ассистент

СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА

И УПРАВЛЕНИЯ «АССИСТЕНТ»

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Версия 3.0 от 01.03.2026 г.

Воронеж 2026

1 Перед установкой Системы удаленного мониторинга и управления «Ассистент» (далее — Системы «Ассистент») необходимо убедиться в том, что целевые рабочие станции и серверы удовлетворяют требованиям к аппаратному и программному обеспечению, приведенным в эксплуатационной документации.

2 Установка и первоначальная настройка Системы «Ассистент» должна производиться в соответствии с эксплуатационной документацией.

3 Эксплуатацию Системы «Ассистент» в информационных системах персональных данных, в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, а также на объектах критической информационной инфраструктуры Российской Федерации рекомендуется осуществлять при условии использования в качестве среды функционирования Системы «Ассистент» следующих операционных систем (далее - ОС) и системы управления базами данных (далее - СУБД):

3.1 ОС для серверной части Системы «Ассистент» (компоненты: ID-сервер, транспортный сервер, серверы самотестирования, аутентификации, оповещения, протоколирования, личного кабинета, инвентаризации, статистики, балансировки нагрузки):

– ОС специального назначения «Astra Linux Special Edition» (РУСБ.10015-01, сертификат соответствия ФСТЭК России № 2557 от 27.01.2012, действителен до 27.01.2026, окончание срока технической поддержки 31.12.2050);

– ОС Альт 8 СП (ЛКНВ.11100-01, сертификат соответствия ФСТЭК России № 3866 от 10.08.2018, действителен до 10.08.2028, окончание срока технической поддержки 10.08.2073);

– изделие «Операционная система РОСА «ХРОМ» (РСЮК.10301-01, сертификат соответствия ФСТЭК России № 4818 от 13.06.2024, действителен до 13.06.2029);

– операционная система «Platform V SberLinux OS Server» (децимальный номер RU.92573301.10006-02, сертификат соответствия ФСТЭК России № 4884 от 04.12.2024, действителен до 04.12.2029);

– операционная система «РЕД ОС» (децимальный номер RU.29926343.02.01-01, сертификат соответствия ФСТЭК России № 4060 от 12.01.2019, действителен до 12.01.2029).

3.2 ОС для клиентского приложения (сетевая станция пользователя):

– Операционная система специального назначения «Astra Linux Special Edition» (РУСБ.10015-01, сертификат соответствия ФСТЭК России № 2557 от 27.01.2012, действителен до 27.01.2026, окончание срока технической поддержки 31.12.2050);

– ОС Альт 8 СП (ЛКНВ.11100-01, сертификат соответствия ФСТЭК России № 3866 от 10.08.2018, действителен до 10.08.2028, окончание срока технической поддержки 10.08.2073);

– изделие «Операционная система РОСА «ХРОМ» (РСЮК.10301-01, сертификат соответствия ФСТЭК России № 4818 от 13.06.2024, действителен до 13.06.2029);

– операционная система «РЕД ОС» (децимальный номер RU.29926343.02.01-01, сертификат соответствия ФСТЭК России № 4060 от 12.01.2019, действителен до 12.01.2029, окончание срока технической поддержки 31.12.2030);

– операционная система «AlterOS» (96636777.58.29.11.001, сертификат соответствия ФСТЭК России № 4393 от 26.04.2021, действителен до 26.04.2026);

– операционная система общего назначения «Основа» (ДВНБ.10001-01, сертификат соответствия ФСТЭК России № 4381 от 31.03.2021, действителен до 31.03.2026).

3.3 СУБД для серверной части Системы «Ассистент» (компоненты: ID-сервер, транспортный сервер, серверы самотестирования, аутентификации, оповещения, протоколирования, личного кабинета, инвентаризации, статистики, балансировки нагрузки):

– Postgres Pro (децимальный номер 643.20663116.00001, сертификат соответствия ФСТЭК России № 3637 от 05.10.2016, действителен до 05.10.2029, бессрочная техническая поддержка);

– PostgreSQL, входящая в состав операционной системы специального назначения «Astra Linux Special Edition» (РУСБ.10015-01, сертификат соответствия ФСТЭК России № 2557 от 27.01.2012, действителен до 27.01.2026, окончание срока технической поддержки 31.12.2050).

3.4 При использовании в качестве среды функционирования операционной системы «Astra Linux Special Edition» (децимальный № РУСБ.10015-01) необходимо

выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в разделе 2 эксплуатационного документа РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1.»

