СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА

И УПРАВЛЕНИЯ «АССИСТЕНТ»

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Версия 2.0 от 04.08.2023 г.

Воронеж 2023

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, 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 осуществляться 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 Microsoft Windows Server 2012 R2 (десятичный номер 501110-002-82487552-2014 st, сертификат соответствия ФСТЭК России № 3366 от 17.03.2015, действителен до 17.03.2021, окончание срока технической поддержки 10.10.2023);

– 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 10.08.2023, окончание срока технической поддержки 10.08.2073);

– изделие «Операционная система РОСА «КОБАЛЬТ» (РСЮК.10201-01, сертификат соответствия ФСТЭК России № 4039 от 07.12.2018, действителен до 07.12.2023);

– ОС типового дистрибутива АИС ФССП России (RU.00083316.02.01-01, сертификат соответствия ФСТЭК России № 4072 от 14.03.2019, действителен до 14.03.2024);

– операционная система «РЕД ОС» (десятичный номер RU.29926343.02.01-01, сертификат соответствия ФСТЭК России № 4060 от 12.01.2019, действителен до 12.01.2024).

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);

– Альт Линукс СПТ 7.0 (КШДС.10514-01, сертификат соответствия ФСТЭК России № 3713 от 22.03.2017, действителен до 22.03.2020, окончание срока технической поддержки 26.06.2023);

– ОС Альт 8 СП (ЛКНВ.11100-01, сертификат соответствия ФСТЭК России № 3866 от 10.08.2018, действителен до 10.08.2023, окончание срока технической поддержки 10.08.2073).

– изделие «Операционная система РОСА «КОБАЛЬТ» (РСЮК.10201-01, сертификат соответствия ФСТЭК России № 4039 от 07.12.2018, действителен до 07.12.2023);

– ОС типового дистрибутива АИС ФССП России (RU.00083316.02.01-01, сертификат соответствия ФСТЭК России № 4072 от 14.03.2019, действителен до 14.03.2024);

– операционная система «РЕД ОС» (децимальный номер RU.29926343.02.01-01, сертификат соответствия ФСТЭК России № 4060 от 12.01.2019, действителен до 12.01.2024).

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 05.10.2024, окончание срока технической поддержки 05.10.2029);

– 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 Microsoft Windows Server Standard 2012 R2 (децимальный номер 501110-002-82487552-2014 St) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в разделах 4 и 5 эксплуатационного документа 501110-002-82487552-2014 РБ «Операционные системы «Microsoft Windows Server Standard 2012 R2», «Microsoft Windows Server Datacenter 2012 R2», «Microsoft Windows Storage Server 2012 R2 Standard», «Microsoft Windows Storage Server 2012 R2 Workgroup», «Microsoft Windows Server Essentials 2012 R2», «Microsoft Windows Server Foundation 2012 R2». Руководство по настройке функций безопасности сертифицированной версии». До восстановления технической поддержки своей продукции на территории Российской Федерации корпорацией Intel(R) рекомендуется деинсталлировать из системы драйвер Intel(R) High Definition Audio.

3.5 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.»

3.6 При использовании в качестве среды функционирования операционной системы Альт Линукс СПТ 7.0 (децимальный № КШДС.10514-01) 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 Линукс СПТ 7.0». Формуляр» КШДС.10514-01 30 01, «Операционная система «Альт Линукс СПТ 7.0». Руководство по КСЗ. Часть 2» КШДС.10514-01 97 01-2, «Операционная система «Альт Линукс СПТ 7.0». Руководство администратора» КШДС.10514-01 98 01.

3.7 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.

3.8 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.

3.9 При использовании в качестве среды функционирования изделие «Операционная система РОСА «КОБАЛЬТ» (децимальный № РСЮК.10201-01) 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 «КОБАЛЬТ». Формуляр» РСЮК.10201-01 30 01, «Операционная система РОСА «КОБАЛЬТ». Руководство администратора» РСЮК.10201-01 92 01, «Операционная система РОСА «КОБАЛЬТ». Руководство пользователя по эксплуатации» РСЮК.10201-01 92 02.

3.10 При использовании в качестве среды функционирования операционной системы типового дистрибутива АИС ФССП России (децимальный № RU.00083316.02.01-01) необходимо выполнять настройку безопасной конфигурации операционной системы, своевременную установку системных пакетов обновления и контроль соответствия сертифицированной версии в соответствии с порядком, определенным в эксплуатационных документах «Автоматизированная информационная система Федеральной службы судебных приставов АИС ФССП

России. Операционная система типового дистрибутива АИС ФССП России. Формуляр» RU.00083316.02.01-01 30.

3.11 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».

3.12 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.».

3.13 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.

3.14 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, 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 февраля 2013 г. № 17, 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 класс защищенности указанных выше средств защиты должен соответствовать классу защищенности информационной системы и задаваться в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

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 кабинете настройка «Расширенные настройки политики» (раздел «Системные настройки» - «Политика доступа по умолчанию») должна быть отключена, а настройка «Прямое управление субъектами» (раздел «Системные настройки» - «Безопасность») должна быть включена.

7 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.

8 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.

9 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».

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

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

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

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

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

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

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

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

11.2 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, программно»;

– 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.

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