УТВЕРЖДАЮ

Министр
промышленности и торговли
Российской Федерации

_____ Д.В. Мантуров

«05» ноября 2019 г.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

к обеспечению защиты информации, содержащейся в информационной системе, используемой при проведении эксперимента по маркировке велосипедов и велосипедных рам средствами идентификации и мониторингу оборота данной продукции в целях автоматизации задач мониторинга движения товаров и апробации маркировки средствами идентификации товаров (товарных групп), не подлежащих обязательной маркировке, выбранных для проведения эксперимента, и информационной безопасности при использовании информационно-телекоммуникационных технологий в рамках эксперимента

Москва 2019

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование системы – информационная система, используемая при проведении эксперимента по маркировке велосипедов и велосипедных рам средствами идентификации и мониторингу оборота данной продукции в целях автоматизации задач мониторинга движения товаров и апробации маркировки средствами идентификации товаров (товарных групп), не подлежащих обязательной маркировке, выбранных для проведения эксперимента (далее – информационная система мониторинга) – информационная система, созданная в целях автоматизации процессов сбора и обработки информации об обороте товаров, не подлежащих обязательной маркировке средствами идентификации, выбранных для проведения эксперимента, хранения такой информации, обеспечения доступа к ней, ее предоставления и распространения, повышения эффективности обмена такой информацией и обеспечения прослеживаемости указанных товаров, а также в иных целях, предусмотренных федеральными законами.

1.2 Сокращенное наименование системы – ИС МТ «Велосипеды и велосипедные рамы», ИС МТ.

1.3 Разработчик ИС МТ «Велосипеды и велосипедные рамы» – ООО «Оператор-ЦРПТ» (далее – Оператор системы).

1.4 Основанием для создания ИС МТ «Велосипеды и велосипедные рамы» является постановление Правительства Российской Федерации от 11 сентября 2019 г. № 1183 «О проведении эксперимента по маркировке

велосипедов и велосипедных рам средствами идентификации и мониторингу оборота данной продукции» (далее соответственно – Постановление, Эксперимент).

1.5 Плановые сроки начала и окончания работ:

Начало работ: «16» сентября 2019 г.

Окончание работ: «31» мая 2020 г.

1.6 В настоящих Технических требованиях используются следующие сокращения:

АСУТП	Автоматизированная система управления технологическими процессами.
БД	База данных
ГС1	Информационная система автоматической идентификации «ЮНИСКАН/ГС1 РУС»
ЕГРИП	Единый государственный реестр индивидуальных предпринимателей
ЕГРЮЛ	Единый государственный реестр юридических лиц
ИНН	Идентификационный номер налогоплательщика
ККТ	Контрольно-кассовая техника
КМ	Код маркировки
КПП	Код причины постановки на учет налогоплательщика
Минпромторг России	Министерство промышленности и торговли Российской Федерации
НДС	Налог на добавленную стоимость
ПЗИ	Подсистема(ы) защиты информации
Роспотребнадзор	Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека
СКЗИ	Средство криптографической защиты информации
КИ	Код идентификации
Велосипеды и велосипедные рамы, велотовары	продукция, независимо от способа ее производства или материалов, из которых она изготовлена, соответствующая кодам ТН ВЭД ЕАЭС 8711 «Велосипеды с установленным вспомогательным двигателем, с колясками или без них», 8712 00

	«Велосипеды двухколесные и прочие велосипеды (включая трехколесные велосипеды для доставки грузов) без двигателя», 8714 91 100 «Рамы велосипедов», 9503 00 100 9 «Трехколесные велосипеды»
ФН	Фискальный накопитель
ФНС России	Федеральная налоговая служба России
ФТС России	Федеральная таможенная служба России
ЦОД	Центр обработки данных

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИС МТ «ВЕЛОСИПЕДЫ И ВЕЛОСИПЕДНЫЕ РАМЫ»

2.1 Назначение ИС МТ «Велосипеды и велосипедные рамы».

ИС МТ «Велосипеды и велосипедные рамы» предназначен для осуществления государственного контроля за оборотом велотоваров.

ИС МТ «Велосипеды и велосипедные рамы» создается в соответствии с методическими рекомендациями для участников эксперимента по маркировке велосипедов и велосипедных рам средствами идентификации и мониторингу оборота данной продукции в Российской Федерации, утвержденными Минпромторгом России (далее – методические рекомендации).

