СЗИ Secret Net LSP

Служба обеспечения совместимости <gost@basealt.ru>, Леонид Кривошеин

Version 1.2, 06.06.2023

Оглавление

1. Системные требования

Процессор	В соответствии с требованиями установленной ОС
Архитектура CPU	**x86_64** (amd64, EM64T)
Количество ядер	Минимум **2 ядра** процессора
Оперативная память	Минимум **2Гб** ОЗУ, рекомендуется **4Гб** ОЗУ
Жёсткий диск	Должно быть доступно для установки **не менее 1Гб**
ОС и ядро ОС	Только из числа поддерживаемых продуктом
Токен или смарт-карта	Опционально, см. стр. 9 руководства администратора СЗИ

1.1. Дистрибутив ОС Альт

В примере ниже все операции выполняются на ОС `Альт Рабочая станция 10.1` (репозиторий p10) с ядром **5.10-std-def**. На момент написания настоящей инструкции продуктом **v1.12** поддерживаются следующие ОС:

- `Альт 8 СП` «рабочая станция» с ядром **5.10-std-def** на репозитории c9f2;
- `Альт Рабочая станция 9.2` с ядром **5.10-std-def** на репозитории p9;
- `Альт Сервер 9.2` с ядром **5.10-std-def** на репозитории p9;
- `Альт Рабочая станция 10` (**5.10-std-def** и **5.15-un-def**, p10);
- `Альт Сервер 10` (**5.10-std-def** и **5.15-un-def**, p10);
- `Альт Рабочая станция K 10` (**5.15-un-def**, p10).

Серверные ОС Альт должны быть развёрнуты с графической средой рабочего стола MATE, при установке ОС Альт Сервер должен выбираться профиль «Офисный сервер».

Следует иметь ввиду, что мажорные версии ядер в дистрибутивах ОС Альт со временем могут меняться, например, ядро **5.10-std-def** в какой-то момент может быть заменно новым LTS-ядром **6.1-std-def**, однако производитель СЗИ в настоящий момент поддерживает такие обновления в течении жизненного цикла ОС.

1.2. Дистрибутив Secret Net LSP v1.11

Пользователям СЗИ `Secret Net LSP v1.11` доступно обновление до версии **1.12**, разница между этими двумя версиями не большая. Для ОС `Альт Рабочая станция 9` и `Альт Сервер 9` предусмотрена упрощённая процедура обновления продукта СЗИ `Secret Net LSP` с версии **1.11** на версию **1.12**. Для остальных ОС переход на новую версию требует предварительного сохранения настроек приложения и полного удаления его с компьютера с последующей установкой и восстановлением настроек из резервной копии.

1.3. Дистрибутив Secret Net LSP v1.12

Table 1. Комплект поставки:

Наименование и версия пакета дистрибутива	**КС ФИКС**
sn-lsp_1.12-334.alt0.c9f2.x86_64.rpm	F7A3E056
sn-lsp_1.12-334.alt0.p9.x86_64.rpm	8F9ADD2C
sn-lsp_1.12-334.alt0.p10.x86_64.rpm	8F9ADD2C
sn-firewall_1.2-144.alt0.c9f2.x86_64.rpm	1883876E
sn-firewall_1.2-144.alt0.p9.x86_64.rpm	E8CDAD39
sn-firewall_1.2-144.alt0.p10.x86_64.rpm	FF441270

Релизный набор пакетов продукта допускает установку на не обновлённую ОС Альт только для перечисленных ниже выпусков операционной системы и версии ядра:

- `Альт Рабочая станция 10.0` с ядром **5.10.82-std-def-alt1**;
- `Альт Сервер 10.0` с ядром **5.10.82-std-def-alt1**.

При обновлении СЗИ `Secret Net LSP` либо установке на обновлённую или не указанную в этом списке ОС Альт, следует использовать не релизный комплект дистрибутива продукта, а пакеты из отдельно подключаемого репозитория:

https://download.securitycode.ru/snlsp/alt/

Изготовитель СЗИ `Secret Net LSP` предпринимает большие усилия, чтобы обновления компонентов продукта и ОС максимально соответствовали актуальным требованием безопасности и были удобны конечным пользователям, для чего организована раздача результатов «догоняющей сборки» через выше указанный публичный репозиторий.

