХ ПРОЕКТИРОВАНИЯ, ОДОБРЕНИЯ ТИПА И ПРОИЗВОДСТВА				
1.1	Ошибка проектирования, приводящая к появлению уязвимости ККТ	Н	Наличие руководств по проектированию ККТ в защищенном исполнении П3, П6, П7, П8 (включает требования к среде функционирования СКЗФД и тематические исследования на предмет отсутствия негативных влияний на СФК СКЗФД, которые проверяются в составе мер П9, П10). Активные проверки при регистрации ККТ А13-А17, проверки в ходе эксплуатации ККТ А19, Р2, технический аудит Р5, Р7	П	Меры проверки модели ККТ при включении в Госреестр ККТ, меры проверки исправности ККТ, оперативные проверки фискальных данных обеспечивают эффективное выявление ошибок проектирования ККТ

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
1.2	Преднамеренное внесение закладки недобросовестным разработчиком ККТ	Н(С)	Аудит безопасности ККТ П12 должен включать меры контроля целостности ККТ, в т.ч. проверки на отсутствие закладки. Активные меры защиты корпуса ККТ и программно-аппаратных средств ККТ А6-А8, проверки при регистрации ККТ А14-А16, проверка ФД А19 и мониторинга работы ККТ А20, аудит Р1, Р4, Р5 и проверки чеков Р2	П	Комплекс перечисленных мер безопасности обеспечивает высокую вероятность обнаружения вредоносной функциональности и выявления ее причин
1.3	Разработка закладки третьим лицом	В	Нормативно-правовая база деятельности поставщиков ККТ и комплектующих П13	С	Ввиду ажиотажного спроса на контрафактную продукцию ККТ следует предполагать, что нормативно-правовые меры, даже в случае применения к нарушителям уголовной ответственности, не обеспечат полное сдерживание активности криминального рынка. Поэтому, наряду с правовым регулированием П13, должен применяться (и нести основную сдерживающую функцию) комплекс эффективных мер выявления закладок и пресечения эксплуатации контрафактной продукции (см. 1.2)

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
1.4	Установка закладки в процессе производства, хранения, транспортировки продукции ККТ	Н	Те же меры, что используются для контроля целостности ККТ (см. 1.2)	П	См. 1.2
2	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ НА ЭТАПЕ РЕГИСТРАЦИИ ККТ				
2.1	Установка закладки в процессе приобретения, ввода в эксплуатацию, перевода ККТ в фискальный режим	В	Те же меры, что используются для контроля целостности ККТ (см. 1.2)	П	См. 1.2. Дополнительно должны включаться меры личной ответственности налогоплательщика и представителя поставщика ККТ, Оператора регистрации или налоговых органов, участвующего в проверке ККТ при ее регистрации (П4, П11, П12, П17, П21)
2.2	Регистрация в качестве ККТ техники, не прошедшей одобрение типа	В	Те же меры, что используются для контроля целостности ККТ при регистрации (см. 2.1)	П	См. 2.1
2.3	Нарушение правил проверки целостности и исправности ККТ при регистрации ККТ	В	Те же меры, что используются для контроля целостности ККТ при регистрации (см. 2.1)	П	См. 2.1
3	УГРОЗЫ ЦЕЛОСТНОСТИ ККТ И ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ ККТ НА ЭТАПЕ ЭКСПЛУАТАЦИИ ККТ				
3.1	Нарушение целостности корпуса (взлом физической защиты) ККТ	В	Нормативно-правовая база эксплуатации ККТ П4, П11, физическая защиты ККТ А6, меры проверок Р1, Р4, Р5	Н	Остаточный риск оценен как «низкий», поскольку угроза является постоянно действующей в течение длительного периода эксплуатации ККТ

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
3.2	Нарушение целостности программно-аппаратных средств ККТ	В	Те же меры, что используются для контроля целостности ККТ (см. 1.2)	Н	См. 1.2. Остаточный риск, в отличие от мер противодействия 1.2, оценен как «низкий», поскольку следует предполагать, что мотивация налогоплательщика к налоговому правонарушению, даже удельно невысокая, является постоянно действующим в течение длительного периода эксплуатации ККТ фактором угрозы и пренебрегать вероятностью налогового нарушения в этом случае невозможно. Поэтому особое внимание следует уделять мерам мониторинга и аудита
3.3	Нарушение целостности модуля фискальной памяти ККТ	С	Те же меры, что используются для контроля целостности ККТ при эксплуатации (см. 3.2)	Н	См. 3.2
3.4	Применение в составе ККТ контрафактных модулей фискальной памяти	С	Те же меры, что используются для контроля целостности ККТ при эксплуатации (см. 3.2)	Н	См. 3.2
3.5	Клонирование ККТ	В	Защита от клонирования ККТ, поскольку клон не будет регистрироваться и передавать фискальные данные в установленном порядке, не достижима путем применения требований к ККТ и мер защиты ККТ. Для выявления	С(Н)	Остаточный риск оценен, как «средний или низкий» по причине того, что выявление техники, не предъявляемой для официальных проверок и информационных взаимодействий, чрезвычайно затруднительно. Показатель «низкий риск» может быть достигнут при

