Средство защиты информации Secret Net LSP
Комментарии к версии 1.9

Данный документ содержит описание новых возможностей СЗИ Secret Net LSP версии 1.9 по сравнению с версией 1.7, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации СЗИ Secret Net LSP.

Оглавление

1. Комплект поставки

1.1. Размещение файлов на установочном диске

Каталог	Содержимое
\Setup\	дистрибутивы
\Documentation\	комплект документации
\Tools\	вспомогательные утилиты, программы для установки и настройки ПО

2. Изменения и новые возможности

2.1. Версия 1.9

Данный раздел содержит описание новых возможностей СЗИ Secret Net LSP версии 1.9 по сравнению с версией 1.7.

1. Добавлена возможность работы Secret Net LSP в среде следующих ОС:

- Альт 8 СП;
- Альт Рабочая станция 8;
- РЕД ОС 7.1/7.2 Муром;
- Astra Linux Common Edition 2.12/2.12.14 Update 19;
- Astra Linux Special Edition 1.5 Update 20190329SE15;
- Astra Linux Special Edition 1.6/1.6 Update 20190222SE16;
- CentOS 7.6.1810;
- Debian 9.5/9.9;
- Oracle Linux 7.6;
- Red Hat Enterprise Linux Server 7.6;
- ROSA Enterprise Linux Desktop;
- Ubuntu 18.04.2 LTS.

2. Secret Net LSP больше не поддерживает работу в среде следующих ОС:

- МСВС 5.0;
- Astra Linux Special Edition 1.4;
- CentOS 7.2.1511/7.1/6.5;
- Debian 8.0/7.6;
- Oracle Linux 7.3/7.2;
- Red Hat Enterprise Linux 7.3/7.2/7.0/6.9/6.5.

3. Реализована интеграция с ПАК "Соболь" версий 3.x и версии 4.

4. Реализована поддержка идентификаторов JaCarta PKI/ГОСТ, JaCarta 2-ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ и смарт-карт JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ.

5. Реализован механизм замкнутой программной среды.

6. В состав дистрибутивов Secret Net LSP включены все обновления, выпускавшиеся для Secret Net LSP версий 1.6 и 1.7.

3. Особенности работы и ограничения

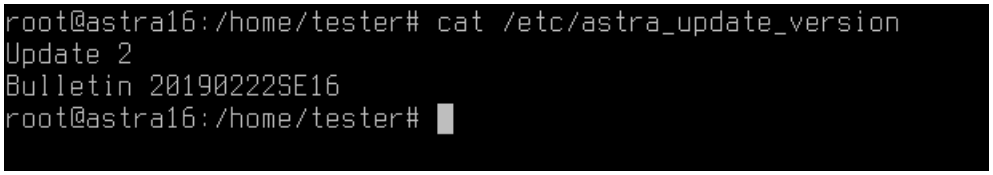
7. При установке Secret Net LSP в среде ОС Astra Linux для обеспечения надежного функционирования Secret Net LSP необходимо учитывать установленные в системе обновления безопасности. Посмотреть текущую версию обновления безопасности ОС Astra Linux 1.5 и 1.6 можно командой:

cat /etc/astra-update-version

Будет показано содержимое файла, создаваемого при установке обновления.

Для ОС Astra Linux Special Edition 1.5 должен быть установлен БЮЛЛЕТЕНЬ № 20190329SE15:

Для ОС Astra Linux Special Edition 1.6 должен быть установлен БЮЛЛЕТЕНЬ № 20190222SE16:



8. При установке Secret Net LSP в среде ОС Astra Linux Special Edition 1.6 выполняющий установку пользователь должен обладать правами высокого уровня для механизма контроля целостности. Учетной записи root такие права по умолчанию не предоставляются. Рекомендуется выполнять установку под встроенной учетной записью администратора безопасности, для которой при входе выбран "Высокий уровень" прав для механизма контроля целостности.

9. В ОС Debian 9.9 и Astra Linux Common Edition 2.12.14 Update 19 в состав системы входят пакеты opensc-pkcs11_0.16.0-3+deb9u1 и opensc_0.16.0-3+deb9u1, использование которых приводят к невозможности чтения пароля из идентификаторов Rutoken ЭЦП и Rutoken S. Для корректной работы с этими идентификаторами следует выполнить откат к версии данных пакетов без "deb9u1": opensc-pkcs11_0.16.0-3 и opensc_0.16.0-3.

10. При использовании Secret Net LSP в среде ОС РЕД ОС 7.2 Муром недоступна возможность блокировки при извлечении идентификатора, т.к. она не поддерживается скринсейвером.