Также следует иметь ввиду, что в процессе жизненного цикла СЗИ `Secret Net LSP` пакеты продукта были переименованы. В формуляре и документации встречаются как новые, так и изначальные названия пакетов:

- `sn-lsp` ⇒ `secretnet` (СЗИ Secret Net LSP)
- `sn-firewall` ⇒ `snlsp-firewall` (Персональный межсетевой экран)

Служба обеспечения совместимости ООО «Базальт СПО» рекомендует выполнять установку пакетов дистрибутива `Secret Net LSP v1.12` только из указанного репозитория обновления, соответствующего бранчу дистрибутива (p9, p10, c9f2).

2. Предварительные условия

Процедуры установки, обновления и удаления Secret Net LSP выполняются администратором, обладающим правами суперпользователя компьютера. Перед установкой СЗИ Secret Net LSP необходимо убедиться в выполнении следующих требований:

- На компьютере установлена поддерживаемая ОС Альт;
- ОС Альт и ядро обновлены из соответствующего дистрибутиву репозитория;
- Ядро операционной системы должно входить в список ядер, заявленных как поддерживаемые компанией — разработчиком СЗИ, и соответствовать устанавливаемому дистрибутиву Secret Net LSP;
- Если необходим доменный функционал, вводить компьютер в домен Windows рекомендуется после установки СЗИ, если же он был введён в домен до установки пакетов СЗИ, необходимо выполнить проверку конфигурационных файлов на соответствие инструкции в руководстве администратора СЗИ на стр. 70-75.

Рекомендуемая процедура обновления ОС и ядра:

```
$ su-
# apt-get update
# apt-get dist-upgrade
# update-kernel [-t std-def |-t un-def]
# reboot

$ su-
# remove-old-kernels [-t std-def |-t un-def]
# apt-get autoremove
# apt-get clean
```

Для поддержки входа в ОС по токенам и смарт-картам выполните такие команды:

```
# apt-get remove --purge openct pcsc-lite-openct
# apt-get install libjcpkcs11 isbc-pkcs11 librtpkcs11ecp
```

Также необходимо установить пакет **apt-https***:*

```
# apt-get install apt-https
```

Посмотреть текущий список поддерживаемых продуктом ядер ОС можно на нижеперечисленных страницах, в зависимости от используемого репозитория:

- c9f2 (Альт 8 СП «рабочая станция»);
- p9 (Альт Рабочая станция 9.2, Альт Сервер 9.2);
- p10 (Альт Рабочая станция 10, Альт Рабочая станция K 10, Альт Сервер 10).

3. Установка Secret Net LSP

3.1. Убедитесь, что текущее ядро поддерживается продуктом (см. предыдущий раздел). При отсутствии поддержки можно воспользоваться архивом репозитория **p9** или **p10** для установки последнего поддерживаемого продуктом ядра. Например, для установки ядра **5.10.176-std-def-alt1** из архива p10, нужно выполнить:

```
$ su-
# apt-repo rm all
# epm repo add archive 2023/03/30
# apt-get update
# update-kernel
# reboot

$ su-
# remove-old-kernels
# apt-get autoremove
# apt-get clean
# apt-repo set p10
```

Но использование архива — не единственный вариант. В случае `Альт 8 СП` архив недоступен. Другой вариант — подождать, когда в репозитории обновления `Secret Net LSP` появится поддержка последнего ядра из ОС Альт. Сборка пакетов в этот репозиторий немного отстаёт от Альт'овых сборок ядра. Третий вариант — получить консультацию в службе технической поддержки ООО «Код безопасности».

Если версия установленного ядра ОС не поддерживается продуктом, продукт нельзя обновлять и нельзя устанавливать!

3.2. Подключите репозиторий обновления продукта.

Пример для продуктов на «десятой платформе»:

```
cat >/etc/apt/sources.list.d/snlsp.list <<EOF
rpm https://download.securitycode.ru/snlsp/alt/10/1.12/updates x86_64 updates
EOF
```

3.3. Обновите индексы:

```
# apt-get update
```

3.4. Установите `Secret Net LSP`:

```
# apt-get install secretnet
```

3.5. Перезагрузите компьютер. При следующем входе в систему появится сообщение: «Отсутствует лицензия. Введите лицензию чтобы активировать Secret Net LSP».

3.6. Пропишите свою лицензию:

```
# snlicensectl -c <Файл_лицензии>.lic
```

При этом не должно появиться сообщений об отвергнутой или просроченной лицензии, в противном случае следует обратиться за консультацией в службу технической поддержки ООО «Код безопасности».