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
			деятельности клонов необходимо применять меры мониторинга и аудита деятельности налогоплательщиков А20, А31 и полный комплекс реактивных мер контроля Р1-Р5. Но определяющее значение для достижения целей безопасности имеет проверка чеков покупателем Р2 при условии целостности пространства доверия средств формирования и проверки фискального признака А21		условии эффективных мер аудита. Большое значение имеют также нормативно-правовые документы «Регламент аудита безопасности ККТ» (П12), нормативно-правовая база и меры стимулирования контроля подлинности фискальных документов со стороны покупателя (П5)
4	СЕТЕВЫЕ УГРОЗЫ ЦЕЛОСТНОСТИ ККТ				
4.1	Взлом ККТ методами сетевого доступа	С	Требования безопасности ККТ П7 должны предусматривать либо полную изоляцию среды сетевого взаимодействия (отсутствие трафика в открытом виде) А3, А23, либо наличие в составе ККТ средств защиты от несанкционированного доступа из сети А4, А24	Н	Рекомендуется режим сетевой изоляции технических средств и систем, исключающий взаимодействие ККТ с объектами сетей связи общего пользования при помощи открытого трафика. В режиме полной изоляции ККТ остаточный риск может быть оценен, как «пренебрежимо малый»

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
4.2	Атаки на ККТ, выполняемые путем распространения опасного мобильного кода	Н	Меры безопасности, перечисленные для атаки 4.1	Н(П)	См. 4.1
4.3	Перехват каналов сетевого управления (конфигурирования) ККТ	В(С)	Для каналов мониторинга и управления должны применяться методы изоляции среды сетевого взаимодействия (отсутствие трафика в открытом виде) А3, А23	Н	См. 4.1
5	УГРОЗЫ ФИСКАЛЬНЫМ ДАННЫМ В ПРОЦЕССЕ ИХ ФОРМИРОВАНИЯ И ОБРАБОТКИ				
5.1	Манипуляции с чеками при их создании	В	Те же меры защиты, что и от атаки 3.5 «Клонирование ККТ»	С(Н)	См. 3.5
5.2	Фальсификация содержания чека	В	Для предотвращения атаки должны быть превентивно предприняты меры защиты целостности ККТ А6-А11, меры безопасности при регистрации ККТ А13-А17, среда проверки чеков должна находиться в едином пространстве доверия и обеспечивать совместимость СКЗФД в клиентской (ККТ) и серверной (АС ОФД) частях – А21. В оперативном порядке должны применяться меры проверки ФП при приеме данных в АС ОФД – А19. Как	П	Эффективное применение мер защиты А19 и Р2 при использовании сертифицированных средств защиты фискальных данных позволяют снизить риск до уровня «пренебрежимо малый»

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
			меры контроля должны применяться мониторинг функционирования ККТ А20, меры проверки чека покупателем Р2 и меры аудита по фактам нарушений Р1, Р3-Р7		
5.3	Фальсификация фискального признака чека	В	Меры защиты аналогичны применяемым для атаки 5.3	П	См. 5.3
5.4	Отложенное формирование или ревизия отчетности с изъятием полного состава (или части) фискальных данных	В(С)	Меры защиты аналогичны применяемым для атаки 5.3 при особом значении меры защиты А11 и мониторинга активности ККТ А20	Н	Доверенное время совершения операции целесообразно обеспечивать наличием доверенных часов реального времени в составе модуля фискальной памяти или другими мерами, которые должны найти отражение в требованиях безопасности ККТ П7, П8
5.5	Фальсификация электронного фискального документа	В	Меры защиты аналогичны применяемым для атаки 5.3 с дополнительным применением мер защиты П1-П3, активных мер защиты А5, А32	П	В случае корректного применения средств криптографической защиты риски искажения электронных документов представляются пренебрежимо малыми, а практика применения электронных документов – безопасной. При этом необходимо установить, как повсеместное, требование на обязательную выдачу покупателю печатного чека. Исключение могут