Подсистемы защиты информации (ПЗИ) предназначены для обеспечения информационной безопасности ИС МТ «Велосипеды и велосипедные рамы» в соответствии с требованиями модели угроз информационной безопасности кодов маркировки продукции, средств и систем их обработки.

2.2 Цели создания ПЗИ ИС МТ «Велосипеды и велосипедные рамы»:

2.2.1 обеспечение информационной безопасности ИС МТ «Велосипеды и велосипедные рамы», средств и систем формирования и обработки кодов маркировки в составе средств идентификации велотоваров;

2.2.2 обеспечение достоверности сведений, поступающих в БД ИС МТ «Велосипеды и велосипедные рамы»;

2.2.3 регистрация в некорректируемом виде событий производства и оборота маркированных товарных и логистических единиц велотоваров;

2.2.4 обеспечение требований безопасности при эмиссии и обработке кодов маркировки в составе средств идентификации велотоваров;

2.2.5 регистрация событий выбытия маркированных велотоваров;

2.2.6 предоставление потребителю достоверных сведений о приобретаемых им велотоваров.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1 Состав объектов ИС МТ «Велосипеды и велосипедные рамы».

3.1.1 Центр обработки данных ИС МТ «Велосипеды и велосипедные рамы», обеспечивающий предоставление услуг системы, включающий:

3.1.1.1 Базу данных кодов маркировки и приложения мониторинга движения маркированных велотоваров.

3.1.1.2 Подсистему криптографической защиты кодов маркировки.

3.1.1.3 Подсистему криптографической проверки кодов маркировки.

3.1.1.4 Подсистему сетевой безопасности ИС МТ.

3.1.1.5 Подсистему мониторинга и управления информационной безопасностью ИС МТ.

3.1.1.6 Подсистему администрирования.

3.1.2 Промышленные регистраторы эмиссии и применения кодов маркировки велотоваров (КМ ТЛП).

3.1.3 Контрольно-кассовую технику (ККТ), содержащую фискальный накопитель (ФН).

3.2 Состав процессов, контролируемых ИС МТ «Велосипеды и велосипедные рамы» и функции информационной безопасности, обеспечиваемые ПЗИ ИС МТ «Велосипеды и велосипедные рамы».

3.2.1 Прием, обработка, исполнение заказов на создание КМ ТЛП.

3.2.2 Генерация криптографических кодов проверки кодов маркировки.

3.2.2.1 Криптографические коды проверки КМ ТЛП должны вычисляться при помощи криптографического преобразования, обеспечивающего защиту (уникальность, непредсказуемость, некорректируемость) КМ, защиту от неавторизованной эмиссии КМ ТЛП, возможность криптографической проверки подлинности КМ ТЛП и возможность прослеживания движения маркированных велотоваров.

3.2.2.2 Функции 3.2.1 и 3.2.2 должна выполнять Подсистема криптографической защиты кодов маркировки в составе ИС МТ во взаимодействии с регистраторами эмиссии и применения КМ ТЛП.

3.2.3 Выдачу по запросам учетных систем (УС) участников оборота или ИС МТ «Велосипеды и велосипедные рамы» кодов маркировки для нанесения на велотовары в составе средств идентификации.

3.2.4 Регистрацию в некорректируемом виде событий эмиссии и применения кодов маркировки, передачу в некорректируемом виде и выгрузку по запросам УС или ИС МТ «Велосипеды и велосипедные рамы» отчетов о применении кодов маркировки.

3.2.4.1 Функции 3.2.3 и 3.2.4, а также функции регистрации выбытия КМ ТЛП, защиты связи с Подсистемой криптографической защиты кодов маркировки и хранения кодов маркировки в доверенном устройстве должны выполнять регистраторы эмиссии и применения кодов маркировки.

3.2.5 Функции проверки средств идентификации велотоваров, регистрации в некорректируемом виде в кассовых чеках выбытия с рынка маркированных велотоваров, формирования и передачи в ИС МТ «Велосипеды и велосипедные рамы» в составе кассовых чеков сведений о выбытии средств идентификации велотоваров.

3.2.5.1 Функцию 3.2.5 выполняться на предприятиях розничной торговли с применением ККТ, содержащей фискальный накопитель, поддерживающих функции проверки КМ ТЛП и взаимодействия с Подсистемой криптографической проверки кодов маркировки.

