

УТВЕРЖДЕН  
РОФ.42584334.58.29.12.01 30 01-ЛУ

Программное обеспечение «Мультифактор»

Формуляр

РОФ.42584334.58.29.12.01 30 01

Листов 34

**СОДЕРЖАНИЕ**

1. Общие указания .....	3
2. Общие сведения .....	4
3. Основные характеристики .....	5
3.1 Требования к безопасности Изделия .....	9
3.1.1 Идентификация и аутентификация пользователей .....	9
3.1.2 Управление доступом пользователей .....	11
3.1.3 Регистрация событий безопасности .....	12
4. Комплектность .....	14
5. Периодический контроль основных характеристик при эксплуатации и хранении .....	17
6. Свидетельство о приемке .....	18
7. Свидетельство об упаковке и маркировке .....	19
8. Указания по эксплуатации .....	20
8.1 Указания по обновлению .....	20
8.2 Указания по устранению уязвимостей .....	22
9. Гарантийные обязательства .....	25
10. Сведения о рекламациях .....	27
11. Сведения о хранении .....	28
12. Сведения о закреплении при эксплуатации .....	29
13. Сведения об изменениях .....	30
14. Особые отметки .....	31
ПРИЛОЖЕНИЕ А .....	33

## 1. Общие указания

Настоящий формуляр на программное обеспечение «Мультифактор» (далее — Изделие, ПО «Мультифактор»), является документом, удостоверяющим гарантированные предприятием-изготовителем основные характеристики Изделия, определяющим комплект поставки и содержащим сведения об изменениях в эксплуатационной документации, а также другие данные за весь период эксплуатации.

Перед эксплуатацией Изделия необходимо внимательно ознакомиться с комплектом документации, поставляемой с Изделием.

В случае обнаружения дефектов на компакт-дисках с загрузочными модулями следует обращаться к изготовителю ООО «Мультифактор».

Все записи в формуляре должны производиться черными или синими чернилами, тушью или пастой отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления не допускаются.

Формы в разделах 10–13 заполняются пользователем. Формы в разделах 6 и 7 заполняются предприятием-изготовителем при передаче Изделия пользователю.

Формуляр должен находиться у должностного лица (администратора службы безопасности информации), ответственного за эксплуатацию ПО «Мультифактор». Все записи в Формуляре должны производиться только чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления не допускаются. Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет ответственное лицо. После подписи проставляют фамилию и инициалы ответственного лица (штамп исполнителя).

## 2. Общие сведения

Наименование изделия: Программное обеспечение «Мультифактор».

Обозначение: РОФ.42584334.58.29.12.01.

Тип изделия: программное обеспечение.

Разработчик и производитель: ООО "МУЛЬТИФАКТОР" (115162, г. Москва, вн.тер.г. Муниципальный Округ Донской, ул Шухова, д. 14, этаж 4, помещение 13, офис 407), <https://multifactor.ru>.

Лицензия на деятельность по разработке и (или) производству средств защиты конфиденциальной информации ФСТЭК России № Л050-00107-77/01567361 от 26.11.2024.

Изделие при выполнении указаний по эксплуатации может применяться в государственных информационных системах до 1-го класса защищенности включительно в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17, в информационных системах персональных данных до 1-го уровня защищенности включительно в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21, в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с Приказом ФСТЭК России от 14.03.2014 № 31, а также в значимых объектах критической информационной инфраструктуры Российской Федерации до 1 категории значимости включительно в соответствии с Приказом ФСТЭК России от 25.12.2017 № 239.

Сведения о сертификации. Система сертификации средств защиты информации по требованиям защиты информации № РОСС RU.0001.01БИ00 (ФСТЭК России). Сертификат соответствия № \_\_\_\_\_, дата внесения в Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 – \_\_\_\_\_.

Пример записи продукции в других документах и (или) при заказе: ПО «Мультифактор».

### 3. Основные характеристики

ПО «Мультифактор» представляет собой систему двухфакторной аутентификации, обеспечивающее защиту учётных записей сотрудников, путем добавления второго фактора при доступе к любым корпоративным ресурсам (VPN, VDI, Windows и Linux-инфраструктура, облачные приложения) с поддержкой технологии единого входа (SSO).

