УТВЕРЖДЕН

АДМГ.40002-01 30 01-ЛУ

ПРОГРАММНОЕ СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ СЛЕДОПЫТSSL

Вариант исполнения № 1 (Изм. 3)

Формуляр

АДМГ.40002-01 30 01

Листов 37

2023

СОДЕРЖАНИЕ

1.Общие указания 3

2.Общие сведения..... 7

3.Основные характеристики..... 8

4.Указания по эксплуатации..... 11

5.Порядок обновления 13

6.Комплектность..... 16

7.Периодический контроль основных характеристик при эксплуатации и хранении . 20

8.Свидетельство о приемке..... 21

9.Гарантийные обязательства..... 22

10.Сведения о рекламациях..... 24

11.Сведения о хранении..... 25

12.Сведения об изменениях 26

13.Сведения о закреплении при эксплуатации 27

14.Особые отметки 28

Перечень терминов и сокращений..... 30

Приложение 1..... 32

Приложение 2..... 33

Приложение 3..... 35

1. ОБЩИЕ УКАЗАНИЯ

1.1. Ввод в эксплуатацию Программного средства криптографической защиты информации СледопытSSL (вариант исполнения № 1) АДМГ.40002-01 (далее – Изделие) проводится в соответствии с эксплуатационной документацией (ЭД), перечень которой приведен в документе «Ведомость эксплуатационных документов» АДМГ.40002-01 20 01.

1.2. Порядок использования и установки Изделия приведен в документе «Правила пользования СКЗИ» АДМГ.40002-01 92 01.

1.3. Изделие является функционально законченным программным изделием, предназначенным для использования на мобильном устройстве (МУ), функционирующем под управлением операционной системы (ОС) Аврора, имеющей один из следующих сертификатов соответствия:

– ФСБ России «Требования к средствам защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа» по классу защиты не ниже АК2;

– ФСТЭК России «Профиль защиты операционных систем типа «А» четвертого класса защиты» и «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» по 4 уровню доверия.

1.4. Оценка корректности встраивания Изделия в ОС Аврора производится в соответствии с положениями документа «Методика встраивания», согласованного с в/ч 43753.

1.5. Изделие совместно с ОС Аврора (версии 4.0.2.249 и выше) предназначено для функционирования на аппаратных платформах, приведенных в таблице (Таблица 1), работающих под управлением ОС Аврора с ядром соответствующей версии.

Таблица 1

Аппаратная платформа	Версия ядра ОС Аврора
Планшет Aquarius NS220 v2.1	3.18.79
Планшет Byterg MVK-2020	3.18.79
Смартфон Mashtab TrustPhone T1	4.14.186
Планшет Fplus Life Tab Plus	4.9.117

ПРИМЕЧАНИЕ. Для проверки версии ядра ОС Аврора необходимо в мобильном приложении (МП) «Terminal» выполнить команду: `uname -srm`.

1.6. При обновлении ОС Аврора, имеющей один из перечисленных выше сертификатов соответствия, не требуется проведение дополнительных исследований СКЗИ в следующих случаях:

– неизменности аппаратных платформ и версий ядра ОС Аврора, для которых была произведена оценка корректности встраивания (см. Таблица 1);

– соответствии контрольным суммам (КС), указанным в разделе 6 настоящего документа.

1.7. Изделие состоит из следующих компонентов:

– RPM-пакетов, входящих в состав загрузочного модуля ОС Аврора:

- `nss`;
- `nss-softokn`;
- `nss-softokn-freebl`;
- `nss-sysinit`;
- `nss-util`;
- `securefs`;
- `sstore`;

– RPM-пакетов, входящих в состав загрузочного модуля Изделия:

- `feature-skzi`;
- `integrityd-config-skzi`;

- `libopenssl`;
- `openssl-gost-engine-cert`;
- `randseed`.

Также в состав загрузочного модуля Изделия входят следующие RPM-пакеты МП «Криптозаметки»:

– `omp-notes`;

– `omp-notes-l10n`;

– `omp-notes-settings`.

1.8. Выделенные регистрационные номера Изделия вносятся в раздел 8 настоящего документа и соответствуют заводскому номеру ОС Аврора, для совместного использования с которой предназначено Изделие.