3.2.6 Функции проверки подлинности кодов маркировки велотоваров потребителем.

3.2.6.1 Функцию 3.2.5.1 должна выполнять Подсистема криптографической проверки кодов маркировки по запросам мобильного приложения пользователя (мобильное приложение не выполняет функций защиты информации).

3.2.6.2 Мобильное приложение должно обеспечивать функции целостности и достоверности для передаваемых данных. В качестве дополнительной меры защиты пользователя от возможной компрометации мобильного устройства ИС МТ должна предлагать несколько независимых каналов проверки кода маркировки велотоваров (например, мобильное приложение и доступ через веб-интерфейс при помощи браузера).

3.2.6.3 Узел доступа мобильных и веб-приложений к услуге проверки кодов маркировки должен быть защищен от атак со стороны пользователей сети Интернет при помощи следующих мер безопасности:

– структуризация сетевого периметра при доступе к веб-услуге; контроль сетевого доступа при помощи межсетевого экрана; при этом периметр, в котором располагаются средства сетевой защиты информации должен быть защищен при помощи межсетевого экрана, сертифицированного ФСБ России; применением всех мер защиты, изложенных в разделе «4.6.2. Требования к Подсистеме сетевой информационной безопасности ЦОД ИС МТ»;

– отказ от применения протокола HTTP, доступ исключительно на основе протокола HHTPS;

– противодействие атакам DoS и DDoS на уровне протоколов прикладного уровня, фильтрация и маршрутизация запросов к веб-службам, противодействие атакам путем «медленных» HTTP-запросов;

– фильтрация данных, вредоносного кода, вредоносного ПО скриптов, включаемых в веб-запросы; меры защиты от перехвата запросов путем подмены временных данных аутентификации (cookies), SQL-инъекций, межсайтового скриптинга; атак, основанных на вводе некорректных данных в веб-формы; атак, основанных на несанкционированной модификации динамический параметров URL;

– контроль доступа между веб-сервером, и серверами баз данных, прикладной логики веб-услуг;

– контроль актуальности и защищенности программного обеспечения узла веб-доступа, обновление ПО, профилактические меры против эксплуатация веб-уязвимостей.

3.2.6.4 Подсистемы сетевой безопасности ИС МТ, мониторинга и управления информационной безопасностью администрирования обеспечивают защиту от внутренних угроз ИС МТ.

4. ТРЕБОВАНИЯ К ИС МТ «ВЕЛОСИПЕДЫ И ВЕЛОСИПЕДНЫЕ РАМЫ»

4.1 Требования к ИС МТ «Велосипеды и велосипедные рамы» в целом.

4.1.1 Состав подсистемы защиты инфомации (ПЗИ) ИС МТ «Велосипеды и велосипедные рамы», требования к способам и средствам связи для информационного обмена между компонентами ИС МТ «Велосипеды и велосипедные рамы».

Средства защиты информации ИС МТ «Велосипеды и велосипедные рамы» представляют собой целостный комплекс взаимосвязанных и взаимодействующих между собой подсистем защиты информации ИС МТ. Перечень подсистем защиты информации ИС МТ приведен в разделах 3.2.2.2, 3.2.4.1, 3.2.5.1, 3.2.6 и 3.2.6.4. При этом:

4.1.1.1 Подсистемы криптографической защиты кодов маркировки, криптографической проверки кодов маркировки, сетевой безопасности ИС МТ, мониторинга и управления информационной безопасностью, администрирования ИС МТ предназначены для эксплуатации в контролируемой зоне ЦОД ИС МТ.

4.1.1.2 Промышленные регистраторы эмиссии и применения кодов маркировки велотоваров, ККТ, содержащая фискальный накопитель, устанавливаются у внешних пользователей услуг ИС МТ «Велосипеды и велосипедные рамы» и могут находиться в распоряжении субъектов, выступающих в роли нарушителей информационной безопасности кодов маркировки, средств и систем их обработки.

4.1.1.3 Удаленные подсистемы ИС МТ, перечисленные в разделе 4.1.1.2, должны взаимодействовать с подсистемами защиты информации, расположенными в ЦОД ИС МТ путем обмена защищенными сообщениями. Требования к протоколу защиты связи между этими подсистемами защиты информации и ЦОД ИС МТ приведены в разделе 4.6.1.