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
					составлять только системы платежей, в которых применение средств печати чеков технически невозможно. Такого рода исключения должны быть строго обоснованы и допускаются по особому разрешению налоговых органов
6	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИСКАЛЬНЫХ ДАННЫХ				
6.1	Любое нарушение целостности фискальных данных произвольным нарушителем из сети	Н	Меры защиты фискальных данных А1-А4, проверка целостности ФД А19, меры защиты каналов связи А22, А23	П	Дополнительно следует рекомендовать все прочие меры защиты от сетевых угроз ФД и АС. При корректном применении средств криптографической защиты фискальных данных риски искажения ФД пренебрежимо малы
6.2	Изъятие из потока (блокировка) или нарушение целостности фискальных данных недобросовестным налогоплательщиком на этапе их передачи от ККТ к ОФД	В	В числе прочих мер сетевой информационной безопасности особое значение имеет обеспечение целостности потока фискальных документов А3	П	При корректном применении средств криптографической защиты фискальных данных риски нарушения целостности потока фискальных данных пренебрежимо малы

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
6.3	Перехват (нарушение конфиденциальности) ФД на этапе их передачи от ККТ к ОФД	С	Защита фискальных данных, сообщений и каналов связи путем их шифрования А4, А23	П	При корректном применении средств криптографической защиты риски нарушения конфиденциальности данных пренебрежимо малы
6.4	Атаки на систему аутентификации участников сетевого взаимодействия	В	Аутентификация участников сетевого взаимодействия А1, А3, А22 (часто выполняется одновременно с А23)	П	При корректном применении средств криптографической защиты риски нарушения аутентификации и перехвата аутентифицированных взаимодействий пренебрежимо малы
6.5	Подавление сетевой активности ККТ	Н	Дополнительно к предлагаемому комплексу средств сетевой безопасности меры защиты отдельного образца ККТ от атак отказа в доступе не предлагаются	Н	В силу того, что атака на единичный образец ККТ мало вероятна, ограничена во времени и не оказывает существенного влияния на функционирование системы в целом, риск подавления отдельных образцов ККТ допустимо принять без обработки
7	УГРОЗЫ АС ЭР ККТ СО СТОРОНЫ ПОСТАВЩИКА ККТ				
7.1	Выпуск незарегистрированной продукции	В	Требования безопасности МФП П8, в составе прочих требований к средствам криптографической защиты фискальных данных, содержат требование поэкземплярного учета продукции. Эту организационную меру целесообразно сочетать с	С(Н)	Учет выпускаемой продукции ККТ и МФП в сочетании с мерами регулирования деятельности участников рынка П13 может существенно ограничить производство и применение контрафактной продукции. Оценка риска «низкий» может быть достигнута в случае эффективной

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
			учетом выпускаемой продукции ККТ в составе нормативно правовой базы П13, контролем сведений о ККТ А13 при регистрации ККТ и проверками Р1, Р3-Р5		организации контроля за выпуском продукции
7.2	Выпуск ККТ, не соответствующей образцу модели, прошедшей одобрение типа	В	Для защиты от выпуска контрафактной продукции с вредоносной функциональностью следует применять также весь комплекс мер защиты от угрозы 3.2	С(Н)	Оценка риска «низкий» может быть достигнута в случае эффективной организации контроля за выпуском продукции
7.3	Применение несертифицированных средств криптографической защиты фискальных данных	В	Комплекс мер защиты совпадает с 7.2	С(Н)	См. 7.2
8	УГРОЗЫ НАРУШЕНИЯ ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕГИСТРАЦИИ ККТ В АС ЭР ККТ				
8.1	Регистрация ККТ, не включенной в Государственный реестр	С	Комплекс мер защиты ККТ А6-А8 и проверок ККТ при регистрации А13-А17 обеспечивает эффективное выявление контрафактной техники	П	Учет продукции ККТ и МФП, наличие у МФП индивидуальных средств аутентификации и ключевых документов, целостность пространства доверия в системах электронной регистрации ККТ А18 и сбора фискальных данных А21, проверка исправности ККТ А16 с проверкой фискального признака