1.9. Изделие может поставляться в виде физической поставки или в виде электронной поставки. Способ поставки[1] Изделия определяется условиями Лицензионного договора (далее – Лицензионный договор).

1.10. Комплектность поставки Изделия приведена в разделе 6 настоящего документа. Комплектность и версия Изделия при поставке определяются условиями Лицензионного договора.

1.11. Формуляр входит в комплект поставки[2] Изделия и должен постоянно храниться в подразделении, ответственном за его эксплуатацию.

1.12. Подробная информация по изготовлению и вводу в эксплуатацию экземпляров Изделия должна приводиться в приложении (Приложение 1) настоящего документа.

1.13. В разделе 14 настоящего документа может быть внесена необходимая дополнительная информация, связанная с эксплуатацией Изделия потребителем.

---

[1] Общая информация о возможных способах передачи и носителях информации Изделия приведена в приложениях (Приложение 2, Приложение 3) настоящего документа.

[2] При электронной поставке Изделия лицо, ответственное за эксплуатацию, распечатывает копию формуляра.

1.14. Все записи в формуляре должны производиться только черными чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления НЕ ДОПУСКАЮТСЯ. Неправильная запись аккуратно зачеркивается, и рядом делается новая, которая заверяется ответственным лицом. После подписи проставляются фамилия и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Полное наименование программного изделия: Программное средство криптографической защиты информации СледопытSSL (вариант исполнения № 1).

2.2. Сокращенное наименование программного изделия: СКЗИ СледопытSSL (вариант исполнения № 1).

2.3. Обозначение программного изделия: АДМГ.40002-01.

2.4. Предприятие-изготовитель: Общество с ограниченной ответственностью (ООО) «Открытая мобильная платформа»):

– юридический адрес: 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Университетская, д. 7, офис 59, ОГРН 1161690087020;

– фактический адрес: 119415, г. Москва, вн.тер.г. муниципальный округ Проспект Вернадского, пр-кт Вернадского, д. 41, 8 этаж.

2.5. Техническая поддержка предприятия-изготовителя: электронная почта support@omp.ru, тел. +7 (495) 269-09-80.

2.6. Изделие соответствует документу «Требования к средствам криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по классу защиты КС2.

2.7. Изделие предназначено для использования на территории Российской Федерации.

2.8. Настоящий документ содержит следующие приложения:

– Приложение 1. Изготовление и ввод в эксплуатацию экземпляров Изделия;

– Приложение 2. Общие положения предприятия-изготовителя по возможным вариантам поставки Изделия;

– Приложение 3. Пример маркировки DVD с Изделием.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. Изделие функционирует на МУ с установленной ОС Аврора и представляет собой программный комплекс, предназначенный для защиты информации, которой являются следующие конфиденциальные данные:

– передаваемые через сети общего пользования (например, сеть Интернет) посредством протокола TLS между СКЗИ и доверенным оконечным оборудованием;

– хранящиеся в локальном криптографическом контейнере (криптоконтейнере).

3.2. Изделие предназначено для выполнения следующих криптографических функций:

– защиты (шифрования) информации, передаваемой по линиям связи по протоколу TLS при установлении соединения с серверами, поддерживающими данную функцию. Защищенное TLS-соединение с использованием отечественных криптоалгоритмов устанавливается автоматически при обращении пользователя к серверу, поддерживающему данную возможность.

ПРИМЕЧАНИЕ. Веб-браузер является типичным пользовательским программным средством, активирующим возможность установки защищенного TLS-соединения. В случае установления защищенного соединения по протоколу TLS с использованием криптографических алгоритмов, браузер будет распознавать веб-страницу как надежную и безопасную, на панели инструментов браузера будет отображаться значок  , при касании которого откроется вкладка с надписью «Безопасное соединение»;

– обеспечения TLS-соединения с односторонней аутентификацией (сервера).

ПРИМЕЧАНИЕ. Защищенное TLS-соединение обеспечивается при взаимодействии с сертифицированными СКЗИ, установленными на сервере;

– защиты (шифрования) информации, хранимой в криптоконтейнере;

ПРИМЕЧАНИЕ. МП «Криптозаметки» является графическим прикладным приложением, реализующим функционал взаимодействия с криптоконтейнером посредством вызова разрешенных функций, описание которых приведено в документе АДМГ.40002-01 92 01.