4.1.2 Требования по организации взаимодействий между ИС МТ со смежными системами.

4.1.2.1 ИС МТ в ходе эксперимента может находиться во взаимодействии с информационными системами операторов фискальных данных (ОФД).

4.1.2.2 Требования по защите каналов связи между ИС МТ и перечисленными информационными системами устанавливаются по согласованию с администрацией этих систем.

4.1.3 Требования по защите средств идентификации велотоваров:

4.1.3.1 Код маркировки в составе средства идентификации должен состоять из 4 составляющих:

- код товара;
- Индивидуального серийного номера;
- Ключа проверки;
- Кода проверки.

4.1.3.2 В качестве кода идентификации (далее КИ) могут использоваться:

- код товара;
- Бинарные данные произвольной длины, по усмотрению (в формате) производителя, семантика которых одобрена для применения в ИС МТ;

4.1.3.3 Подсистема эмиссии кодов маркировки ИС МТ должна выполнять запросы (заказы) на генерацию ключей проверки и кодов проверки для заданного набора КИ. При этом в рамках одного запроса (заказа) должны использоваться КИ только одного вида товара, однородного для всего заказа, типа.

4.1.3.4 Подсистема эмиссии кодов маркировки ИС МТ должна иметь возможность самостоятельно генерировать КИ по заказам пользователей.

4.1.3.5 Форматы кодов идентификации, ключей проверки и кодов проверки должны согласовываться с ФСБ России.

4.1.3.6 Алгоритмы криптографического преобразования, применяемые для защиты кодов маркировки, должны соответствовать стандартам Российской Федерации.

4.1.3.7 Для каждого КИ ИС МТ должна иметь возможность (а) создать и (б) проверить код проверки установленного формата.

4.1.4 Требования по показателям назначения

4.1.4.1 Требования к ПЗИ ИС МТ, применяемым на этапе эксперимента, изложены как рамочные и представлены, если специально не оговорено иное, в формате оценки верхних границ масштабирования системы. ИС МТ на этапе эксперимента может не достигать указанных показателей и требований, однако не должна ограничивать возможность масштабирования показателей системы в указанных границах на этапах эксплуатации по завершении эксперимента.

4.1.4.2 В случаях, когда ограничения этапа эксперимента касаются снижения требований безопасности ПЗИ ИС МТ, в настоящих Технических требованиях сделаны отдельные примечания.

4.1.4.3 ИС МТ на дату завершения эксперимента должна обеспечивать поддержку оборота не менее 500 миллионов кодов маркировки.

4.1.4.4 ИС МТ должна в перспективе масштабироваться для обслуживания оборота 3 миллиарда кодов маркировки в год. Архитектура ИС МТ не должна ограничивать возможности такого масштабирования.

4.1.4.5 ИС МТ должна поддерживать возможность обслуживания не менее 20 тысячи участников оборота велотоваров.

4.1.4.6 ИС МТ должна обслуживать парк до 10 тысяч регистраторов эмиссии и применения кодов маркировки велотоварову участников оборота маркированных велотоваров.

4.1.4.7 ИС МТ должна обслуживать парк не менее 50 тысяч единиц ККТ с поддержкой функции проверки кодов маркировки на этапе эксперимента. ИС МТ должна в перспективе масштабироваться для обслуживания до 500 тысяч единиц ККТ. Архитектура ИС МТ не должна ограничивать возможности такого масштабирования.

4.1.4.8 Заказ кодов маркировки, поступающий в Подсистему криптографической защиты кодов маркировки, должен содержать от 1 до 100 000 КИ или требование на генерацию по шаблону пользователя от 1 до 100 000 кодов маркировки.

4.1.4.9 Заказ кодов маркировки должен выполняться Подсистемой криптографической защиты кодов маркировки с вероятностью 90 % за 30 минут. Максимальное время выполнения заказа кодов маркировки должно составлять 120 минут.

4.1.4.10 Подсистема криптографической проверки кодов маркировки должна обслуживать не менее 100 тысяч запросов на проверку кодов маркировки в сутки.

4.1.4.11 Запрос на проверку средства идентификации при помощи мобильного приложения должен выполняться Подсистемой криптографической проверки кодов маркировки с вероятностью 90 % за 15 секунд (в условиях доступа к услуге по через 3G мобильный интернет). Мобильное приложение должно обеспечивать функции целостности и достоверности для передаваемых данных.