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
					«нулевого» чека практически исключают риск регистрации контрафактной техники
8.2	Регистрация неисправной контрольно-кассовой техники	С	Комплекс мер защиты совпадает с 8.1	П	См. 8.1
8.3	Регистрация ККТ без уведомления налоговых органов	С	Регистрация ККТ без уведомления налоговых органов, как и угрозы клонирования ККТ 3.5 и манипуляции с чеками опасны тем, что могут не оставлять следов в системах регистрации, мониторинга и аудита налоговых органов. Для устранения рисков от такого типа атак следует применять меры защиты от атаки 3.5	С(Н)	См. 3.5. Дополнительной мерой защиты от угрозы 8.3 является контроль за выпуском продукции. Для предотвращения атак регистрации ККТ без уведомления налоговых органов, выполняемых путем применения ложных автоматизированных систем регистрации и проверки фискального признака (угрозы 11.4, 11.9, 13.2 и 13.3) необходимы меры обеспечения целостности пространства доверия автоматизированных систем А18 и А21
8.4	Нарушение целостности корпуса ККТ при регистрации ККТ	С	Защитой от нарушения целостности корпуса ККТ при ее регистрации является комплекс мер защиты от атаки 3.1. Отличие атаки 8.4 от атаки 3.1 состоит в том, что в процессе	Н	В контексте атаки 8.4 марка-пломба выступает не только как препятствие для несанкционированного вскрытия корпуса ККТ, но и как критерий, по которому можно разграничить ответственность производителя ККТ, налогоплательщика и

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
			регистрации появляется дополнительный канал атаки - сговор между налогоплательщиком и специалистом техподдержки, осуществляющим операцию регистрации. В силу того, что угроза имеет коррупционную природу, ее риск всегда остается относительно высоким и требует применения мер Р1, Р4, Р5		представителя технической поддержки (Оператора регистрации)
8.5	Нарушение правил проверки целостности ККТ при регистрации ККТ	С	Для защиты от нарушений правил проверки целостности и регистрации ККТ необходимо предпринимать те же меры защиты, что используются для защиты от атаки 2.1. Отличие атаки 8.5 в наличии возможного канала коррупционного сговора между налогоплательщиком и представителем технической поддержки	Н	В отличие от атаки 2.1 риск оценен как «низкий», поскольку канал атаки связан с человеческим фактором. По этой же причине особое внимание следует уделить проверкам Р1, Р4, Р5
8.6	Оформление ложных регистрационных документов	Н	В случае оформления регистрационных документов в электронном виде следует применять меры защиты А32	Н(П)	В случае, если речь идет об оценке технических рисков – оценку риска следует принять как «пренебрежимо малый» в силу применения средств криптографической защиты

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
					информации. Однако для случаев, когда ложные документы оформляются в результате коррупционного сговора между налогоплательщиком и представителем технической поддержки, величину риска следует принять, как «низкий» и применять меры ответственности налогоплательщика и представителя техподдержки в соответствии с П4, П11, П21, Р1, Р4, Р5
9	УГРОЗЫ ЦЕЛОСТНОСТИ РЕГИСТРАЦИОННЫХ ДАННЫХ ККТ				
9.1	Подача налогоплательщиком Оператору регистрации неверных сведений для регистрации ККТ	В	В соответствии с регламентом регистрации ККТ, П17 должен выполняться контроль сведений о налогоплательщике А13	Н	В случае, если сведения о налогоплательщике подаются в виде бумажного документа, операция требует личного участия представителя техподдержки. Во избежание вовлечения представителя техподдержки в коррупционный сговор с налогоплательщиком, следует организовать меры ответственности налогоплательщика и представителя техподдержки в соответствии с П4, П11, П21 и реактивные проверки Р1, Р4, Р5

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
9.2	Ввод в ККТ недостоверной регистрационной информации	В	Технические средства ввода регистрационных данных в ККТ подлежат мерам защиты А12, А24-А26, А27-А29, А33	Н	Средства информационной безопасности технических средств проверки исправности ККТ и технической поддержки регистрации ККТ (АРМ АС ЭР ККТ) подлежат оценке (сертификации и аттестации) в установленном порядке. Во избежание вовлечения представителя техподдержки в коррупционный сговор с налогоплательщиком, следует организовать меры ответственности налогоплательщика и представителя техподдержки в соответствии с П4, П11, П21 и реактивные проверки Р1, Р4, Р5
9.3	Нарушение целостности регистрационной информации при ее вводе в ККТ	В	Меры защиты ККТ от нарушения целостности регистрационной информации должны обеспечиваться комплексом мер защиты, приведенным для атаки 9.2, а также применением мер защиты А7-А10	Н	См. 9.2
10	УГРОЗЫ ТЕХНИЧЕСКИМ СРЕДСТВАМ ДИСТАНЦИОННОЙ ПРОВЕРКИ ИСПРАВНОСТИ ККТ				