В состав ПО «Мультифактор» входят: управляющий сервер (далее платформа ПО «Мультифактор»), компоненты, разворачивающиеся в периметре клиента и мобильное приложение Мультифактор.

#### Платформа ПО «Мультифактор»

В платформу ПО «Мультифактор» входят следующие компоненты:

- Личный кабинет администратора ПО «Мультифактор»;
- Партнёрский кабинет ПО «Мультифактор»;
- Суперпанель администратора, служащая для управления остальными личными кабинетами ПО «Мультифактор»;
- Сервер авторизации ПО «Мультифактор»;
- API управления пользователями ПО «Мультифактор»;
- СУБД MongoDB (версии r6.0.14);

В состав среды функционирования для платформы ПО «Мультифактор» входят:

- Программное обеспечение «Deckhouse Platform Certified Security Edition» (сертификат соответствия №4860, действителен до 04.10.2029) или оркестратор контейнеров из состава репозитория Astra Special Edition (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026);
- RabbitMQ (версии 3.8.1 и выше из состава репозитория Astra Special Edition сертифицированная версия из государственного реестра сертифицированных средств защиты информации ФСТЭК).

Поддерживаемые ОС:

- Astra Linux (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026)

Дополнительные требования:

- Для функционирования Изделия необходима установка .NET 6 и 8 из состава репозитория Astra Special Edition сертификат соответствия №2557, действителен до 27.01.2026).

Таблица 1 – Аппаратные требования к платформе ПО «Мультифактор».

Параметр	Значение
Количество ядер процессора	от 28
Объем ОЗУ	от 54 GB
Свободное место на жестком диске или твердотельном накопителе	от 1720 GB

К компонентам ПО «Мультифактор», имеющим подключение к управляющему серверу, относятся:

**MultiFactor Radius Adapter** — RADIUS сервер, разработанный и поддерживаемый компанией Мультифактор для двухфакторной аутентификации пользователей при использовании удаленного доступа.

Таблица 2 – Аппаратные требования Radius сервера для Windows

Параметр	Значение
Количество ядер процессора	от 2
Объем ОЗУ	от 4 GB
Свободное место на жестком диске или твердотельном накопителе	от 40 GB

Таблица 3 – Аппаратные требования Radius сервера для Linux

Параметр	Значение
Количество ядер процессора	от 1
Объем ОЗУ	от 2 GB
Свободное место на жестком диске или твердотельном накопителе	от 8 GB

Поддерживаемые ОС:

- Astra Linux (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026)
- РЕД ОС (сертификат соответствия №4060, действителен до 12.01.2029)
- АЛБТ (версия 8 СП, сертификат соответствия №3866, действителен до 10.08.2028)
- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 (релизы Standart или Datacenter) и выше;

**MultiFactor Ldap Adapter** — LDAP проху сервер, разработанный и поддерживаемый компанией Мультифактор для двухфакторной аутентификации пользователей в приложениях, использующих LDAP аутентификацию.

Таблица 4 – Аппаратные требования Ldap сервера для Windows

Параметр	Значение
Количество ядер процессора	от 2
Объем ОЗУ	от 4 GB
Свободное место на жестком диске или твердотельном накопителе	от 40 GB

Таблица 5 – Аппаратные требования Ldap сервера для Linux

Параметр	Значение
Количество ядер процессора	от 1
Объем ОЗУ	от 2 GB
Свободное место на жестком диске или твердотельном накопителе	от 8 GB

Поддерживаемые ОС:

- Astra Linux (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026)
- РЕД ОС (сертификат соответствия №4060, действителен до 12.01.2029)
- АЛБТ (версия 8 СП, сертификат соответствия №3866, действителен до 10.08.2028)
- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 (релизы Standart или Datacenter) и выше;

**MultiFactor SelfService Portal** — веб-сайт, разработанный и поддерживаемый компанией Мультифактор для самостоятельной регистрации второго фактора аутентификации пользователями с учётными записями из Active Directory или других LDAP каталогов в том числе ALD Pro, входящий в «Единый реестр российских программ для ЭВМ и баз данных».