4.2 Требования к Подсистеме криптографической защиты кодов маркировки.

4.2.1 Подсистема криптографической защиты кодов маркировки должна обеспечивать сетевое взаимодействие с двумя типами объектов:

4.2.1.1 с промышленными регистраторами эмиссии и применения кодов маркировки;

4.2.1.2 с рабочим местом (терминалом) доверенного сотрудника участника оборота.

4.2.1.3 Прочие взаимодействия должны быть запрещены.

4.2.2 Взаимодействия подсистемы криптографической защиты кодов маркировки с регистраторами эмиссии в зоне производства велотоваров и у участников оборота велотоваров должны осуществляться по защищенному на основе протокола, требования к которому изложены в разделе 4.6.1, каналу связи.

4.2.3 Подсистема криптографической защиты кодов маркировки должна обеспечивать конфигурирование параметров и сохранять конфигурации подключенных регистраторов, установленных в зоне участника оборота велотоваров.

4.2.4 Для выполнения криптографических преобразований в составе подсистемы криптографической защиты кодов маркировки должен применяться специализированный программно-аппаратный комплекс, являющийся средством криптографической защиты информации (СКЗИ), сертифицированным ФСБ России на предмет соответствия требованиям, предъявляемым ФСБ России к СКЗИ класса КС3. Средства криптографической защиты информации должны поставляться в комплекте с копией сертификата ФСБ России, формуляра СКЗИ, Правил пользования СКЗИ. Допускается поставка перечисленных документов в электронной форме и (или) предоставление пользователю СКЗИ возможности скачать документы с сайта производителя СКЗИ. Эксплуатация СКЗИ должна быть организована в строгом соответствии с правилами пользования, поставляемыми разработчиком СКЗИ.

4.2.5 Специализированный программно-аппаратный комплекс, предназначенный для защиты кодов маркировки должен обеспечивать выполнение операций в режиме изоляции криптографических ключей. Мастер ключи, на основе которых будут формироваться криптографические ключи для защиты кодов маркировки, должны выдаваться ФСБ России. Криптографические ключи для защиты кодов маркировки должны помещаться на специальные носители и вводиться в специализированный программно-аппаратный комплекс уполномоченными представителем разработчика СКЗИ в режиме регламентированного Правилами пользования СКЗИ технического обслуживания.

4.2.6 Специализированный программно-аппаратный комплекс должен пройти исследования по оценке влияния на него Подсистемы криптографической защиты кодов в соответствии с требованиями ФСБ России.

На этапе Эксперимента в Подсистеме криптографической защиты кодов допускается использование опытных образцов СКЗИ, разрабатываемых в соответствии с техническими заданиями, согласованными ФСБ России.

4.3 Требования к Подсистеме криптографической проверки кодов маркировки.

Требования к Подсистеме криптографической проверки кодов маркировки аналогичны требованиям, изложенным в разделе 4.2.

4.4 Требования к Промышленному регистратору эмиссии велотоваров у участников оборота маркированных велотоваров.

4.4.1 Регистраторы эмиссии должны устанавливаться в пределах контролируемой зоны участника оборота велотоваров или оператора обработки кодов маркировки.

4.4.2 Регистраторы эмиссии должны обеспечивать заказ кодов маркировки, прием их от Подсистемы криптографической защиты кодов маркировки и выполнение функций регистрации событий обработки кодов маркировки, описанных в разделе 3.2.

4.4.3 Регистратор эмиссии должен идентифицироваться при помощи индивидуального криптографического модуля идентификации регистратора.

4.4.4 Криптографический модуль идентификации регистратора должен выполнять следующие функции:

4.4.4.1 Поставлять достоверные, метрологически поверенные данные о времени совершения регистрируемых событий и, опционально, достоверные географические координаты местонахождения.

4.4.4.2 Хранить криптографические ключи регистратора эмиссии и применения кодов маркировки.

4.4.4.3 Выполнять функции взаимной аутентификации между регистратором эмиссии и применения кодов маркировки и Подсистемой криптографической защиты кодов маркировки в составе ЦОД ИС МТ.

4.4.4.4 Хранить сведения об операциях, выполняемых Регистратором эмиссии и применения кодов маркировки.