3.5 При использовании в качестве среды функционирования операционной системы Альт 8 СП (децимальный № ЛКНВ.11100-01) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в эксплуатационных документах «Операционная система Альт 8 СП». Формуляр» ЛКНВ.11100-01 30 01, «Операционная система Альт 8 СП». Руководство по комплексу средств защиты» ЛКНВ.11100-01 99 01, «Операционная система Альт 8 СП». Руководство администратора» ЛКНВ.11100-01 90 01.

3.6 При использовании в качестве среды функционирования СУБД «Postgres Pro» (децимальный № 643.20663116.00001) необходимо выполнять настройку безопасной конфигурации в соответствии с порядком, определенным в разделе 7.1 эксплуатационного документа «Система управления базами данных «Postgres Pro». Описание комплекса средств защиты информации» 643.20663116.00001-01 32.

3.7 При использовании в качестве среды функционирования изделие «Операционная система РОСА «ХРОМ» (децимальный № РСЮК.10301-01) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в эксплуатационных документах «Операционная система РОСА «ХРОМ». Формуляр» РСЮК.10301-01 30 01, «Операционная система РОСА «ХРОМ». Руководство администратора» РСЮК.10301-01 32 01, «Операционная система РОСА «ХРОМ». Руководство пользователя» РСЮК.10301-01 34 02.

3.8 При использовании в качестве среды функционирования операционной системы «РЕД ОС» (децимальный № RU.29926343.02.01-01) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в пункте 1.6, разделах 5 и 6 эксплуатационного документа «Операционная система «РЕД ОС». Руководство администратора. RU.29926343.02.01-01 32 1-1».

3.9 При использовании в качестве среды функционирования Изделия операционной системы «AlterOS» (96636777.58.29.11.001) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в разделах 3, 4 эксплуатационного документа «Операционная система «AlterOS». Руководство администратора. 96636777.58.29.11.001– 01 91».

3.10 При использовании в качестве среды функционирования Изделия операционной системы общего назначения «Основа» (ДВНБ.10001-01) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком,

определенным в пунктах 11.3, 11.4 эксплуатационного документа «Операционная система общего назначения «ОСнова». Руководство администратора. ДВНБ.10001-01 94 01».

3.11 При использовании в качестве среды функционирования СУБД «PostgreSQL», входящую в состав операционной системы специального назначения «Astra Linux Special Edition» (децимальный № РУСБ.10015-01), необходимо выполнять настройку безопасной конфигурации в соответствии с порядком, определенным в разделе 1 эксплуатационного документа РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2.».

3.12 В случае отправки подсистемой протоколирования Системы «Ассистент» версии 4 и выше данных «Протокола удаленного взаимодействия», соответствующих стандарту syslog (Syslog Protocol), в стороннюю SIEM систему (Security information and event management) по протоколам TCP или UDP, потребителем должны быть реализованы меры по защите каналов связи между серверной частью изделия и SIEM системой.

3.13 Перечень операционных систем для серверной и клиентской частей изделия, для которых предприятие-разработчик гарантирует его работоспособность, указаны в подразделе «Сертификация» на странице https://мойассистент.рф/вопрос_ответ.

4 В случае отсутствия у потребителя нормативных и иных требований к использованию сертифицированных ОС и СУБД рекомендуется использовать операционные системы и системы управления базами данных (для которых производитель гарантирует работоспособность Системы «Ассистент»), указанные в подразделе «Сертификация» на странице https://мойассистент.рф/вопрос_ответ или эксплуатационной документации с наложенными средствами защиты информации в соответствии с приведенными далее требованиями.

5 Эксплуатация Системы «Ассистент» должна производиться персоналом, изучившим техническую документацию, а также документацию на рабочие станции, под управлением которых работает Система «Ассистент».

6 Эксплуатация Системы «Ассистент» в информационных системах персональных данных, в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, в автоматизированных системах управления производственными и технологическими процессами, в информационных системах объектов критической информационной инфраструктуры Российской Федерации должна осуществляться при условии принятия в указанных системах технических мер, определенных приказом ФСТЭК России от 18 февраля 2013 № 21, приказом ФСТЭК России от 11 апреля 2025 г. № 117, приказом

ФСТЭК России от 14 марта 2014 г. № 31, приказом ФСТЭК России от 25 декабря 2017 года № 239 соответственно, обеспечивающих:

- межсетевое экранирование информационной системы;
- защиту каналов связи, выходящих за границы контролируемой зоны;
- антивирусную защиту;
- обнаружение вторжений.