– генерации псевдослучайных последовательностей (посредством датчика случайных чисел);

– простой или усиленной неквалифицированной электронной подписи (ЭП) (выработки и проверки) файлов с данными пользователей;

– контроля целостности файлов с данными учетной записи пользователя с использованием хеш-функции;

ПРИМЕЧАНИЕ. Выработка и проверка ЭП, контроля целостности файлов с данными учетной записи осуществляются сторонними приложениями с использованием экспортируемых функций СКЗИ СледопытSSL в соответствии с документом «Руководство программиста» АДМГ.40002-01 33 01.

– выработки ключевой информации.

ПРИМЕЧАНИЕ. Перечень параметров функций, подаваемых на вход Изделия и обеспечивающих возможность их использования, приведен в документе АДМГ.40002-01 33 01.

3.3. Изделие реализует следующие основные возможности:

– защищенное соединение по протоколу TLS с использованием криптографических алгоритмов: ГОСТ 28147-1989, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015;

– защищенное соединение по протоколу TLS 1.2 в соответствии с рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;

– выработку ключевой информации с использованием кода безопасности и защиты такой информации (Р 50.1.111-2016);

– формирование транспортных ключевых контейнеров для ключей в соответствии с ГОСТ Р 34.10-2012 (Р 50.1.112-2016);

– выработку общей ключевой информации с использованием разделяемого сторонами пароля и последующей аутентификации при взаимодействии по каналу (Р 50.1.115-2016);

– вычисление кода аутентификации HMAC на основе хеш-функции ГОСТ Р 34.11-2012 (Р 50.1.113-2016);

– порождение ключевого материала на основе функций диверсификации KDF_GOSTR3411_2012_256, KDF_TREE_GOSTR3411_2012_256 (Р 50.1.113-2016);

– создание криптографических сообщений формата CMS в соответствии с документом ТС 26.2.001-2020 (Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS, 2014 г.);

– работу с сертификатами и списками отзыва сертификатов инфраструктуры открытых ключей X.509 с поддержкой алгоритмов ГОСТ 34.10, ГОСТ 34.11 в соответствии с документом ТС 26.2.001-2020.

4. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

4.1. Эксплуатация Изделия должна осуществляться в соответствии с ЭД, перечисленной в документе АДМГ.40002-01 20 01.

ВНИМАНИЕ! Допускается использование СКЗИ СледопытSSL для криптографической защиты персональных данных, а также для обработки информации, не составляющей государственную тайну.

4.2. Изделие может быть установлено на МУ с ОС Аврора, функционирующей на аппаратных платформах, приведенных в таблице (см. Таблица 1).

4.3. Защита от несанкционированного доступа к СКЗИ обеспечивается за счет механизмов контроля целостности и аутентификации, реализованных в ОС Аврора, для совместного использования с которой предназначено СКЗИ СледопытSSL.

4.4. Пользователь должен выполнять следующие действия:

– при эксплуатации СКЗИ СледопытSSL руководствоваться положениями документа АДМГ.40002-01 92 01, а также:

- документа «Операционная система Аврора. Формуляр» АДМГ.10034-02 30 01;
- документа «Операционная система Аврора. Руководство пользователя» АДМГ.10034-02 90 01;
- документа «Операционная система Аврора. Руководство администратора» АДМГ.10034-02 91 01.

– контролировать уровень защищенности установленного TLS-соединения;

– хранить конфиденциальные данные в криптоконтейнере;

– в случае нештатных ситуаций действовать в соответствии с документом АДМГ.40002-01 92 01.

4.5. Пользователям запрещается:

– разглашать конфиденциальную информацию, допуск к которой он имеет;

– осуществлять подключение к точкам доступа беспроводных сетей (WLAN, Bluetooth®) и МУ, не вызывающим доверия;

ПРИМЕЧАНИЕ. Перечень точек доступа, разрешенных для подключения, должен быть сформирован на месте эксплуатации МУ лицом, ответственным за организацию системы связи.