4.4.4.5 Формировать квалифицированную электронную подпись для электронных документов.

4.4.5 Криптографический модуль идентификации регистратора, регистратор эмиссии и применения кодов маркировки со встроенным в него криптографическим модулем идентификации регистратора являются программно-аппаратными средствами криптографической защиты информации, которые должны быть сертифицированы ФСБ России. В соответствии с требованиями Модели угроз [**Ошибка! Источник ссылки не найден.**], данные средства криптографической защиты должны быть устойчивы к атакам нарушителя с правами пользователя СКЗИ и должны соответствовать классу СКЗИ не ниже КС3. Средства криптографической защиты информации должны поставляться в комплекте с копией сертификата ФСБ России, формуляра СКЗИ, Правил пользования СКЗИ. Допускается поставка перечисленных документов в электронной форме и (или) предоставление пользователю СКЗИ возможности скачать документы с сайта производителя СКЗИ. Эксплуатация СКЗИ должна быть организована в строгом соответствии с правилами пользования, поставляемыми разработчиком СКЗИ.

На этапе Эксперимента в качестве криптографического модуля идентификации регистратора, Регистратора эмиссии и применения кодов маркировки допускается использование опытных образцов СКЗИ, разрабатываемых в соответствии с техническими заданиями, согласованными ФСБ России.

4.5 ККТ и фискальный накопитель должны соответствовать требованиям, установленным законодательством Российской Федерации о применении контрольно-кассовой техники.

4.5.1 Запросы на проверку статуса кодов маркировки должны направляться в Подсистему криптографической проверки кодов маркировки для каждой товарной позиции фискального документа «Кассовый чек (бланк строгой отчетности)», содержащей маркированные велотовары.

4.5.2 Статус кода маркировки должен проверяться в течение не более чем 15 секунд.

4.5.3 Информационные системы ОФД и ИС МТ должны быть интегрированы в целях обеспечения взаимодействие с Подсистемой криптографической проверки кодов маркировки, направленного на:

4.5.3.1 передачу в ИС МТ отчетов о выбытии маркированных продукции.

4.6 Требования к Подсистеме сетевой безопасности ИС МТ.

4.6.1 Требования к протоколу взаимодействия между удаленными ПЗИ и ЦОД ИС МТ.

Протокол взаимодействия между удаленными подсистемами защиты информации (регистраторами эмиссии и применения кодов маркировки, ККТ с фискальным накопителем) и подсистемами защиты информации, работающими в ЦОД ИС МТ (Подсистема криптографической эмиссии кодов маркировки и Подсистема криптографической проверки кодов маркировки), далее по тексту раздела – «протокол», должен соответствовать следующим требованиям:

4.6.1.1 Для взаимодействия подсистем должны применяться сети общего пользования на основе протоколов TCP/IP.

4.6.1.2 Протокол должен обеспечивать взаимодействие клиент-сервер с применением функций защиты информации на прикладном уровне (криптографическая защита сообщений).

4.6.1.3 Передача сообщений от клиента к серверу должна завершаться подтверждением их приема сервером.

4.6.1.4 Гарантированная доставка сообщений должна осуществляться методом их настойчивой повторной передачи клиентом.

4.6.1.5 Сообщения должны быть идентифицированы. На повторную передачу сообщения клиента сервер должен отвечать повтором ранее переданного сообщения. Клиент должен игнорировать повторно поступающие ответы сервера.

4.6.1.6 Функции криптографической защиты сообщений должны обеспечивать:

- взаимную аутентификацию участников взаимодействия;
- конфиденциальность и целостность передаваемой информации;
- должны обеспечиваться защита от атак повторной передачи сообщений нарушителем информационной безопасности и от передачи ложных сообщений;
- передача информации в открытом виде должна быть запрещена.

4.6.1.7 Для выполнения функций безопасности из раздела 4.1.4.6 должны использоваться криптографические алгоритмы, соответствующие стандартам Российской Федерации.

4.6.2 Требования к Подсистеме сетевой информационной безопасности ЦОД ИС МТ

Подсистема сетевой информационной безопасности ЦОД ИС МТ должна соответствовать, дополнительно к требованиям раздела 4.6.1 следующим требованиям:

4.6.2.1 Для отдельных сетевых объектов ИС МТ должен применяться режим работы, в котором исключаются любые незащищенные (не аутентифицированные, не шифрованные) сетевые взаимодействия (режим изоляции сетевого взаимодействия).