6.1 При использовании Системы «Ассистент» в составе информационных систем персональных данных класс защищенности указанных выше средств защиты должен соответствовать уровню защищенности персональных данных и задаваться в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

6.2 При использовании Системы «Ассистент» в составе государственных информационных систем, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений класс защищенности указанных выше средств защиты должен соответствовать классу защищенности информационной системы и задаваться в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11 апреля 2025 г. № 117.

6.3 При использовании Системы «Ассистент» в составе автоматизированных систем управления производственными и технологическими процессами класс защищенности указанных выше средств защиты должен соответствовать классу защищенности информационной системы и задаваться в соответствии с Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31.

6.4 При использовании Системы «Ассистент» в составе информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации класс защищенности указанных выше средств защиты должен соответствовать категории значимости объекта и задаваться в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 года № 239.

6.5 В случае эксплуатации Системы «Ассистент» в информационных системах персональных данных, в государственных информационных системах, в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, а также на объектах критической информационной инфраструктуры Российской Федерации в личном настройка «Прямое управление субъектами» (раздел «Системные настройки» - «Параметры») должна быть включена.

7 При использовании Системы «Ассистент» в редакциях «Корпорация+» или «Корпорация+ ФСТЭК» следует выполнять рекомендации по ограничению доступа при использовании программного средства nginx.

7.1 На уровне конфигурационного файла ID-сервера необходимо задать список доверенных IP-адресов, с которых будет разрешен доступ. Для этого в файле **/usr/share/assistant/ast-id/appsettings.json** необходимо указать параметр: `"AdminSafeList": "192.168.71.62;192.168.71.63" // Разрешенные ip-адреса`

Значение параметра может содержать один или несколько IP-адресов, разделенных «;» (точкой с запятой). Если параметр `AdminSafeList` отсутствует, то доступ к ID-серверу будет разрешен со всех IP-адресов.

7.2 Ограничение доступа к id-серверу

В файл конфигурации `ast-id.conf` необходимо добавить следующие блоки:

```
# Разрешить доступ к маршруту /api/exec из любых источников
location ^~ /api/exec {
allow all;
}
# Запросы разрешены только с указанных IP
location / {
allow 127.0.0.1;
allow 10.0.0.0/8;
deny all;
}
```

7.3 Ограничение доступа к log-серверу

В файл конфигурации `ast-log.conf` необходимо добавить следующие блоки:

```
# Разрешенные эндпоинты для приема логов
location ^~ /api/log/post {
allow all;
}
location ^~ /api2/log/post {
allow all;
}
location ^~ /api/session/post {
allow all;
}
# Запросы разрешены только с указанных IP
location ^~ /api/ {
allow 127.0.0.1;
```

```
allow 10.0.0.0/8;
deny all;
}
```

7.4 Ограничение доступа к серверу аутентификации

В файл конфигурации `ast-auth.conf` необходимо добавить следующие блоки:

```
# Запросы разрешены только с указанных IP
location / {
allow 127.0.0.1;
allow 10.0.0.0/8;
deny all;
}
```

7.5 Ограничение доступа к серверу оповещений

В файл конфигурации `ast-notify.conf` необходимо добавить следующие блоки:

```
# Запросы разрешены только с указанных IP
location / {
allow 127.0.0.1;
allow 10.0.0.0/8;
deny all;
}
```

7.6 Ограничение доступа к серверу id-статистики

В файл конфигурации `ast-idstat.conf` необходимо добавить следующие блоки:

```
# Запросы разрешены только с указанных IP
location / {
allow 127.0.0.1;
allow 10.0.0.0/8;
deny all;
}
```

7.7 Ограничение доступа к модулю регистрации статистики

В файл конфигурации `ast-webapi.conf` необходимо добавить следующие блоки:

```
# Запросы разрешены только с указанных IP
location / {
allow 127.0.0.1;
allow 10.0.0.0/8;
deny all;
}
```

8 Потребителям Системы «Ассистент» рекомендуется разработать организационно-распорядительную документацию, определяющую:

1) порядок допуска пользователей к ресурсам Системы «Ассистент» и назначения их полномочий;