– передавать МУ лицам, не допущенным к эксплуатации;

– оставлять МУ без присмотра;

– осуществлять самостоятельное вскрытие МУ, в т.ч. для проведения самостоятельного ремонта;

– подключать МУ и осуществлять зарядку от недоверенных устройств, например, электронно-вычислительных машин.

ПРИМЕЧАНИЕ. Рекомендуется заряжать МУ от зарядного устройства, входящего в комплект поставки, при этом предварительно следует выключить МУ.

5. ПОРЯДОК ОБНОВЛЕНИЯ

5.1. В рамках поддержки жизненного цикла Изделия предприятие-изготовитель вносит в него изменения, направленные на улучшение эксплуатационных характеристик и устранение недостатков.

5.2. Доведение информации о выпуске обновлений Изделия осуществляется до каждого потребителя Изделия путем отправки сообщений на электронные адреса потребителей и/или посредством публикации на официальном веб-сайте предприятия-изготовителя (https://www.omp.ru, https://auroraos.ru).

5.3. Предусмотрены следующие способы предоставления обновлений потребителям:

– отправка новой версии Изделия с сопроводительным письмом;

– публикация ISO образа загрузочного модуля новой версии Изделия на официальном веб-сайте предприятия-изготовителя (https://www.omp.ru, https://auroraos.ru);

– загрузка пакетов обновлений, полученных из официального репозитория предприятия-изготовителя.

5.4. Потребитель также имеет возможность получить информацию о выходе обновлений через службу технической поддержки предприятия-изготовителя по тел.: +7 (495) 269-09-80 или по электронной почте: support@omp.ru.

5.5. Обновления Изделия, при их наличии, вводятся в эксплуатацию после проведения дополнительных испытаний для поддержания Изделия в сертифицированном статусе. В случае внесения в Изделие изменений, связанных с устранением уязвимостей, предприятие-изготовитель информирует потребителей о необходимости обновления Изделия и доводит до потребителей обновления Изделия до проведения дополнительных испытаний. Автоматическое обновление сертифицированной версии Изделия не допускается.

5.6. Для установки сертифицированных обновлений оператор должен выполнить следующие действия:

– получить от предприятия-изготовителя Изделия сертифицированные обновления Изделия, а также обновленный в соответствии с извещением об изменениях комплект ЭД на Изделие;

– произвести проверку подлинности и целостности посредством проверки ЭП Изделия. Дополнительные материалы по работе с ЭП размещены на веб-сайте предприятия-изготовителя Изделия (https://auroraos.ru/documentation);

– провести расчет КС файлов сертифицированных обновлений Изделия с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.) «Уровень-3», константа по умолчанию;

– сравнить КС файлов обновлений с приведенными в соответствующем разделе обновленного формуляра на Изделие. При расхождении КС с эталонными значениями, приведенными в формуляре, необходимо обратиться в службу технической поддержки предприятия-изготовителя Изделия;

– в случае соответствия КС файлов сертифицированных обновлений Изделия эталонным значениям произвести установку сертифицированных обновлений Изделия в соответствии с требованиями, приведенными в документе АДМГ.40002-01 33 01.

5.7. Если потребитель Изделия не может реализовать компенсирующие меры по защите информации или ограничения по применению Изделия, то он прекращает его применение.

5.8. Если уязвимости (недекларированные возможности) Изделия не могут быть устранены с помощью компенсирующих мер по защите информации или ограничений по применению, предприятие-изготовитель Изделия незамедлительно и гарантированно, с подтверждением, сообщает об этом всем потребителям и ФСБ России. Потребители прекращают применение Изделия.

6. КОМПЛЕКТНОСТЬ

6.1. Комплектность поставки[3] Изделия должна соответствовать комплектности, указанной в таблице (Таблица 2) в строгой зависимости от способа передачи[4] и спецификации Изделия, предусмотренной в соответствующем Лицензионном договоре.