Таблица 6 – Аппаратные требования SelfService Portal для Windows

Параметр	Значение
Количество ядер процессора	от 2
Объем ОЗУ	от 4 GB
Свободное место на жестком диске или твердотельном накопителе	от 40 GB

Таблица 7 – Аппаратные требования SelfService Portal для Linux

Параметр	Значение
Количество ядер процессора	от 1
Объем ОЗУ	от 2 GB
Свободное место на жестком диске или твердотельном накопителе	от 8 GB

Поддерживаемые ОС:

- Astra Linux (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026)
- РЕД ОС (сертификат соответствия №4060, действителен до 12.01.2029)
- АЛЪТ (версия 8 СП, сертификат соответствия №3866, действителен до 10.08.2028)
- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 (релизы Standart или Datacenter) и выше;

**MultiFactor Logon** — программный компонент, экран входа в операционную систему Windows. Работает как при локальном входе в операционную систему, так и при подключениях через удалённый рабочий стол.

Поддерживаемые ОС:

- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 Standart и выше, Microsoft Windows Server 2016 Datacenter и выше;

**MultiFactor.ADFS.Adapter** — плагин для Active Directory Federation Services (ADFS), разработанный и поддерживаемый компанией Мультифактор для двухфакторной аутентификации пользователей, при доступе к корпоративным приложениям через ADFS.

Требования для установки:

- Компоненту необходим доступ к хосту *api.multifactor.ru* по TCP порту 443 (TLS) напрямую или через HTTP прокси;
- На сервере должно быть установлено правильное время.

Поддерживаемые ОС:

- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 Standart и выше, Microsoft Windows Server 2016 Datacenter и выше;

**MultiFactor.IIS.Adapter** — программный компонент, разработанный и поддерживаемый компанией Мультифактор, расширение для Microsoft Exchange Server. Позволяет подключить мультифакторную аутентификацию пользователей к Outlook Web Access (OWA).

Требования для установки:

- Компоненту необходим доступ к хосту *api.multifactor.ru* по TCP порту 443 (TLS) напрямую или через HTTP прокси;
- Outlook Web Access должен работать с валидным SSL сертификатом.
- На сервере должно быть установлено правильное время.

Поддерживаемые ОС:

- Клиентские ОС семейства Windows: Microsoft Windows 10 и выше;
- Серверные ОС семейства Windows: Microsoft Windows Server 2016 Standart и выше, Microsoft Windows Server 2016 Datacenter и выше;

**Ram\_mf** — РАМ модуль разработанный и поддерживаемый компанией Мультифактор, для двухфакторной аутентификации пользователей в системах с ОС Linux.

Поддерживаемые ОС:

- Astra Linux (версия Special Edition, сертификат соответствия №2557, действителен до 27.01.2026)
- РЕД ОС (сертификат соответствия №4060, действителен до 12.01.2029)
- АЛБТ (версия 8 СП, сертификат соответствия №3866, действителен до 10.08.2028)

**Мобильное приложение Multifactor** является собственной разработкой компании Мультифактор, дистрибутив предоставляется в соответствии со спецификацией. В мобильном приложении предусмотрен прямой способ подтверждения второго фактора или через генерацию одноразовых паролей. В приложении имеются возможность настройки наложенных мер обеспечения безопасности информации от утечки, например, дополнительный пароль при входе.

Поддерживаемые ОС:

- Аврора: версия 4.0 и выше.

### **3.1 Требования к безопасности Изделия**

#### **3.1.1 Идентификация и аутентификация пользователей**

3.1.1.1 ПО «Мультифактор» обеспечивает однозначную идентификацию и аутентификацию пользователей при их доступе в систему. (ИАФ.1)

3.1.1.2 При доступе к ПО «Мультифактор» осуществляется идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. (ИАФ.1)

3.1.1.3 Аутентификация пользователей в Изделии должна осуществляться с использованием следующего набора факторов аутентификации: мобильное приложение Multifactor, OTP аппаратный токен, HOTP Токен, OTP программный Токен Google authenticator/Я Ключ, СМС сообщение, звонок на мобильное устройство, универсальный метод подтверждения второго фактора. (ИАФ.1)

3.1.1.4 В ПО «Мультифактор» обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами. (ИАФ.1)

3.1.1.5 В ПО «Мультифактор» обеспечивается многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

- с использованием сети связи общего пользования, в том числе сети Интернет;

3.1.1.6 ПО «Мультифактор» обеспечивает многофакторную (двухфакторную) аутентификацию для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

- с использованием сети связи общего пользования, в том числе сети Интернет;

3.1.1.7 В ПО «Мультифактор» обеспечивается многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ.