4.6.2.2 В тех случаях, когда применение режима защищенного протокола передачи данных невозможно (при взаимодействии с внешними информационными системами, при организации веб-доступа к ИС МТ), а также по отношению к внешнему сетевому трафику после снятия криптографической защиты необходимо применять следующие меры защиты:

- фильтрация трафика, сетевой контроль доступа при помощи межсетевых экранов;
- средства обнаружения вторжений (IDS) и/или противодействия вторжениям (IPS), контролирующие, в том числе, качество фильтрации межсетевых экранов.

4.6.2.3 Локальные вычислительные сети ИС МТ должны быть сегментированы. Серверные ресурсы информационных систем должны быть выделены в отдельные сегменты локальных вычислительных сетей, между сегментами локальных сетей должен быть организован контроль доступа с применением технологий коммутации.

4.6.2.4 Средства криптографической защиты информации Подсистемы криптографической эмиссии кодов маркировки и Подсистемы криптографической проверки кодов маркировки должны помещаться в отдельных сегментах (виртуальных локальных вычислительных сетях) ЛВС ИС МТ.

4.6.2.5 Защита от опасного мобильного кода (вирусов, червей, spyware и т.п.) должна осуществляться:

– в точках взаимодействия компонентов информационных систем с сетями связи общего пользования, в которых может распространяться опасный мобильный код;

– на шлюзах взаимодействия с внешними организациями;

– внутри и на границах сегментов локальных сетей;

– на рабочих местах пользователей (в первую очередь – при применении съемных носителей данных).

4.6.2.6 Защита от опасного мобильного кода должна осуществляться на основе отдельной политики безопасности, разработанной применительно к конкретному объекту защиты.

4.6.2.7 Применяемые средства антивирусной защиты должны быть сертифицированы ФСБ России.

4.6.2.8 Внутри локальных вычислительных сетей должен быть организован контроль аномальных активностей, применением средств обнаружения вторжений и межсетевых экранов прикладного уровня в составе серверных систем.

4.6.2.9 Периметрические и серверные средства обнаружения вторжений, средства контроля за распространением опасного мобильного кода рекомендуется интегрировать со средствами сетевой информационной безопасности на периметре сети и средствами коммутации внутри локальных систем с тем, чтобы они могли изолировать и блокировать аномальные активности, несанкционированный доступ, атаки опасного мобильного кода.

4.6.2.10 Информационные системы (в первую очередь, системы эмиссии и проверки кодов маркировки) должны быть защищены от атак на подавление услуги (DoS, DDoS). В качестве мер защиты от атак этого типа должны быть приняты следующие меры безопасности:

– применение на входе в информационные системы из сетей общего пользования специализированных средств противодействия атакам на отказ в доступе;

– дизайн протоколов доступа, относительно устойчивый к атакам отказа в доступе, для криптографических протоколов – для атак повторной передачи легитимного сообщения;

– резервирование инфраструктуры информационных систем, в том числе диверсификация точек обработки, каналов доступа, применение средств балансирования сетевой нагрузки; применение резервированных систем коммутации внутри локальных сетей;

– контракт с коммуникационным провайдером, подразумевающий сотрудничество по предотвращению атак на отказ в доступе.

Меры защиты рекомендуется проработать в составе технического проекта информационных систем и сопроводить нагрузочными испытаниями при проведении приемки системы.

4.7 Требования к Подсистеме мониторинга и управления информационной безопасностью ИС МТ.

4.8 Требования к Подсистеме администрирования ИС МТ.

4.8.1 В Подсистеме администрирования ИС МТ должны быть организованы две роли пользователей с правами администраторов системы:

4.8.1.1 администратор;

4.8.1.2 аудитор.

4.8.2 Администратор Подсистемы администрирования ИС МТ должен выполнять функции:

4.8.2.1 управления компонентами и ресурсами комплекса технических средств ИС МТ;

4.8.2.2 подключения, отключения, конфигурирования Регистраторов эмиссии и применения кодов маркировки;

4.8.2.3 мониторинга работы системы в целом.

4.8.3 Действия администраторов ИС МТ подлежат детальному событийному протоколированию.