Таблица 2

Обозначение	Наименование	Кол.	Физическая поставка	Электронная поставка
АДМГ.40002-01	Программное средство криптографической защиты информации СледопытSSL	1	DVD с загрузочным модулем Изделия	В электронном виде
АДМГ.40002-01 30 01	Программное средство криптографической защиты информации СледопытSSL. Формуляр	1	В печатном виде (формат А5)[5]	В электронном виде
	Программное средство криптографической защиты информации СледопытSSL. Комплект эксплуатационных документов	1	В электронном виде на DVD	В электронном виде
Заверенная копия выданного ФСБ России сертификата соответствия на Программное средство криптографической защиты информации СледопытSSL		1	В печатном виде (формат А5)	В электронном виде

[3] Комплектность и версия Изделия при поставке определяются условиями Лицензионного договора.

[4] Общая информация о возможных способах передачи и носителях информации Изделия приведена в приложениях (Приложение 2, Приложение 3) настоящего документа.

[5] При физической поставке независимо от количества поставляемых комплектов ЭД формуляр на Изделие поставляется в 1 экземпляре на бумажном носителе на каждую партию МУ.

Комплект ЭД, входящей в поставку Изделия, определен в документе АДМГ.40002-01 20 01.

6.2. Изделие характеризуется следующими КС:

– КС RPM-пакетов, входящих в состав загрузочного модуля;

– КС системных файлов, выводимых на экран МУ.

КС RPM-пакетов, входящих в состав загрузочного модуля Изделия, рассчитаны с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.) «Уровень-3», константа по умолчанию.

КС системных файлов, выводимых на экран МУ, считаются с помощью ГОСТ для каждого файла, указанного ниже, с последующим сложением по модулю 2:

– /usr/bin/omp-notes;

– /usr/bin/securefs;

– /usr/sbin/randseedsrv;

– /usr/lib/engines-1.1/gost.so.1.1;

– /usr/lib/libcrypto.so.1.1;

– /usr/lib/libssl.so.1.1;

– /usr/lib/libnss3.so;

– /usr/lib/libnssdbm3.so;

– /usr/lib/libfreebl3.so;

– /usr/lib/libfreeblpriv3.so;

– /usr/lib/libsoftokn3.so;

– /usr/lib/libsmime3.so;

– /usr/lib/libssl3.so;

– /ust/sbin/sstored;

– /usr/lib/qt5/qml/ru/omprussia/sstore/libsstoreplugin.so;

– /usr/lib/qt5/qml/ru/omprussia/sstore/PasswordDialog.qml;

– /usr/lib/qt5/qml/ru/omprussia/sstore/PasswordResetDialog.qml;

– /usr/lib/qt5/qml/ru/omprussia/sstore/PasswordResetPage.qml;

– /usr/lib/qt5/qml/ru/omprussia/sstore/SStore.qml.

ВНИМАНИЕ! Функционирование сертифицированного Изделия возможно только после установки всех его компонентов. Признаком установки в ОС Аврора сертифицированного Изделия является вывод на экран МУ значений КС, указанных в таблице (Таблица 3).

Таблица 3

КС	Способ подсчета КС	Размер (байт)	КС (шестн.)
КС RPM-пакетов, входящих в состав загрузочного модуля	«ФИКС 2.0.2»	1648276	2d0e3173
КС системных файлов, выводимых на экран МУ	Сложение по модулю 2	98e7d246feffd4079c4b452937ab20b62bc7c4b7da60e7cb64814e597b6a829d	

6.3. КС RPM-пакетов, входящих в состав загрузочного модуля Изделия, рассчитывается следующим образом:

– из заголовка контролируемого elf-файла исключаются секции «.note.gnu.build-id» и «.gnu_debuglink»;

– секция «.note.gnu.build-id» содержит идентификатор, который генерируется редактором связей (GNU ld) при сборке исполняемого файла. Идентификатор намеренно меняется для каждой сборки, поэтому содержимое секции не должно учитываться при подсчете КС;

– секция «.gnu_debuglink» содержит имя файла с отладочными символами. Этот файл соответствует исполняемому и содержит тот же идентификатор «build-id». Таким образом, отладчик может проверить, что исполняемый файл и файл с отладочными символами соответствуют друг другу. Файл имеет название вида: «имя.версия.релиз.debug». Поскольку номер релиза инкрементируется при сборке, содержимое этой секции меняется и не должно учитываться при подсчете КС;

– выполняется расчет КС для каждого файла.

