Средство защиты информации Secret Net LSP
Комментарии к версии 1.10

Документ содержит описание новых возможностей СЗИ Secret Net LSP версии 1.10, 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 1.10

1. Разработан персональный межсетевой экран (МЭ).

2. Добавлен функционал построения правил замкнутой программной среды (ЗПС) на основании анализа журнала аудита.

3. Реализована возможность задания максимального периода неактивности пользователя до блокировки экрана.

4. Реализована блокировка учетной записи на временной интервал при превышении количества попыток ввода пароля.

5. Появилась возможность оповещения пользователя о последнем успешном входе в систему.

6. Реализована поддержка управления групповыми политиками с сервера безопасности (СБ) СЗИ Secret Net Studio (SNS).

7. Добавлена возможность работы Secret Net LSP в среде следующих операционных систем (ОС):

- Альт 8 СП (версия ядра 4.19.109-un-def-alt0.M80C.1, DE: MATE);
- Альт Рабочая станция 9.0 (версия ядра 4.19.79-std-def-alt1, DE: MATE);
- Лотос (версия ядра 4.19.50, DE: MATE);
- РЕД ОС 7.2 Муром (версия ядра 4.19.79-1.el7.x86_64, DE: MATE);
- Astra Linux Common Edition 2.12.21 (версия ядра 4.15.3-1-generic #astra21, 4.15.3-1-hardened #astra21, DE: Fly);
- Astra Linux Common Edition 2.12.22 (версия ядра 4.15.3-1-generic #astra21, 4.15.3-1-hardened #astra21, DE: Fly);
- Astra Linux Common Edition 2.12.29 (версия ядра 5.2.13 generic, DE: Fly);
- Astra Linux Common Edition 2.12.29 (версия ядра 4.15.3-2-generic #astra25, 4.15.3-2-hardened #astra25, DE: Fly);
- Astra Linux Special Edition 1.5 (версия ядра 4.2.0-24-generic #1astra4+c1, DE: Fly);
- Astra Linux Special Edition 1.6 (версии ядра 4.15.3-1-generic #astra21, 4.15.3-1-hardened #astra21, с установленным пакетом обновлений № 20191029SE16, DE: Fly);
- CentOS 7.7 (версия ядра 3.10.0-1062.9.1.el7.x86_64, DE: GNOME);
- CentOS 8.0 (версия ядра 4.18.0-80.el8.x86_64, DE: GNOME);
- Debian 10.1 (версия ядра 4.19.0-6, DE: GNOME);
- Red Hat Enterprise Linux 7.7 (версия ядра 3.10.0-1062.9.1.el7.x86_64, DE: GNOME);
- Red Hat Enterprise Linux 8.0 (версия ядра 4.18.0-80.el8.x86_64, DE: GNOME);
- Ubuntu 18.04.2 LTS (версия ядра 4.18.0-15-generic #16~18.04.1-Ubuntu, DE: GNOME);
- Ubuntu 18.04.3 LTS (версия ядра 4.15.0-55-generic #60~16.04.2-Uubntu, DE: GNOME).

8. Выпущен пакет исправлений sncupsd_astra2.12-upd31_fix.run для для операционных систем Astra Linux Common Edition 2.12.29 (версия ядра 4.15.3-2-generic #astra25, 4.15.3-2-hardened #astra25, DE: Fly), Astra Linux Common Edition 2.12.29 (версия ядра 5.2.13 generic, DE: Fly).

9. Работа Secret Net LSP больше не поддерживается в следующих средах:

- Альт Рабочая станция 8 (версия 8.2, версия ядра 4.9.71-std-def-alt0.M80P.1, DE: MATE);
- РЕД ОС 7.1 Муром (версия ядра 4.9.79-1.el7.x86_64, DE: MATE);

- CentOS 7.3.1611 (версия ядра 4.4.80-1.el7.elrepo.x86_64, DE: GNOME);
- CentOS 7.6.1810 (версия ядра 3.10.0-957.el7.x86_64, DE: GNOME);
- Debian 9.5 (версия ядра 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1, DE: GNOME);
- Debian 9.9 (версия ядра 4.9.0-9-amd64 #1 SMP 4.9.168-1+deb9u2~deb8u1, DE: GNOME);
- Oracle Linux 7.6 (версия ядра 3.10.0-957.el7.x86_64, DE: GNOME);
- Red Hat Enterprise Linux Server 6.8 (версия ядра 2.6.32 642.13.1. el6.x86_64);
- Red Hat Enterprise Linux Server 7.6 (версия ядра 3.10.0-957.el7. x86_64, DE: GNOME);