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
10.1	Нарушение целостности, неисправность технических средств проверки ККТ	С	Те же меры, что используются для защиты от атаки 9.3	Н	См. 9.3
11	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЭР ККТ				
11.1	Перехват, нарушение конфиденциальности регистрационных данных	С	Меры защиты каналов связи и сообщений А22, А23. Защита от внутренних атак А33	П	При корректном применении средств шифрования регистрационных данных риски нарушения их конфиденциальности пренебрежимо малы
11.2	Перехват, нарушение целостности (фальсификация) регистрационных данных	Н	Меры защиты каналов связи и сообщений А22, А24. Защита от внутренних атак А33	П	При корректном применении средств криптографической защиты риски искажения регистрационных данных пренебрежимо малы
11.3	Фальсификация регистрационной сессии. Подмена сетевого узла, регистрирующего ККТ	С	Те же меры, что используются для защиты от атаки 11.2	П	См. 11.2
11.4	Фальсификация регистрационной сессии. Подмена сетевого сервера АС ЭР ККТ (фишинг)	С	Те же меры, что используются для защиты от атаки 11.2. Дополнительно, для защиты от одновременного выпуска контрафактной продукции и создания ложных средств ее регистрации следует принять меры обеспечения целостности пространства доверия А18	Н	Риск повышен до оценки «низкий» (в сравнении с атакой 11.2) на том основании, что практика одновременного создания контрафактной продукции и средств ее «проверки» распространена на рынке ККТ в настоящее время

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
11.5	Нарушение целостности АРМ АС ЭР ККТ, установка закладки из сети в процессе регистрации ККТ	Н	Те же меры, что используются для защиты от атаки 9.2	П	См. 9.2
11.6	Несанкционированный доступ из сети, нарушение целостности, вирусопоражение АС ЭР ККТ, установка закладки из сети в АС ЭР ККТ	С	Технические средства ввода регистрационных данных в ККТ подлежат мерам защиты А12, А23-А26, А27-А29, А33	Н	См. примечание 9.2
11.7	Перехват, нарушение конфиденциальности и целостности данных, передаваемый между Оператором регистрации и налоговыми органами	В	Те же меры, что используются для защиты от атаки 11.1	П	См. 11.1
11.8	Подавление услуги АС ЭР ККТ	В	Дополнительно к мерам защиты от атак 11.5, 11.6 следует применять меры защиты А26, А28	С(Н)	Ввиду эффективности атак на отказ в обслуживании и отсутствия эффективных мер борьбы с ними, остаточный риск от этих атак всегда следует считать достаточно высоким
11.9	Выпуск незарегистрированной и/или не соответствующей образцу модели, прошедшей одобрение типа, контрольно-кассовой	В	Те же меры, что используются для защиты от атаки 11.4		См. 11.4

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
	техники с одновременным предоставлением фальсифицированных (фишинг) средств регистрации ККТ				
12	ЮРИДИЧЕСКИЕ РИСКИ ОПЕРАТОРА РЕГИСТРАЦИИ				
12.1	Отказ участником процесса регистрации ККТ от факта выполнения действия (операции)	С	Выполнение регламента регистрации ККТ П17, включающего комплекс мер защиты А6-А11 и комплекс проверок А13-А17, должно выполняться при помощи аутентифицированного терминала АРМ АС ЭР ККТ (А12) и с оформлением мер защиты электронных документов А32. В случае, если отдельные операции выполняются на различных этапах и/или различными участниками процесса, результаты атомарных операций должны оформляться в виде защищенных электронных документов, снабженных электронной подписью лица, ответственного за результат операции (А32)	Н	Регламент процесса электронной регистрации ККТ П17 должен быть построен так, чтобы можно было четко разграничить ответственность субъектов за выполнение атомарных операций в процессе регистрации. Деятельность Оператора регистрации должна соответствовать комплексу мер защиты от внутренних угроз А33. При документированном процессе с разделением ответственности риск отказа от выполнения операции следует признать низким

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
12.2	Непризнание налогоплательщиком причин (фактов) отказа в регистрации ККТ	Н	Те же меры, что используются для защиты от атаки 12.1	П	В случае, если документы, свидетельствующие об объективных причинах отказа в регистрации ККТ оформлены, как юридически значимые, риски судебного преследования налоговых органов со стороны налогоплательщика пренебрежимо малы
13	СЕТЕВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ОФД				
13.1	Подавление услуги АС ОФД	В	Те же меры, что используются для защиты от атаки 11.8	С(Н)	Применительно к АС ОФД атака на отказ в доступе (подавление услуги) является значительно более опасной, чем подавление услуги АС ЭР ККТ. Поэтому меры защиты А26 должны быть усилены резервированием инфраструктуры, мерами политики обеспечения непрерывности бизнес-процессов А28, мерами повышения доступности данных А29 и созданием резервированной и катастрофоустойчивой инфраструктуры А30, защиты от внутренних атак А33
13.2	Создание ложного сервера АС ОФД	С	Те же меры, что используются для защиты от атаки 6.4. Дополнительно – комплекс мер сетевой безопасности А22-А24	Н	См. 6.4