6.4. Для отображения информации о КС на экране МУ необходимо выполнить следующие действия:

– открыть меню настроек касанием значка  на Экране приложений;

– коснуться пункта меню «Контрольные суммы» системных настроек. На открывшейся странице отобразится информация о КС Изделия.

7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

7.1. Контроль Изделия проводится при его первичной установке и закреплении за ответственным лицом и в дальнейшем – в соответствии с порядком проведения регламентных работ комплекса средств автоматизации объекта, но не реже 1 раза в год.

7.2. Контроль Изделия включает визуальный осмотр DVD на предмет выявления механических повреждений и проверку сохранности информации, записанной на DVD.

7.3. Проверка сохранности информации осуществляется путем вычисления КС загрузочного модуля Изделия, размещенного на DVD. Вычисление КС проводится с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.), «Уровень-3», константа по умолчанию.

7.4. Результаты контроля основных характеристик при эксплуатации и хранении фиксируются в таблице (Таблица 4).

Таблица 4

Контрольная характеристика	Версия ПО	Дата проверки/ Подпись

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное средство криптографической защиты информации СледопытSSL (наименование программного изделия) АДМГ.40002-01 (обозначение) Зав. № _____

соответствует требованиям документа «Технические условия» АДМГ.40002-01 99 01 и признано годным для эксплуатации.

Выделенные регистрационные номера Изделия[6] _____

Количество экземпляров Изделия[7] _____

Дата выпуска

Руководитель предприятия[8] _____ (подпись) _____ (расшифровка подписи) _____ (дата)

М. П.

Ответственный исполнитель[9] _____ (подпись) _____ (расшифровка подписи) _____ (дата)

[6] Выделенные регистрационные номера Изделия регистрируются в Журнале учета регистрационных номеров Изделия.

[7] Подробная информация по изготовлению и вводу в эксплуатацию экземпляров Изделия должна приводиться в приложении (Приложение 1) настоящего документа.

[8] При электронной поставке маркирование Изделия осуществляется с применением ЭП, которая проставляется на титульном листе настоящего документа.

[9] При электронной поставке маркирование Изделия осуществляется с применением ЭП, которая проставляется на титульном листе настоящего документа.

9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

9.1. Предприятие-изготовитель гарантирует работоспособность Изделия в соответствии с заявленными характеристиками, предусмотренными настоящим документом, при соблюдении потребителем требований ЭД.

9.2. Предприятие-изготовитель проводит мониторинг общедоступных источников информации, публикующих сведения об уязвимостях, на предмет появления в них сведений об уязвимостях в компонентах Изделия, и принимает меры, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителями выявленных уязвимостей.

9.3. Предприятие-изготовитель обеспечивает устранение критических уязвимостей Изделия посредством предоставления потребителям описания необходимых организационно-технических процедур, направленных на устранение выявленной критической уязвимости. Также предприятие-изготовитель, в рамках проведения работ по устранению выявленных критических уязвимостей, разрабатывает обновления ПО.

9.4. Предприятие-изготовитель не предоставляет гарантий или условий (явных или подразумеваемых законодательством Российской Федерации) относительно товарной пригодности, интегрируемости, годности к использованию для выполнения конкретных задач потребителя, отсутствия ошибок, возможности функционирования при использовании совместно с любым программным или аппаратным обеспечением.

9.5. В случае выявления в Изделии ошибок и дефектов, свидетельствующих о несоответствии Изделия ЭД и не являющихся критическими уязвимостями Изделия, предприятие-изготовитель по факту получения рекламации потребителя обязуется устранить ошибки и/или дефекты при выпуске обновленных версий Изделия и уведомить об этом потребителей Изделия.

9.6. Рекламации потребителя принимаются при условии, что дефект в Изделии не вызван допущенными со стороны потребителя нарушениями при эксплуатации, хранении и транспортировке Изделия.

9.7. Адрес предприятия-изготовителя для направления рекламаций: 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Университетская, д. 7, офис 59, ОГРН 1161690087020.

10. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

10.1. Потребитель может предъявить рекламацию предприятию-изготовителю в период гарантийного срока эксплуатации Изделия при обнаружении дефектов функционирования Изделия, а также при несоответствии комплектности, упаковки и маркировки поставленного Изделия требованиям ЭД.

10.2. Рекламации предъявляются предприятию-изготовителю в письменном виде с указанием даты обнаружения неисправности (несоответствия), характера ее проявления и условий возникновения.

10.3. Рекламация подписывается руководителем подразделения, принимающего или эксплуатирующего Изделие.

10.4. Поступающие к предприятию-изготовителю рекламации регистрируются в журнале учета рекламаций (Таблица 5).

Таблица 5

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

11. СВЕДЕНИЯ О ХРАНЕНИИ

11.1. При электронной поставке Изделие распространяется по сетям связи. Процедура получения Изделия приведена в приложении (Приложение 2) настоящего документа.

11.2. При физической поставке DVD с загрузочным модулем Изделия и ЭД должны храниться в вертикальном положении на предназначенном для этой цели стеллаже в упаковке, поставленной предприятием-изготовителем, при температуре окружающего воздуха от +10°С до +20°С и относительной влажности воздуха от 20% до 65%.

11.3. В помещении для хранения не должно быть агрессивных примесей, вызывающих разрушение лакокрасочных покрытий и пластмасс.

11.4. При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°С/ч) и воздействия внешних магнитных полей напряженностью более 4000 А/м.

11.5. Сроки и условия хранения Изделия заносят в таблицу (Таблица 6).

Таблица 6

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

12. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

12.1. Изменения в Изделие разрешается вносить представителям предприятия-изготовителя в присутствии службы эксплуатации на основании бюллетеней об изменении.

12.2. Сведения об изменениях заносят в таблицу (Таблица 7).

Таблица 7

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись лица, ответственного за проведение изменения	Подпись лица, ответственного за эксплуатацию программного Изделия

13. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРИ ЭКСПЛУАТАЦИИ

13.1. Сведения о закреплении Изделия заносят в таблицу (Таблица 8). При первичном закреплении необходимо провести контроль Изделия в соответствии с разделом 7 настоящего документа.

ВНИМАНИЕ! Подробная информация по изготовлению и вводу в эксплуатацию экземпляров Изделия должна вноситься в приложение (Приложение 1) настоящего документа.

Таблица 8

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

14. ОСОБЫЕ ОТМЕТКИ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 9).

Таблица 9

Термин/ Сокращение	Расшифровка
Доверенное оконечное оборудование	Автоматизированная информационная система, обеспечивающая защищенное взаимодействие по протоколу TLS и реализующая криптографические алгоритмы: ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015
Изделие	Программное средство криптографической защиты информации СледопытSSL (вариант исполнения № 1)
Криптоконтейнер	Криптографический контейнер
КС	Контрольная сумма
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ПО	Программное обеспечение
Предприятие-изготовитель	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
СКЗИ	Средство криптографической защиты информации
СКЗИ СледопытSSL	Программное средство криптографической защиты информации СледопытSSL (вариант исполнения № 1)
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭД	Эксплуатационная документация
ЭП	Электронная подпись
CMS	Cryptographic Message Syntax – синтаксис криптографических сообщений

Термин/ Сокращение	Расшифровка
DVD	Digital Video Disc – оптический носитель информации, выполненный в форме диска, для хранения различной информации в цифровом виде
HMAC	Hash-Based Message Authentication Code – код аутентификации (проверки подлинности) сообщений, использующий хеш-функции. Один из механизмов проверки целостности информации, позволяющий гарантировать то, что данные, передаваемые или хранящиеся в ненадежной среде, не были изменены посторонними лицами
IMEI	International Mobile Equipment Identity – уникальный номер МУ, состоящий из 15 цифр
ISO-образ	Образ оптического диска, содержащий файловую систему стандарта ISO 9660
RPM-пакет	Файл формата RPM, позволяющий устанавливать, удалять и обновлять приложение на МУ
SSL	Secure Sockets Layer – криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером
TLS	Transport Layer Security – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет
WLAN	Wireless Local Area Network – локальная сеть, построенная на основе беспроводных технологий

ПРИЛОЖЕНИЕ 1

Изготовление и ввод в эксплуатацию экземпляров Изделия[10]

Изготовление и ввод в эксплуатацию экземпляров Изделия приведены в таблице (Таблица 1.1).