3. Особенности работы и ограничения

1. Особенности работы в ОС Debian. Для подключения к СБ СЗИ SNS необходимо установить пакеты libssl1.1_1.1.1c-1ubuntu4_amd64.deb и openssl_1.1.1c-1ubuntu4_amd64.deb. Пакеты находятся в локальном репозитории. Для остальных ОС пакет openssl рекомендуется устанавливать из локального репозитория SN LSP, во избежание проблем взаимодействия с СБ SNS.

2. ОС Debian, Ubuntu. При использование механизмов ЗПСи МЭ рекомендуется отключить Wayland. При включенном Wayland также могут наблюдаться проблемы при отображении статуса лицензии при входе в систему. Для отключения необходимо в конфигурационном файле /etc/gdm3/daemon.conf задать параметр WaylandEnable=false.

3. ОС Ubuntu. При установке Secret Net LSP в среде ОС Ubuntu необходимо предварительно установить пакет libboost-filesystem во избежание дальнейшей блокировки системы или ее некорректного функционирования.

При обновлении СЗИ SN LSP с версии 1.9 до версии 1.10 в deb-дистрибутиве не сохраняются настройки ЗПС. Их нужно переместить с помощью утилиты snbckctl. Причем необходимо воосстановить отдельную резервную копию (бэкап) для ЗПС, иначе пропадают политики Users.

4. ОС Astra Linux SE 1.6. Для запуска SNManager пользователю в политике безопасности необходимо установить высокий уровень целостности (Панель управления ->Панель безопасности ->Пользователи -> Выбрать пользователя ->МРД).

Пользователь, выполняющий установку Secret Net LSP, 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.

5. ОС Astra Linux SE 1.6. В случае использования замкнутой программной среды ОС Astra Linux при установленном Secret Net LSP необходимо скорректировать конфигурационный файл /opt/secretnet/etc/snfc.conf для каталога/boot.

В зависимости от желаемого результата для строки /boot/NORMALBACKLOCK:

- не требуется реакция на изменения – убрать строку;
- требуется отслеживать события изменения – изменить значение на NORMAL;
- требуется отслеживать события изменения и заблокировать станцию – изменить значение на NORMALLOCK;
- после изменения значения – выполнить переинициализацию БД из-под учетной записи root: # /opt/secretnet/sbin/snfc -i

6. ОС Astra Linux SE 1.5. СЗИ Secret Net LSP не поддерживает режим ЗПС программной среды ОС Astra Linux.

7. ОС Astra Linux SE 1.5. В Secret Net LSP межсетевое экранирование трафика не поддерживается.

8. ОС Astra Linux CE 2.12, SE 1.5/1.6. В Secret Net LSP проявляются следующие особенности при работе с идентификаторами:

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

9. ОС Astra Linux SE 1.6. В Secret Net LSP не работает подсистема контроля печати.

10. ОС Astra Linux CE 2.12, SE 1.6. Выключение подсистемы затирания информации происходит после перезагрузки компьютера.

11. ОС Astra Linux CE 2.12, SE 1.5/1.6. При настройке параметров аутентификации в списке параметров отсутствует режим для метода аутентификации – "Приватный ключ считан с идентификатора, а пароль с клавиатуры".

12. ОС Astra Linux CE 2.12, SE 1.5/1.6. После включения жесткого режима работы ЗПС Secret Net LSP блокирует процессы, запущенные учетной записью root.

13. ОС Astra Linux CE 2.12. На компьютерах под управлением ОС Astra Linux Common Edition 2.12.21 в версии ядра hardened функционирование модуля межсетевого экранирования SN LSP не поддерживается.

14. ОС Альт Рабочая станция 9. Из-за конфликта с пакетом OpenCT не работает идентификатор Rutoken S.

Существуют два способа решения проблемы.

1 способ. Удаление пакета OpenCT.

$ sudo rpm –e openct

Внимание! Также в системе не должен быть установлен пакет pcsc-lite-openct. Если пакет установлен, то его необходимо удалить.