3.1.1.8 ПО «Мультифактор» использует механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ.

3.1.1.9 В ПО «Мультифактор» обеспечены следующие функции управления идентификаторами пользователей:

- определение администратора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей;
- формирование идентификатора, который однозначно идентифицирует пользователя;
- присвоение идентификатора пользователю;
- блокирование идентификатора пользователя. (ИАФ.3)

3.1.1.10 ПО «Мультифактор» обеспечивает следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей:

- изменение аутентификационной информации (средств аутентификации);

- установление характеристик пароля: задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

Для нового пользователя:

- должен содержать цифры и буквы;
- должен быть более 12 символов;
- при интеграции с LDAP каталогами компоненты используют политику заданную в LDAP каталоге.

Для существующего пользователя (смена/восстановление пароля):

- должен содержать цифры и буквы;
- должен быть не короче 12 символов;
- не должен совпадать с предыдущими 4-мя паролями этого пользователя;
- при интеграции с LDAP каталогами компоненты используют политику заданную в LDAP каталоге. (ИАФ.4)

3.1.1.11 В ПО «Мультифактор» осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля отображаются условными знаками «точка». (ИАФ.5)

### **3.1.2 Управление доступом пользователей**

3.1.2.1 В ПО «Мультифактор» установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- объединение учетных записей в группы;
- заведение, активация, блокирование и уничтожение учетных записей пользователей. (УПД.1)

3.1.2.2 Методы управления доступом администраторов ПО «Мультифактор» включают ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности администратора). (УПД.2)

3.1.2.3 Типы доступа пользователей в ПО «Мультифактор» включают операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению

пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа. (УПД.2)

3.1.2.4 Правила разграничения доступа реализуются для пользователей, на основании групповых политик в личном кабинете Мультифактор, для администраторов на основании присвоения роли в личном кабинете Мультифактор.

3.1.2.5 В ПО «Мультифактор» правила разграничения доступа обеспечивают управление доступом субъектов (администраторов и пользователей) при входе в информационную систему.

3.1.2.6 В ПО «Мультифактор» установлено ограничение количества неуспешных попыток входа (по умолчанию 4) за период времени (по умолчанию 90 секунд), установленный оператором, а также обеспечено блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ПО. (УПД.6)

3.1.2.7 В ПО «Мультифактор» обеспечивается завершение сеанса пользователя (выхода из системы) после превышения установленного оператором времени бездействия (неактивности) пользователя по умолчанию 30 минут. (УПД.10)

3.1.2.8 Для заблокированного сеанса осуществляется блокирование любых действий по доступу к ПО «Мультифактор», кроме необходимых для разблокирования сеанса. (УПД.10)

3.1.2.9 Блокирование сеанса доступа пользователя ПО «Мультифактор» сохраняется до прохождения им повторной идентификации и аутентификации. (УПД.10)

3.1.2.10 В изделии установлен перечень действий пользователей, разрешённых до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешённых действий, до прохождения ими процедур идентификации и аутентификации. В перечень разрешённых действий входит регистрация нового кабинета администратора и запрос на восстановления забытого пароля. (УПД.11)

### **3.1.3 Регистрация событий безопасности**

3.1.3.1 Изделие обеспечивает регистрацию и хранение следующих событий информационной безопасности:

- вход и попытки входа субъектов доступа, включая процедуры аутентификации;
- действия, совершаемые с использованием привилегированных учетных записей;
- операции с критически важными данными и системными настройками.

Для зарегистрированных событий безопасности устанавливаются и поддерживаются регламентированные сроки хранения соответствующих записей. (РСБ.1)

3.1.3.2 В изделии определен состав и содержание информации о событиях безопасности, подлежащих регистрации. (РСБ.2)

3.1.3.3 ПО «Мультифактор» осуществляет генерацию (сбор, запись) и хранение записей регистрации (аудита) для событий безопасности в течение установленного оператором времени хранения. (РСБ.3)

3.1.3.4 В ПО «Мультифактор» осуществляется синхронизация системного времени. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ПО «Мультифактор» достигается посредством применения внутренних системных часов информационной системы. (РСБ.6)

Соответствие функций безопасности Изделия мерам по обеспечению безопасности, приведенным в Приказе 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», Приказе ФСТЭК России от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказе ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а также в методическом документе от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах», приведено в Таблице 7.