11. Если при работе в среде ОС ROSA Enterprise Linux Desktop не выполнен вход пользователя в систему, на сервере безопасности Secret Net Studio будет отображаться пользовательская сессия для системной записи (unknow).

12. В ОС Astra Linux Common Edition 2.12 и Astra Linux Special Edition 1.5/1.6 проявляются следующие особенности при работе с идентификаторами:

- идентификация пользователя осуществляется только при вводе имени пользователя;
- недоступна возможность блокировки при извлечении идентификатора.

13. В ОС Astra Linux Special Edition 1.5 добавление доменного пользователя в локальную группу осуществляется с помощью утилиты командной строки groupmems. В ОС при блокировке экрана доменным пользователем вход в систему под этим же пользователем запрещен.

14. В ОС CentOS 7.6.1810 необходимо ввести любой символ и нажать клавишу <Enter> при считывание системой данных из идентификатора, подключенного к считывателю на момент входа пользователя, при включенных политиках (логин определен идентификатором и установлен смешанный режим идентификации). Считывание учетной записи с идентификатора не происходит, если не установлена учетная запись.

15. В ОС Astra Linux Special Edition 1.6 отсутствует сервер печати CUPS от Secret Net LSP.

16. Secret Net LSP удаляется с ОС Альт 8 СП только при отключении системы принудительного контроля доступа selinux.

17. Если после удаления Secret Net LSP компьютер остался заблокированным, для его разблокировки войдите в систему под учетной записью с правами root и выполните следующие действия:

- удалите файл /etc/bashrc.d/00Lock.sh;
- удалите файл /etc/profile.d/00Lock.sh;
- удалите содержимое файла /etc/nologin и перезагрузите компьютер.

18. В ОС Debian 9.5 и Лотос для корректной работы с идентификаторами после установки Secret Net LSP необходимо установить пакеты opensc_0.16.0-3_amd64.deb и opensc-pkcs11_0.16.0-3_amd64.deb, расположенные на соответствующих дистрибутивах.

19. При работе с идентификатором Jacarta ГОСТ необходимо установить персональный идентификационный номер с помощью ПО Аладдин jcadmin.

20. После удаления Secret Net LSP на ОС CentOS 7.6.1810, Red Hat Enterprise Linux Server 7.6 и Oracle Linux 7.6 будут выполнены процедура переопределения меток SELinux и двойная перезагрузка системы.

21. После включения жесткого режима работы ЗПС на ОС Astra Secret Net LSP блокирует процессы, запущенные учетной записью root.

22. В ОС CentOS 7.3.1611 для корректной работы sncupsd необходимо обновить пакеты cups-libs и dbus-libs на пакеты от ОС CentOS 7.6.1810 до версий:

- cups-libs-1.6.3-35.el7.x86_64;
- dbus-libs-1.10.24-12.el7.x86_64.

23. Для входа в графический интерфейс пользователя под учетной записью root в ОС Debian 9.5 требуется удалить user != root из конфигурационного файла /etc/pam.d/xdm, для этого необходимо отключить immutable флаг: chattr –i /etc/pam.d/xdm, удалить user != root и установить immutable флаг: chattr +i /etc/pam.d/xdm.

24. Для доменного пользователя запрещается чтение закрытого ключа с идентификатора.

25. Выключение подсистемы затирания информации в ОС Astra Linux Special Edition 1.6 и Astra Linux Common Edition 2.12 происходит после перезагрузки компьютера.

26. При настройке параметров аутентификации в ОС Astra Linux Common Edition 2.12 и Astra Linux Special Edition 1.5/1.6 в списке параметров отсутствует режим для метода аутентификации: "Приватный ключ считан с идентификатора, а пароль с клавиатуры".

4. Сведения о совместимости с другим ПО

Данный раздел содержит сведения о совместимости СЗИ Secret Net LSP версии 1.9 с некоторыми другими программными средствами при совместном функционировании.

27. Реализована совместимость Secret Net LSP со следующими продуктами компании ООО "Код Безопасности":

- Secret Net 7.7;
- Secret Net Studio 8.4, 8.5;
- ПАК «Соболь» 3.0.9/3.0.6/3.1/3.2/4.2;
- СКЗИ «Континент-АП» версия 3.7.5;

28. Реализована совместимость Secret Net LSP со следующим ПО:

- Мой Офис на ContinentOS;
- Kaspersky Endpoint Security 10;
- Dr.Web Desktop Security Suite версии 11;
- Антивирус Касперского 8.0 для Linux File Servers;
- Kaspersky Security 8.0 для Linux Mail Server.

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	(495) 982-30-20
E-mail:	info@securitycode.ru
Web:	https://www.securitycode.ru