2 способ. Удаление записей об идентификаторе в конфигурационном файле openct.conf.

С помощью текстового редактора в файле /etc/openct.conf необходимо изменить строки, относящиеся к Rutoken S, добавив символ # в начало строки. Например:

```
#       usb:0a89/0020,   # Aktiv Rutoken S
#       usb:0a89/0012,   # Aktiv uaToken S
```

15. ОС Альт 8 СП. Вход в систему после предъявления идентификатора выполняется автоматически без запроса пароля, а для разблокирования экрана потребуется ввести пароль с клавиатуры.

16. ОС Альт 8 СП. Удаление Secret Net LSP возможно только при отключении системы принудительного контроля доступа SELinux.

17. ОС Лотос . В текущей версии Secret Net LSP счетчик попыток аутентификации пользователя увеличивается как при выборе пользователя из списка на экране входа в систему, так и при выходе из графической сессии.

18. ОС РЕД ОС 7.2 Муром. В Secret Net LSP недоступна возможность блокировки при извлечении идентификатора, т. к. она не поддерживается скринсейвером.

19. ОС ROSA Enterprise Linux Desktop. Если не выполнен вход пользователя в систему, на СБ СЗИ SNS будет отображаться пользовательская сессия для системной записи (unknown).

20. При развертывании Secret Net LSP при установке зависимостей Postfix рекомендуется устанавливать значения по умолчанию.

21. В режиме усиленной аутентификации доменных пользователей имя (логин) при входе в систему должно содержать только латинские символы. Если в имени присутствуют символы кириллицы, параметру «Усиленная аутентификация» следует установить значение "Выключено".

22. В текущей версии персонального межсетевого экрана Secret Net LSP при применении параметра reject уведомление об отклонении сетевого пакета взаимодействующему клиенту не отправляется.

23. Для получения информации о доменном пользователе Secret Net LSP используется атрибут пользователя userPrincipalName из Active Directory. Для корректной работы с доменными пользователя у них должен присутствовать данный атрибут.

24. Начиная с Secret Net LSP 1.9 для считывания данных о пользователе с идентификатора при включенных политиках (логин определен идентификатором или установлен смешанный режим идентификации) необходимо:

- для CLI – ввести имя пользователя или любой символ, нажать "Ввод", после чего будет опрошен идентификатор;
- для GUI – выбрать пользователя из списка или ввести его имя в зависимости от гритера системы.

25. 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.

26. При работе с идентификатором Jacarta ГОСТ необходимо предварительно выполнить его инициализацию и установить персональный идентификационный номер с помощью ПО Аладдин jcadmin.

27. Для доменного пользователя игнорируется чтение закрытого ключа с идентификатора.

28. Если в домене используется большое количество учетных записей/групп, то рекомендуется отключить перечисление для пользователей/групп в системных сервисах, отвечающих за взаимодействие с доменом (sssd/smaba).

Для sssd –в конфигурационном файле /etc/sssd/sssd.conf необходимо изменить значение:

enumerate = false

Для samba – в конфигурационном файле /etc/samba/smb.conf необходимо изменить значения:

winbind enum users = no

winbind enum groups = no

При этом для доменных пользователей не будет возможности назначать права средствами SNManager.

Для назначении прав доменному пользователю в дальнейшем необходимо будет использовать CLI-утилиты Secret Net LSP.

После того как доменному пользователю будут назначены права средствами CLI-утилит, пользователь отобразится в SNManager для подсистемы, на которую были назначены права и появится возможность управления из SNManager.

29. В Secret Net LSP не поддерживается работа с именами пользователей, в которых содержатся кириллические символы.

4. Сведения о совместимости с другим ПО

В разделе содержатся сведения о совместимости СЗИ Secret Net LSP версии 1.10 со сторонними программными средствами при совместном функционировании.

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

- СЗИ Secret Net 7.7;
- СЗИ Secret Net Studio 8.4, 8.5, 8.6;
- ПАК "Соболь" 3.0.6, 3.0.9, 3.1, 4.2, 4.3;
- СКЗИ "Континент-АП" 3.7 (исполнения 5, 6).

2. Реализована совместимость СЗИ 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
Email:	info@securitycode.ru
Web:	https://www.securitycode.ru