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
13.3	Создание ложного канала проверки фискального признака	В	Для предотвращения атак на систему сбора фискальных данных, выполняемых путем одновременного применения контрафактной ККТ и ложной АС ОФД, необходимы меры обеспечения целостности пространства доверия А18 и совместимость СКЗФД, применяемых в ККТ и в АС ОФД	Н	Средства управления криптографическими ключами и ключевыми документами должны соответствовать требованиям ФСБ России и быть сертифицированы в установленном порядке. Дополнительно требуется корректная организация контроля за составом парка ККТ (см. меры защиты от угроз 3.1-3.5), поскольку практика одновременного создания контрафактной продукции и средств «проверки» ее данных распространена в современной практике налоговых правонарушений
14	ЮРИДИЧЕСКИЕ РИСКИ ОПЕРАТОРА ФИСКАЛЬНЫХ ДАННЫХ				
14.1	Перенаправление к ОФД претензий покупателей в случае отказа владельца ККТ от фискального документа	В	Те же меры, что используются для защиты от атаки 12.1. Дополнительно – комплекс мер защиты фискальных данных А1-А3, А19, А21, А22, Р2	П	Риск пренебрежимо мал. В случае, если фискальный признак формируется в составе ККТ при помощи СКЗФД, сертифицированных в установленном порядке, покупатель может адресовать претензии исключительно к налогоплательщику

№	Способ реализации угрозы (атака)	Риск	Меры защиты	Ост. риск	Примечание
14.2	Претензия налогоплательщика в случае легализации ОФД фальшивого фискального документа	В	Меры защиты А1 и А19, выполняемые при помощи сертифицированных СКЗФД	П	В случае, если фискальный признак формируется СКЗФД в составе ККТ и ОФД производит проверку фискального признака каждого чека при его приеме от ККТ, возможность легализации ОФД ложного чека (и вытекающая из нее юридическая претензия) исключена

8.2 Заключение об эффективности мер защиты фискальных данных, средств и систем обработки фискальных

В результате проведенного анализа угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных, можно сделать следующие выводы:

1. Применение контрольно-кассовой техники с передачей данных дает ряд ощутимых преимуществ как для бизнеса, так и для осуществления контрольной работы налоговых органов. В то же время, подключение контрольно-кассовой техники к сетям связи общего пользования, расширение состава технических средств (включая так называемую мобильную и инновационную технику), выполнение электронной регистрации контрольно-кассовой техники без непосредственного присутствия представителей налоговых органов при осуществлении процесса регистрации – изменяют условия эксплуатации контрольно-кассовой техники, создают предпосылки для доступа к ней значительно большего количества нарушителей информационной безопасности и тем самым порождают ряд качественно новых угроз. Появление новых угроз, наряду с уже существующей масштабной криминальной индустрией, обслуживающей интересы налоговых правонарушителей, требует усиления мер защиты фискальных данных, средств и систем обработки фискальных данных.
2. Несмотря на то, что количество угроз информационной безопасности фискальных данных, средств и систем обработки фискальных данных в новом порядке применения ККТ увеличивается, их анализ показывает, что адекватные меры противодействия этим угрозам позволяют:
   - Обеспечить требуемый режим безопасности функционирования контрольно-кассовой техники с передачей данных.
   - Построить необходимые для эксплуатации контрольно-кассовой техники с передачей данных автоматизированные системы в защищенном исполнении.
   - Решить задачи качественно нового информационного обеспечения, построения систем риск-ориентированного анализа, повышения эффективности деятельности контрольной работы налоговых

органов за счет адресной ориентации проверок на потенциального налогового правонарушителя.

3. Важнейшим мотивом перехода к новому порядку применения контрольно-кассовой техники является снижение нагрузки на бизнес. Анализ показывает, что достигнуть перечисленных выше целей нового порядка применения ККТ можно без практического влияния на бюджет налогоплательщика, а по некоторым статьям – с возможным его сокращением. Решающим фактором сокращения издержек в экономике средств и систем фискального контроля является применение криптографических технологий, поскольку именно криптографические, в отличие от инженерно-технических, меры защиты информации обладают одновременно большей стойкостью и меньшей стоимостью.