3.7. Проверить установленную лицензию можно командой:

```
# snlicensectl -s
```

3.8. Установите модуль персонального межсетевого экрана (ПМЭ), если это допускает ваша лицензия, и включите соответствующую политику:

```
# apt-get install snlsp-firewall
# snpolctl -p firewall -c firewall,state,1
Request for policy change sent successfully
```

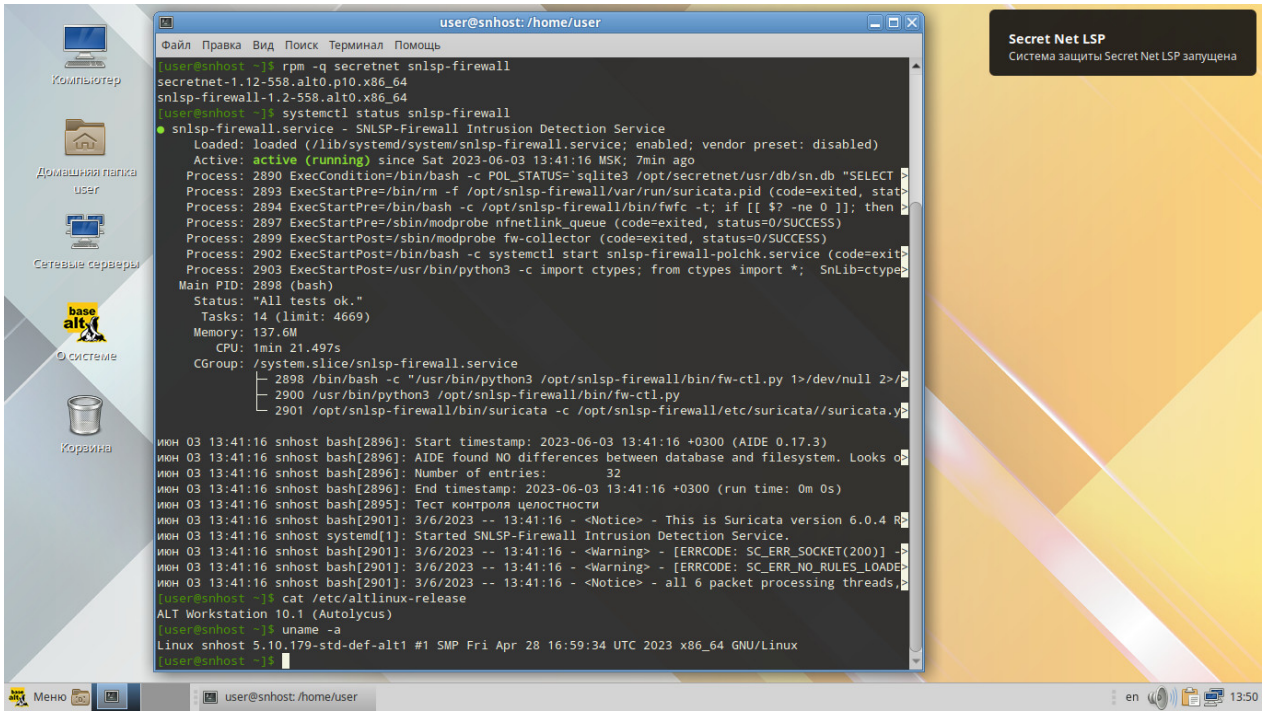
3.9. Убедитесь, что служба ПМЭ успешно стартовала:

```
# systemctl status snlsp-firewall
* snlsp-firewall.service - SNLSP-Firewall Intrusion Detection Service
     Loaded: loaded (/lib/systemd/system/snlsp-firewall.service; enabled; vendor preset:
     Active: active (running) since Sat 2023-06-03 13:17:09 MSK; 8s ago
...
```

4. Проверка работы Secret Net LSP

Отделами тестирования ООО «Базальт СПО» и ООО «Код безопасности» выполнена полная проверка функционала продукта, в соответствии с документацией, включая работу в домене, поддержку входа по токенам и смарт-картам, контроля доступа к локальным устройствам, работу ПМЭ и взаимодействие с `Secret Net Studio` под Windows. Вы можете повторить все шаги руководств пользователя и администратора СЗИ, а можете проверить работу продукта по быстрому, как предлагается ниже.