2) обеспечение физической сохранности ПЭВМ с установленными компонентами Системы «Ассистент» и исключение возможности доступа к ней/ним лиц, не имеющим доступа к ресурсам Системы «Ассистент»;

3) запрет установки в информационной системе любых программных средств, не предусмотренных политикой безопасности предприятия, а также любых средств разработки и отладки программ;

4) назначение администратора безопасности Системы «Ассистент», отвечающего за правильную эксплуатацию Системы «Ассистент»;

5) ограничение доступа к автоматизированному рабочему месту администратора безопасности Системы «Ассистент» организационными и техническими мерами (в т.ч. средствами идентификации и аутентификации);

6) сохранение в секрете идентификаторов (имен) и паролей (кодов) администратора безопасности Системы «Ассистент»;

7) периодическую смену паролей (кодов) администратора безопасности Системы «Ассистент»;

8) предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (в т.ч. администраторов информационной системы);

9) размещение автоматизированного рабочего места администратора безопасности Системы «Ассистент» в пределах контролируемой зоны и оснащение данного рабочего места сертифицированными по требованиям безопасности информации средствами антивирусной защиты с последними обновлениями баз данных признаков компьютерных вирусов;

10) регулярное выполнение администратором безопасности контроля состава установленного в информационной системе программного обеспечения на предмет его соответствия политике безопасности предприятия;

11) регулярное выполнение администратором безопасности Системы «Ассистент» контроля целостности программной и информационной частей Системы «Ассистент»;

12) проведение ежедневной проверки программной среды, использующейся в качестве административной консоли Системы «Ассистент», на наличие вредоносного программного обеспечения;

13) своевременную установку в среде функционирования Системы «Ассистент» имеющихся обновлений и патчей общесистемного программного обеспечения, обеспечивающих устранение известных уязвимостей;

14) порядок получения администратором безопасности информации о выходе обновлений Системы «Ассистент» через службу технической поддержки производителя и внесения соответствующих отметок в разделы формуляра.

9 В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения информационной системы, работа Системы

«Ассистент» должна быть прекращена. По данному факту должно быть

проведено служебное расследование комиссией и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

10 В случае обнаружения недостатка и/или дефекта Системы «Ассистент», в том числе при выявлении уязвимостей и недекларированных возможностей программного обеспечения Системы «Ассистент», потребитель должен в течение одних суток известить производителя, используя официальный сайт Системы «Ассистент» (https://мойассистент.рф) или электронную почту office@safib.ru, и в последствии предоставить производителю информацию, запрошенную для расследования инцидента информационной безопасности и устранения соответствующего недостатка или дефекта Системы «Ассистент».

11 Получение обновлений несертифицированной версии Системы «Ассистент» производится пользователем с использованием личного кабинета официального сайта Системы «Ассистент» (https://лк.мойассистент.рф) в следующем порядке:

11.1 Войти в личный кабинет пользователя, на электронную почту которого оформлена (выдана) лицензия. Выбрать и открыть необходимую лицензию.

11.2 Выбрать версию Системы «Ассистент» и на вкладке «Обновление сервера» скачать дистрибутив для необходимой ОС (обновление сервера включает в себя обновление клиентского приложения).

11.3 По окончании скачивания провести расчет контрольных сумм файлов дистрибутива Системы «Ассистент».

11.4 Сверить полученную контрольную сумму дистрибутива Системы «Ассистент» с эталонным значением, указанным в личном кабинете пользователя.

11.5 При расхождении рассчитанных контрольных сумм с эталонными значениями обратиться в службу технической поддержки производителя.

12 Получение обновлений сертифицированной версии Системы «Ассистент» осуществляться пользователем в следующем порядке:

12.1 Получение обновлений по доверенному каналу связи, определенному в договоре или документации Системы «Ассистент» (Почта России, курьерская служба и т.д.).

12.2 При получении обновлений перед их установкой (инсталляцией) необходимо проверить целостность соответствующих файлов. С этой целью:

– провести расчет контрольных сумм файлов обновлений ВСЗ ПК «Ассистент» с использованием программы «ФИКС» по алгоритму «Уровень-1»;

– сравнить контрольные суммы файлов обновлений с указанными в приложении А к формуляру (высылается в электронном виде вместе с файлами обновлений);

– при расхождении контрольных сумм с эталонными значениями обратиться в службу технической поддержки предприятия-производителя.

13 Установка обновлений допускается при полном совпадении контрольных сумм с эталонными значениями.