Таблица 1.1

№ экземпляра Изделия	IMEI МУ	Модель МУ	Дата установки Изделия на МУ	Выделенные регистрационные номера Изделия	Потребитель Изделия	Подпись ответственного лица	Должность, фамилия ответственного лица

[10] В раздел 14 настоящего документа также может быть внесена необходимая дополнительная информация, связанная с эксплуатацией Изделия потребителем.

ПРИЛОЖЕНИЕ 2

Общие положения предприятия-изготовителя по возможным вариантам поставки Изделия

Основные положения по получению Изделия потребителем:

1. Изделие поставляется в строгом соответствии с Лицензионным договором;

2. Комплектность Изделия соответствует положениям раздела 6 настоящего документа и условиям Лицензионного договора;

3. Варианты носителей информации Изделия могут быть следующими:

– поставка на электронном носителе: DVD – оптический носитель информации, при этом DVD изготавливается предприятием-изготовителем Изделия и передается потребителю в подготовленном виде, в соответствии с положениями документа «Технологическая инструкция изготовления изделия. Программное средство криптографической защиты информации СледопытSSL»;

– поставка по электронным каналам связи: информационный ресурс предприятия-изготовителя, информация по доступу, а также правила работы с ним доводятся до потребителя при заключении Лицензионного договора. Подлинность и целостность Изделия обеспечивается применением ЭП.

Способ передачи Изделия по электронным каналам связи предусматривает следующее обязательное условие: подготовка DVD, входящих в комплект поставки Изделия, производится на стороне потребителя.

Пример маркировки с указанием обязательных полей подготовленного потребителем DVD приведен в приложении (Приложение 3) настоящего документа.

При передаче Изделия по электронным каналам связи потребитель должен выполнить следующие действия:

– после загрузки загрузочного модуля Изделия и комплекта ЭД необходимо произвести проверку подлинности и целостности путем проверки ЭП[11];

– произвести расчет КС DVD Изделия с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.) «Уровень-3», константа по умолчанию;

– сравнить значения КС с приведенными в соответствующем разделе обновленного формуляра на Изделие. При расхождении КС с эталонными значениями, приведенными в формуляре, необходимо обратиться в службу технической поддержки предприятия-изготовителя.

[11] Дополнительные материалы по работе с ЭП размещены на веб-сайте предприятия-изготовителя: https://auroraos.ru/documentation.

ПРИЛОЖЕНИЕ 3

Пример маркировки DVD с Изделием

1. Пример маркировки

Маркировка DVD, входящего в комплект поставки Изделия, должна быть выполнена в соответствии с примером оформления, приведенным на рисунке[12] (Рисунок 3.1).

Рисунок 3.1

[12] На рисунке (Рисунок 3.1) приведен пример маркировки DVD с загрузочным модулем Изделия.

2. Описание полей маркировки

Описание полей маркировки DVD при электронной поставке Изделия приведено в таблице (Таблица 3.1).

Таблица 3.1

Поле	Информация по заполнению	Примечания
Наименование Изделия	Соответствует положениям раздела 6 настоящего документа и условиям Лицензионного договора	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия
Обозначение Изделия (децимальный номер)	АДМГ.40002-01	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия
Дата изготовления	Проставляется в соответствии с актом приема-передачи Изделия. Также может быть проставлена дата фактического изготовления DVD	Поле является обязательным к заполнению при любом из возможных вариантов и способов поставки Изделия
Контрольная сумма	Соответствует положениям раздела 6 (Таблица 3) настоящего документа и условиям Лицензионного договора	Поле является обязательным к заполнению ТОЛЬКО для DVD, содержащего загрузочный модуль Изделия. Заполняется при любом из возможных вариантов и способов поставки Изделия
Зав. №	Соответствует положениям раздела 8 настоящего документа и условиям Лицензионного договора	Поле является обязательным к заполнению ТОЛЬКО для DVD, содержащего загрузочный модуль Изделия. Заполняется при любом из возможных вариантов и способов поставки Изделия

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					