Таблица 8 – Функциональные возможности Изделия по выполнению требований к мерам защиты в информационных системах

Приказ №17 <sup>1</sup>	Приказ №21 <sup>2</sup>	Приказ №31 <sup>3</sup>	Приказ №239 <sup>4</sup>	№ пункта требований назначения
ИАФ.1	ИАФ.1	ИАФ.1	ИАФ.1	3.1.1.1 3.1.1.2 3.1.1.3 3.1.1.4
ИАФ.3	ИАФ.3	ИАФ.3	ИАФ.3	3.1.1.9
ИАФ.4	ИАФ.4	ИАФ.4	ИАФ.4	3.1.1.10
ИАФ.5	ИАФ.5	ИАФ.7	ИАФ.7	3.1.1.11
УПД.1	УПД.1	УПД.1	УПД.1	3.1.2.1
УПД.2	УПД.2	УПД.2	УПД.2	3.1.2.2 3.1.2.3 3.1.2.4
УПД.6	УПД.6	УПД.6	УПД.6	3.1.2.6
УПД.10	УПД.10	УПД.10	УПД.10	3.1.2.7 3.1.2.8 3.1.2.9
УПД11	УПД11	УПД11	УПД11	3.1.2.10
РСБ.1	РСБ.1	АУД.1	АУД.1	3.3.1.1
РСБ.2	РСБ.2	АУД.2	АУД.2	3.3.1.2
РСБ.3	РСБ.3	АУД.4	АУД.4	3.3.3.3
РСБ.6	РСБ.6	АУД.6	АУД.6	3.3.3.4

<sup>1</sup> Меры защиты информации в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17)

<sup>2</sup> Меры защиты информации в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21)

<sup>3</sup> Меры защиты информации в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31)

<sup>4</sup> Меры защиты информации в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239)

#### 4. Комплектность

Поставка Изделия осуществляется согласно спецификации. Комплектность поставки приведена в Таблице (Таблица 9).

Таблица 9 – Комплектность поставки.

№ п/п	Наименование (обозначение)	Кол-во	Примечание
1 <sup>5</sup>	Дистрибутив ПО «Мультифактор» РОФ.42584334.58.29.12.01.02	В соответствии со спецификацией	Размещается на usb-носителе
1.2 <sup>5</sup>	Дистрибутив ПО «Мультифактор» (мобильное приложение) РОФ.42584334.58.29.12.01.03	В соответствии со спецификацией	Размещается на usb-носителе
1.3 <sup>5</sup>	Дистрибутив ПО «Мультифактор» (коннекторы) РОФ.42584334.58.29.12.01.04	В соответствии со спецификацией	Размещается на usb-носителе
1.3 <sup>5</sup>	Платформа ПО «Мультифактор» РОФ.42584334.58.29.12.01.01	В соответствии со спецификацией	Размещается на компакт диске
2	Формуляр РОФ.42584334.58.29.12.01 30 01	1	На бумажном носителе
3	Электронное приложение к Формуляру РОФ.42584334.58.29.12.01 30 01-CD	1	Размещается на usb-носителе
4	Заверенная копия сертификата ФСТЭК России	1	На бумажном носителе
5	Руководство администратора РОФ.42584334.58.29.12.01 РА 01	1	Размещается на usb-носителе
6	Руководство оператора (пользователя)	1	Размещается на usb-носителе

<sup>5</sup> Поставка дистрибутива Изделия осуществляется в соответствии со спецификацией на покупку Изделия.

№ п/п	Наименование (обозначение)	Кол-во	Примечание
	РОФ.42584334.58.29.12.01 РП 01		
7	Упаковка	1	

## **5. Периодический контроль основных характеристик при эксплуатации и хранении**

Контроль основных характеристик Изделия осуществляется:

- непосредственно перед установкой Изделия посредством расчета контрольных сумм файлов дистрибутива Изделия;
- непосредственно после установки Изделия посредством расчета контрольных сумм файлов на жестком диске программно-аппаратного комплекса после инсталляции;
- периодически при выполнении контроля посредством расчета итогового значения контрольных сумм файлов, установленных на жесткий диск программно-аппаратного комплекса;
- непосредственно после обновления Изделия.