4. Результаты анализа угроз информационной безопасности фискальных данных, средств и систем их обработки позволяют выделить следующие ключевые направления обеспечения безопасности нового порядка применения ККТ:

   – Контроль за отсутствием вредоносной функциональности в составе контрольно-кассовой техники, развитие системы одобрения типа ККТ, заложенной в основе Государственного реестра контрольно-кассовой техники, в направлении расширения функциональности ККТ, обеспечения передачи фискальных данных, применения инновационных платформ ККТ.

   – Внедрение государственной услуги и системы автоматизации электронной регистрации контрольно-кассовой техники, обеспечивающей на практике автоматизацию мер контроля Государственного реестра ККТ.

   – Обеспечение безопасности эксплуатации контрольно-кассовой техники с передачей данных и автоматизированных систем сбора и обработки фискальных данных.

   – Гармонизацию законодательства и нормативно-правовой базы для обеспечения нового порядка применения контрольно-кассовой техники.

Дальнейшие выводы детализируют результаты анализа угроз информационной безопасности фискальных данных, средств и систем их обработки применительно к этим ключевым направлениям.

5. В области контроля за парком применяемой ККТ наиболее актуальной угрозой безопасности средств обработки фискальных данных является разработка контрафактной продукции с функциями поддержки налоговых правонарушений. Главной защитой от этой угрозы является развитие мер одобрения типа ККТ, установленных в системе Государственного реестра ККТ, для применения в ККТ с передачей данных и в новых платформах ККТ. Поскольку новый порядок применения ККТ расширяет, не изменяя основ, функциональность ККТ, представляется возможным преемственное расширение требований существующей в рамках Государственного реестра системы контроля и автоматизация этого контроля для вновь вводимой услуги электронной регистрации ККТ. Основными принципами защиты от угроз применения вредоносной контрафактной продукции являются контроль за парком техники (обоснованное включение ККТ в Государственный реестр), учет выпускаемой продукции (в том числе поэкземплярный учет средств криптографической защиты фискальных данных), проверка исправности ККТ при ее регистрации.

6. Автоматизированная услуга электронной регистрации ККТ является одновременно важным фактором снижения нагрузки на бизнес и эффективным средством контроля за действующим парком ККТ. Наиболее актуальными угрозами средствам фискального контроля в этой области являются всякого рода способы нарушить целостность регистрируемой контрольно-кассовой техники или подменить модель одобренного типа контрафактным устройством с вредоносной функциональностью. Важнейшим элементом защиты на этом этапе является автоматизированная проверка исправности ККТ, которая может выполняться дистанционно и в автоматическом режиме. Однако некоторые функции, такие, как осмотр (контроль целостности) корпуса ККТ, контроль подлинности предъявленной модели ККТ, контроль подлинности сведений о налогоплательщике и документов ККТ, если эти документы представлены в бумажном виде,

– не поддаются полной автоматизации и потребуют присутствия представителя поставщика ККТ или специалиста Оператора регистрации.

7. На этапе эксплуатации ККТ, при выполнении регистрации информации о платежах и расчетах, более всего опасны манипуляции с чеками и фальсификация фискальных данных. В тех случаях, когда в результате налоговых правонарушений при выполнении расчетных операций покупателю выдается чековый суррогат, определяющее значение приобретают средства криптографической защиты фискальных данных, позволяющие однозначно выявить фальсификации в ходе учета фискальных данных. Для защиты от фальсификации чеков требуется применение средств криптографической защиты в составе каждого экземпляра ККТ, соблюдение требований по эксплуатации ККТ, исключающих подмену и блокирование этих средств криптографической защиты. Особое значение приобретает построение систем проверки фискального признака покупателем. Такие средства были апробированы в эксперименте ФНС России, показали положительный результат их применения и представляют существенный резерв для обеспечения безопасности фискальных данных. Для того, чтобы социальный ресурс покупателей, мобилизованный на выполнение этих проверок, не растрачивался впустую, следует уделить внимание однородности средств криптографической защиты фискальных данных и целостности пространства доверия в зоне генерации и проверки фискальных данных. Недостаточное внимание этим вопросам может приводить к одновременному созданию недобросовестными производителями контрафактной продукции ККТ и средств «проверки» формируемых ею «фискальных признаков». Прецеденты создания таких систем имеются уже сегодня, до введения нового порядка применения ККТ.