4.8.4 Администратор должен иметь доступ ко всем техническим средствам и информационным ресурсам (активам) ИС МТ за исключением:

4.8.4.1 криптографических ключей и функций (ресурсов) СКЗИ, прерогатива обслуживания которых принадлежит, в соответствии с Правилами пользования, изготовителю СКЗИ;

4.8.4.2 администрирования систем событийного протоколирования;

4.8.4.3 доступа к данным систем событийного протоколирования с правами «Создать», «Модифицировать», «Уничтожить».

4.8.5 Аудитор ИС МТ выполняет функции:

4.8.5.1 управления компонентами и ресурсами подсистемы событийного протоколирования ИС МТ;

4.8.5.2 доступа к доступным администраторам ресурсами комплекса технических средств ИС МТ с правами «Только чтение»;

4.8.5.3 доступа к данным подсистемы событийного протоколирования.

4.8.6 Действия аудиторов ИС МТ подлежат детальному событийному протоколированию.

4.9 Требования к режимам функционирования ИС МТ.

Все функциональные модули ИС МТ, за исключением ККТ, работающих посменно сменами до 24-х часов, должны обеспечивать непрерывный режим функционирования.

4.10 Требования к надежности ИС МТ и доступности ресурсов.

4.10.1 Коэффициент доступности услуг ИС МТ должен составлять 99,5 % (до 48 часов простоя в год). Архитектура ИС МТ не должна ограничивать возможности доведения в перспективе показателя доступности до 99,9 %.

4.10.2 Время восстановления услуги ИС МТ после сбоя на этапе эксперимента не должно превышать 45 минут (в перспективе – 10 минут).

4.11 Требования к условиям эксплуатации и защите от влияния внешних воздействий

4.11.1 Технические средства ИС МТ должны эксплуатироваться в условиях, соответствующих группе 1 в соответствии с требованиями ГОСТ 21552- 84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение».

4.11.2 Корпус средств криптографической защиты и их опытных образцов должен поставляется и эксплуатироваться в опечатанном виде. Несанкционированное вскрытие корпуса является нарушением правил использования СКЗИ.

4.12 Требования к численности и квалификации персонала ИС МТ.

4.12.1 Администратор ИС МТ должен обладать высшим техническим образованием, опытом эксплуатации автоматизированных систем непрерывного цикла функционирования, профессиональными знаниями в области информационной безопасности, базовыми знаниями в области криптографии, знаниями правил пользования средствами криптографической защиты информации (СКЗИ), сертифицированными ФСБ России.

4.12.2 В штат администраторов ИС МТ должен входить сотрудник, обладающий правами создания учетных записей администраторов и аудиторов.

4.12.3 Аудитор ИС МТ должен обладать высшим техническим образованием, профессиональными знаниями в области информационной безопасности.

4.12.4 Номинальный штат администраторов ИС МТ должен составлять 3 человека.

На этапе эксперимента номинальный штат администраторов ИС МТ может быть менее 3-х человек.

4.12.5 Прочие требования определяются применительно к составу программно-технических требований ИС МТ общего назначения.

5. ИСТОЧНИКИ РАЗРАБОТКИ

5.1 Технические требования к информационной системе, используемой при проведении эксперимента по маркировке велосипедов и велосипедных рам средствами идентификации и мониторингу оборота данной продукции в целях автоматизации задач мониторинга движения товаров и апробации маркировки средствами идентификации товаров (товарных групп), не подлежащих обязательной

маркировке, выбранных для проведения эксперимента;

5.2 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

5.3 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

5.4 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

5.5 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

5.6 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

5.7 Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

5.8 Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

5.9 Приказ ФНС России от 21.03.2017 № ММВ-7-20/229@ «Об утверждении дополнительных реквизитов фискальных документов и форматов фискальных

документов, обязательных к использованию» (Зарегистрирован в Минюсте России 13.04.2017 № 46361);

5.10 ФНС России. Описание протокола взаимодействия между контрольно-кассовой техникой и информационной (автоматизированной) системой оператора фискальных данных. Версия 1.1 от 15.12.2016.

5.11 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденна ФСТЭК России 14.02.2008;

5.12 «Методический документ. Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014;

5.13 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК России 15.02.2008;

5.14 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом Гостехкомиссии России от 30.08.2002 № 282;

5.15 ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

5.16 ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

5.17 ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

5.18 ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;

5.19 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

5.20 ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

5.21 ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

5.22 РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;

5.23 РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.