Расчет контрольных сумм файлов поставляемого комплекта Изделия осуществляется по алгоритму «Уровень-1, программно» с использованием специализированной программы «ФИКС» (версии 2.0.2).

Соответствие контрольных сумм подтверждает подлинность ПО «Мультифактор» и его соответствие требованиям Технических условий РОФ.42584334.58.29.12.01 90 01.

Контрольные суммы файлов компакт-диска должны соответствовать контрольным суммам, указанным в приложении А настоящего документа.

**6. Свидетельство о приемке**

Изделие РОФ.42584334.58.29.12.01 соответствует Техническим условиям РОФ.42584334.58.29.12.01 90 01 и признано годным к эксплуатации.

Заводской номер \_\_\_\_\_

Дата выпуска: \_\_\_\_\_

Ответственный за технический контроль продукции ООО «МУЛЬТИФАКТОР»

М.П.

\_\_\_\_\_  
личная подпись\_\_\_\_\_  
расшифровка подписи\_\_\_\_\_  
год, месяц, число



## **8. Указания по эксплуатации**

При эксплуатации изделия требуется соблюдение следующих рекомендаций и ограничений при эксплуатации:

- регламентация запрета применения изделия для защиты информации, содержащей сведения, составляющие государственную тайну;
- использование сертифицированных операционных систем и/или системных средств защиты информации при применении изделия для защиты информации конфиденциального характера;
- наличие администратора информационной безопасности Изделия, отвечающего за необходимую настройку политик безопасности;
- сохранение в секрете паролей пользователей Изделия;
- обеспечение физической защиты технических средств, на которых развернуто Изделие, а также наличие надежных препятствий для несанкционированного проникновения в помещение с Изделием;
- периодическое тестирование (не реже одного раза в год) функций защиты Изделия администратором информационной безопасности;
- периодическая проверка программной среды автоматизированного рабочего места, используемого в качестве административной консоли, и сервера с установленным Изделием на наличие вредоносного программного обеспечения;
- использование средств периодического контроля за целостностью программной части Изделия;
- регистрация результатов тестирования и проверок Изделия в формуляре.

Для того чтобы ПО «Мультифактор» функционировало корректно и не нарушались требования по безопасности Изделия (в том числе — необходимые организационные меры), необходимо соблюдать указанные ниже условия установки и функционирования.

ПО «Мультифактор» должно устанавливаться и администрироваться специалистом, обладающим достаточной квалификацией для работы и администрирования Изделия.

Изделие должно устанавливаться и администрироваться в соответствии с документом «Руководство администратора».

### **8.1 Указания по обновлению**

Перед установкой ПО «Мультифактор» необходимо установить все обновления безопасности для среды функционирования Изделия. В ходе эксплуатации Изделия администратор безопасности должен периодически, не реже одного раза в три месяца, осуществлять поиск уязвимостей среды функционирования в общедоступных источниках

информации об уязвимостях. В качестве общедоступных источников в первую очередь должна использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также некоторые дополнительные источники, например, securitylab.ru, cve.mitre.org и др. В случае обнаружения информации об уязвимостях среды функционирования администратор безопасности должен выполнить поиск и установку обновлений безопасности операционной системы, устраняющих выявленные уязвимости. При отсутствии обновлений безопасности администратор обращается в техническую поддержку разработчика Изделия.

Администратор безопасности должен получать информацию о выходе обновлений Изделия посредством электронной рассылки. Обновления, не связанные с безопасностью, устанавливаются после внесения изменений в Изделие и после согласования материалов проведенных испытаний со стороны ФСТЭК России (в том числе — после завершения процедуры переоформления сертификата соответствия, если это требуется). Обновления, связанные с устранением уязвимостей (недекларированных возможностей) Изделия, устанавливаются до проведения испытаний, о чем разработчик информирует потребителей посредством электронной рассылки. Перед установкой полученных от разработчика обновлений Изделия администратор должен выполнить контроль их целостности путем подсчета контрольных сумм файлов обновления и их сравнения со значениями, указанными разработчиком.