8. Внедрение перечисленных мер информационной безопасности фискальных данных, средств и систем обработки фискальных данных требует обновления и гармонизации действующего законодательства и нормативно-правовой базы эксплуатации ККТ. Основными задачами в этом направлении являются:

– Расширение правил ведения Государственного реестра контрольно-кассовой техники с учетом новых функциональных возможностей ККТ, новых процессов ее регистрации и эксплуатации, применения новых аппаратно-программных платформ ККТ.

– Разработка технических требований и регламентов эксплуатации новых систем обработки фискальных данных, важнейшими из которых являются системы электронной регистрации ККТ и сбора фискальных данных.

– Нормативно-правовая база должна быть расширена для организации ответственности нарушителей безопасности систем, эксплуатирующих угрозы нового типа.

9. Приложение 1. Источники разработки

1. ФНС России. «Концепция информационной безопасности Федеральной налоговой службы Российской Федерации» (утверждена приказом Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@).
2. Федеральный закон от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт» (Собрание законодательства Российской Федерации, 2003, N 21, ст. 1957; 2009, N 23, ст. 2776; N 29, ст. 3599; 2010, N 31, ст. 4161).
3. Постановление Правительства Российской Федерации от 23 июля 2007 г. № 470 «Об утверждении Положения о регистрации и применении контрольно-кассовой техники, используемой организациями и индивидуальными предпринимателями» (Собрание законодательства Российской Федерации, 2007, N 31, ст. 4089; 2008, N 24, ст. 2869).
4. Постановление Правительства Российской Федерации от 30 июля 1993 г. № 745 «Об утверждении Положения по применению контрольно-кассовых машин при осуществлении денежных расчетов с населением и Перечня отдельных категорий предприятий (в том числе физических лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в случае осуществления ими торговых операций или оказания услуг), организаций и учреждений, которые в силу специфики своей деятельности либо особенностей местонахождения могут осуществлять денежные расчеты с населением без применения контрольно-кассовых машин» (Собрание законодательства Российской Федерации, 1993, N 32, ст. 3017; 1995, N 44, ст. 4182; 1997, N 3, ст. 384; 1998, N 1, ст. 125; 1998, N 33, ст. 4016; N 36, ст. 4525; N 48, ст. 5932; 1999, N 3, ст. 338; 2000, N 50, ст. 4898; 2003, N 33, 3270).

5. ФСБ России. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утверждено приказом ФСБ России от 09.02.2005 г. № 66, зарегистрировано в Минюсте России 03.03.2005 г. № 6382.
6. Требования ФСБ России к СКЗИ.
7. Требования ФСБ России к СКЗФД.
8. ФСБ России. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г., №149/5-144.
9. ФСТЭК России. Руководящий документ «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации», утвержден 30 марта 1992 г.
10. ФСТЭК России. Руководящий документ «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утвержден 4 июня 1999 г.
11. ФСТЭК России. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены 02 марта 2001 г.
12. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
13. ГОСТ 34.601-90 Автоматизированные системы. Стадии создания.
14. ЗАО «Атлас-карт». Отчет о работе нормативно методического характера по теме «Разработка предложений по совершенствованию организационной, программно-аппаратной,

законодательной системы государственного контроля при осуществлении наличных денежных расчетов при реализации товаров (работ, услуг) в целях налогообложения, на основе международного опыта», выполненного по заказу №0173100007812000049 в рамках госконтракта от 17.09.2012 № 5-7-02/169 ФНС России.

15. «Административный регламент предоставления Федеральной налоговой службой государственной услуги по регистрации контрольно-кассовой техники, используемой организациями и индивидуальными предпринимателями в соответствии с законодательством Российской Федерации», утвержден Приказом Министра финансов Российской Федерации от 29 июня 2012 г. № 94н.

16. Приложение №1 к «Положению о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», «Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств», утвержден постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

17. «Доклад об оценке результатов эксперимента по применению контрольно-кассовой техники при осуществлении наличных

денежных расчетов и (или) расчетов с применением платежных карт, обеспечивающей передачу налоговым органам информации в электронном виде информации о таких расчетах, на территории Республики Татарстан, Калужской области, Московской области и г. Москвы с 1 августа 2014 года до 1 февраля 2015 г.», приложение к письму ФНС России в Правительство Российской Федерации № ЕД-16-2/62@ от 05.03.2015.

18. ГОСТ Р 51901.1-2002. «Менеджмент риска. Анализ риска технологических систем».

19. ФСБ России «Требования к средствам электронной подписи и удостоверяющего центра», утверждены приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 796.