4.1. При входе в систему под любым пользователем должно появиться сообщение о том, что система защиты `Secret Net LSP` запущена (рис. 1):



4.2. Посмотрите версию установленного в системе ядра:

```
$ uname -a
Linux snhost 5.10.179-std-def-alt1 #1 SMP
 Fri Apr 28 16:59:34 UTC 2023 x86_64 GNU/Linux
```

4.3. Посмотрите версию установленной ОС:

```
$ cat /etc/altlinux-release
ALT Workstation 10.1 (Autolycus)
```

4.4. Посмотрите версии установленных пакетов продукта:

```
$ rpm -q secretnet snlsp-firewall
secretnet-1.12-558.alt0.p10.x86_64
snlsp-firewall-1.2-558.alt0.p10.x86_64
```

4.5. Убедитесь, что служба ПМЭ успешно стартовала:

```
$ systemctl status snlsp-firewall
* snlsp-firewall.service - SNLSP-Firewall Intrusion Detection Service
     Loaded: loaded (/lib/systemd/system/snlsp-firewall.service; enabled; vendor preset:
     Active: active (running) since Sat 2023-06-03 13:17:09 MSK; 8s ago
...
```

4.6. Посмотрите белый список пользователей и групп:

```
$ su-
# snaecctl view -U -G
Белый список пользователей:
Белый список групп:
Источник политики: локальный
```

4.7. Проверьте работу экспорта настроек:

```
# snbckctl -b
Резервное копирование выполнено успешно
Копирование параметра управления доступом: OK
Копирование правил ЗПС: OK
Копирование параметров аутентификации: OK
Копирование журналов: OK
Копирование политик: OK
Копирование настроек SecretNet: OK
Копирование пользователей и групп: OK
```

4.8. Посмотрите информацию о созданной резервной копии:

```
# snbckctl -l
ID копии:    1654847340
Дата:        03.06.2023 13:49:00
Сохраненные данные:
    пользователи и группы
    настройки SecretNet
    журналы
    политики
    параметры аутентификации
    контроль доступа
    замкнутая программная среда
```

5. Удаление Secret Net LSP

Удаление СЗИ Secret Net LSP необходимо производить после того, как будет удалён модуль персонального межсетевого экрана (ПМЭ).

5.1. Войдите в учётную запись **root** и отключите политику ПМЭ:

```
$ su-
# snpolctl -p firewall -c firewall,state,0
```

5.2. Удалите модуль ПМЭ:

```
# apt-get remove --purge snlsp-firewall
```

При этом в каталоге **/opt/snlsp-firewall** останутся файлы журналов и файлы конфигурации. При необходимости, этот каталог можно удалить вручную.

5.3. Удалите пакет СЗИ Secret Net LSP:

```
# apt-get remove --purge secretnet
```

При удалении Secret Net LSP в ОС Альт сохраняется каталог **/opt/secretnet-archive** с файлами журналов установки/удаления СЗИ. Если после удаления Secret Net LSP эта информация больше не нужна, каталог и его содержимое можно удалить вручную.

5.4. Перезагрузите компьютер.

6. Обновление Secret Net LSP и ОС Альт

Порядок обновления СЗИ описан в разделе 8 на стр. 16 формуляра продукта. СЗИ Secret Net LSP может обновляться штатными средствами обновления ОС при соблюдении следующих условий:

- На объекты файловой системы не наложено ограничений, препядствующих штатной процедуре обновления ОС и ядра ОС;
- Обновляемое ядро ОС входит в список поддерживаемых продуктом ядер.

Для обновления штатным способом достаточно выполнить рекомендуемую процедуру, описанную в разделе 2 настоящей инструкции. Далее описан более сложный механизм обновления, предусматривающий удаление и установку СЗИ.

В случае обновления ОС Альт, под управлением которой находится защищаемый компьютер, в СЗИ Secret Net LSP реализована возможность сохранения ранее выполненных настроек ПО. Для обновления ОС и пакетов ПО СЗИ:

6.1. Создайте резервную копию настроек СЗИ Secret Net LSP с помощью утилиты **snbckctl** (см. стр. 57 руководства администратора СЗИ);

6.2. Выполните удаление СЗИ Secret Net LSP (см. предыдущий раздел);

6.3. Выполните штатное обновление ОС Альт и ядра ОС рекомендуемым способом (см. раздел 2 настоящей инструкции);

6.4. Выполните установку зависимостей и актуальной версии СЗИ Secret Net LSP (см. разделы 2-3 настоящей инструкции и стр. 28 руководства администратора СЗИ).

6.5. Восстановите выполненные ранее настройки СЗИ Secret Net LSP с помощью утилиты **snbckctl** (см. стр. 57 руководства администратора СЗИ).

См. также Главу 2 руководства администратора СЗИ.