Изделие собрано и сконфигурировано таким образом, чтобы в ходе установки правильно применялись все необходимые меры и политики безопасности, которые предотвращают возможность реализации существующих угроз безопасности. Для поддержания данного состояния необходимо после установки ПО «Мультифактор»:

- не менять параметры среды функционирования Изделия;
- не открывать другие дополнительные порты и интерфейсы для передачи данных среды функционирования Изделия кроме тех, которые используются для работы Изделия;
- не создавать новых учетных записей пользователей среды функционирования Изделия;
- обеспечить конфиденциальность аутентификационных данных (логина и пароля) пользователя с правами администратора среды функционирования Изделия;

- обеспечить защиту канала связи администратора безопасности с консолью управления Изделия (организационно-техническими мерами и/или с использованием средств криптографической защиты информации).

## 8.2 Указания по устранению уязвимостей

Процедуры устранения уязвимостей в сертифицированном Изделии обеспечивают возможность обновления программного обеспечения для устранения актуальных уязвимостей. Устранение уязвимостей должно осуществляться разработчиком Изделия посредством выполнения мероприятий организационно-технического характера.

Разработчик Изделия периодически, не реже одного раза в месяц, должен проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях средств защиты информации (СЗИ) и средах их функционирования. В качестве общедоступных источников в первую очередь должна использоваться база данных уязвимостей в составе банка данных угроз (БДУ) безопасности информации ФСТЭК России ([bdu.fstec.ru](http://bdu.fstec.ru)), а также некоторые дополнительные источники, например, [securitylab.ru](http://securitylab.ru), [cve.mitre.org](http://cve.mitre.org) др.

Поиск информации в базах данных по уязвимостям проводят с целью проверки соответствия функциональных возможностей СЗИ требованиям, указанным в ТУ и задании по безопасности, а также требованиям безопасной эксплуатации средства на месте установки.

По результатам поиска разработчик должен провести анализ выявленных уязвимостей СЗИ и среды его функционирования.

При анализе уязвимостей необходимо учитывать следующие критерии:

- тип ошибки;
- версию программного обеспечения, подверженную уязвимости;
- уровни опасности уязвимости:
  - критическая (critical);
  - высокая (high);
  - средняя (medium);
  - низкая (low);
- информацию об устранении.

В случае выявления информации об уязвимости СЗИ, среды его функционирования и отсутствия информации об этой уязвимости в БДУ разработчик предоставляет информацию о данной уязвимости во ФСТЭК России для размещения в БДУ.

По результатам анализа выявленных уязвимостей разработчик выполняет тестирование на проникновение средства защиты информации в используемой среде функционирования. В случае обнаружения пригодных для использования уязвимостей разработчик выполняет мероприятия, указанные далее.

При выявлении уязвимостей в СЗИ разработчик должен выполнить следующие мероприятия:

- разослать информационное сообщение об уязвимостях в СЗИ посредством электронной рассылки;
- выполнить сборку СЗИ с устраненными уязвимостями (разработать патч);
- разработать и предоставить конечным пользователям перечень (регламент) организационно-технических мероприятий, направленных на недопущение попыток использования выявленных уязвимостей злоумышленниками, посредством электронной рассылки **в срок не более 60 дней с момента обнаружения уязвимости;**
- **разработать компенсирующие меры по защите информации или ограничений по применению средства, а также довести информации о таких мерах и ограничениях до потребителей в срок не более 48 часов с момента обнаружения уязвимости;**
- подготовить извещение об изменениях в СЗИ, внести необходимые изменения в эксплуатационную документацию и представить их в испытательную лабораторию и ФСТЭК России;
- провести работы по контролю устранения выявленных уязвимостей в испытательной лаборатории;
- при положительном результате контроля устранения выявленных уязвимостей оповестить конечных пользователей СЗИ о необходимости установки обновленной версии (патча) СЗИ и предоставить им:
  - заверенную копию обновленного сертификата ФСТЭК России;
  - файлы с обновленной версией СЗИ, с наложенной на них электронной цифровой подписью. Файлы должны быть переданы с информационного ресурса разработчика <https://multifactor.ru/> ;
  - заверенную копию измененного формуляра;
- в случае невозможности устранения уязвимостей средства защиты информации, в том числе путем применения обновления, разработчик определяет ограничения по применению СЗИ, которые незамедлительно доводит до испытательной лаборатории;
- если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, разработчик незамедлительно и

гарантированно с подтверждением доводит его до пользователей. Пользователи реализуют указанное ограничение по применению СЗИ. Если пользователи не могут реализовать ограничение по применению СЗИ, они прекращают его применение;

– если уязвимость не устраняется путем установления ограничений по применению, разработчик незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и ФСТЭК России. Пользователи прекращают применение средства защиты информации.

