15. Указания по эксплуатации

15.1 Установка изделия на автоматизированные рабочие места должна проводиться с дистрибутива изделия, расположенного на компакт-диске в составе верифицированного инсталляционного комплекта, или загруженного с Центра сертифицированных обновлений Производителя (https://update.prp.su), или их копий, изготовленных в соответствии с п.15.5. Реквизиты для доступа к Центру сертифицированных обновлений указаны в п.7.2 Формуляра.

15.2 Настройка, использование и контроль средств защиты информации изделия должны проводиться ответственными за эксплуатацию изделия (администраторами) в соответствии с утвержденной политикой безопасности организации, организационно-методическими документами принятой системы защиты информации, руководством администратора и настоящим формуляром.

Для затруднения и исключения использования сканеров с целью сбора информации и поиска уязвимостей администратору рекомендуется настроить службу «Межсетевой экран». Запрещено отключать службу «Межсетевой экран».

Длинна пароля должна быть не менее 8 символов (буквенно-цифровой последовательности длинной ≥ 8 символов с добавлением специальных символов (#, $, * и т.д.)) с назначением уникального идентификатора администратора.

Администратору рекомендуется производить смену пароля не реже одного раза в месяц.

В процессе эксплуатации изделия необходимо исключить доступ пользователей операционной системы к приложениям, выполняющимся с более высокими правами доступа, чем права, предоставленные им согласно дискреционной матрице доступа. Администратор после окончания работы с приложениями, запущенными им с правами суперпользователя, должен завершить их работу.

Администратору необходимо произвести настройку Изделия в соответствии с рекомендациями раздела 5 «Дополнительные настройки безопасности» документа «Руководство администратора ЦАУВ.14001-01 91 01 Дополнение № 1» и исключить использование потенциально уязвимых служб SNMP, LDAP, memcached в соответствии с рекомендациями раздела 2 «Настройка и ограничение программной среды» дополнения № 1 к руководству администратора.

Для удаленного входа в систему рекомендуется использовать протокол SSH.

В среде функционирования изделия должны быть реализованы мероприятия, направленные на достижение целей безопасности для среды, идентифицированных в задании по безопасности на изделие.

Изделие, как сертифицированное средство, может применяться только в оцененной конфигурации.

Администратору рекомендуется периодически проверять Центр сертифицированных обновлений (https://update.prp.su) на наличие сведений об уязвимостях и обновлении ПО (закрывающем уязвимости) изделия.

Для сертифицированной версии изделия должны быть установлены все актуальные обязательные сертифицированные обновления безопасности.

15.3 Сертифицированные обновления изделия должны устанавливаться с Центра сертифицированных обновлений, или с верифицированных инсталляционных комплектов наборов обновлений на материальных носителях, или с их копий, изготовленных в соответствии с п.15.5.

15.4 Перед установкой дистрибутива изделия и наборов сертифицированных обновлений, загруженных с Центра сертифицированных обновлений Производителя, необходимо провести их верификацию одним из следующих способов:

15.4.1 Проверить контрольные суммы дистрибутива и наборов обновлений изделия с помощью сертифицированных средств контроля эффективности (целостности) средств защиты информации, реализующих алгоритм «Уровень-3» (например, с помощью программ ФИКС 2.0.1, ФИКС 2.0.2, ФИКС Unix 1.0). Рассчитанная КС дистрибутива должна совпадать с КС, приведенной в Таблице 1 Формуляра (алгоритм «Уровень-3»).

15.4.2 Проверить усиленную квалифицированную электронную подпись (ЭП), которой подписаны дистрибутив изделия или набор сертифицированных обновлений. ЭП должна принадлежать Производителю изделия, в дистрибутиве и наборах сертифицированных обновлений должны отсутствовать изменения, ЭП не должна быть отозванной на момент подписания. Инструкции по проверке ЭП располагаются на сайте Производителя в разделе Поддержка / Документация / Контроль соответствия СЗИ.

15.5 При изготовлении ответственными за эксплуатацию изделия (администраторами) копий дистрибутива изделия и наборов сертифицированных обновлений из верифицированных инсталляционных комплектов и загруженных с Центра сертифицированных обновлений версий, они должны быть верифицированы согласно п.15.4.

Изготовленные копии дистрибутива, наборов сертифицированных обновлений изделия и документации на него должны быть учтены установленным в организации-пользователе порядком, а сведения о них (учетные/инвентарные номера) указаны в разделах 9, 10, 11, 14 и Таблице 1 настоящего Формуляра.

15.6 Руководство по загрузке дистрибутива изделия, его сертифицированных обновлений и эксплуатационной документации с Центра сертифицированных обновлений и их верификации расположено на сайте Производителя в разделе Поддержка.

15.7 Актуальные значения контрольных сумм исполняемых файлов, подлежащих периодическому контролю после установки сертифицированных обновлений, а также контрольные суммы наборов сертифицированных обновлений и дистрибутивов изделия с включенными наборами обновлений, указываются в документации соответствующих наборов сертифицированных обновлений и формуляре на изделие. Указанная документация доступна на сайте Производителя в разделе Поддержка / Документация / Контроль соответствия СЗИ, а также входит в комплект поставки верифицированных инсталляционных комплектов наборов обновлений на материальных носителях.