## **9. Гарантийные обязательства**

Срок гарантийного обслуживания ПО «Мультифакто» составляет 60 месяцев.

В течение гарантийного срока Изготовитель обязуется обеспечивать техническую поддержку Изделия, при условии соблюдения Заказчиком условий и правил хранения, транспортирования и эксплуатации. Базовая техническая поддержка включает в себя:

- производство безвозмездной замены дефектного программного изделия (включая замену носителей с дистрибутивами программного изделия);
- обеспечение устранения уязвимостей и недеklarированных возможностей программного изделия;
- информирование потребителей об обновлении программного изделия;
- доведение до потребителей дистрибутивных файлов обновлений и изменений в эксплуатационной документации.

В случае внесения Заказчиком в период эксплуатации программного изделия каких-либо изменений в дистрибутив, программные компоненты или документацию без согласования с Изготовителем, действие гарантийных обязательств на ПО «Мультифакто» прекращается с момента начала внесения изменений.

Носители с дистрибутивами ПО «Мультифакто» должны обеспечивать возможность хранения информации и чтения ее с машинных носителей в течение срока гарантийного обслуживания, начиная со дня ввода в эксплуатацию. Создание собственных копий дистрибутива изделия или его компонентов без согласования с Изготовителем запрещено. Гарантийные обязательства не распространяются на копии дистрибутивов изделия, машинного носителя, эксплуатационной документации, изготовленных по инициативе Заказчика.

Гарантийные обязательства не распространяются на случаи нарушения работоспособности ПО «Мультифакто», связанные с несоблюдением конечными пользователями правил хранения, положений эксплуатационной документации, нарушением режимов эксплуатации при отклонении параметров: влажности, температурных режимов, напряжения электропитания и других причин (возникших не по вине Изготовителя), из-за которых в течение гарантийного срока изделие вышло из строя.

Изготовитель информирует потребителя и ФСТЭК России об окончании производства и (или) прекращении технической поддержки Изделия не позднее, чем за 1 (один) год до окончания производства и (или) прекращении технической поддержки.

Обращения, связанные с удовлетворением гарантийных обязательств, могут быть предъявлены в форме рекламаций в соответствии с формой, определенной в формуляре на изделие.













**ПРИЛОЖЕНИЕ А****(ОБЯЗАТЕЛЬНОЕ)****КОНТРОЛЬНЫЕ СУММЫ ФАЙЛОВ ДИСТРИБУТИВА  
ПО «МУЛЬТИФАКТОР»**

Перечни контрольных сумм файлов дистрибутива ПО «Мультифактор» представлены в таблицах А.1, А.2.

Т а б л и ц а А.1 – Контрольные суммы файлов дистрибутива ПО «Мультифактор»

Имя файла	Контрольная сумма
Дистрибутив ПО «Мультифактор»	
Портал.zip	d9c40b6e
Дистрибутив ПО «Мультифактор» (коннекторы)	
Коннекторы.zip	69ee17ee
Дистрибутив ПО «Мультифактор» (мобильное приложение)	
Мобильное приложение.zip	c0cc733b
Руководство администратора и пользователя	
Руководства.zip	fea24200
Электронное приложение к Формуляру РОФ.42584334.58.29.12.01 30 01-CD	
РОФ.42584334.58.29.12.01 30 01 ФО 01-CD.html	339114fd
Итого	33b4ee94

Т а б л и ц а А.2 – Контрольные суммы файлов дистрибутива платформы ПО «Мультифактор».

Имя файла	Контрольная сумма
Платформа ПО «Мультифактор»	
asp-front.tar	aa920df1
asp.tar	4230bf4c
api.tar	adcf5f30
eml.tar	b5b31dde
geo.tar	eda49bcf
idp.tar	79a8fd89

mgm.tar	e17d5792
mongod	1d63b0ea
pam.tar	48cc20b4
pus.tar	a2f57c6b
rds.tar	6acd2215
sip.tar	f26f64c7
sms.tar	ca6437d5
Итого	c2d847f4