SELinux в НАЙС.ОС — мандатный контроль доступа по умолчанию

SELinux (Security-Enhanced Linux) — это система мандатного контроля доступа, встроенная в ядро Linux и расширяющая стандартную модель безопасности. Она обеспечивает чёткое разграничение прав на основе политик безопасности, а не только пользовательских прав. В НАЙС.ОС SELinux включён по умолчанию и работает в режиме targeted, ограничивая действия системных служб, пользовательских приложений и контейнеров. В редакциях с повышенными требованиями безопасности доступна и политика MLS (многоуровневая защита). Что получает пользователь: Защиту от эксплойтов, эскалации прав и нарушений изоляции; Контроль доступа даже для процессов с правами root; Гарантию, что один сервис не сможет прочитать данные другого — даже при уязвимости; Логи и аудит событий безопасности через journalctl и auditd. Итог: SELinux делает систему стойкой к взлому на архитектурном уровне. В НАЙС.ОС он работает «из коробки», без дополнительной настройки.

1. Что такое SELinux: базовая модель

SELinux (Security-Enhanced Linux) — это подсистема ядра Linux, реализующая мандатный контроль доступа (MAC). Она была разработана **Агентством национальной безопасности США (NSA)** и впервые появилась в ядре Linux 2.6. Сейчас SELinux полностью интегрирован в основной *upstream* и активно поддерживается в дистрибутивах Fedora, RHEL, Debian, Gentoo и, конечно, **НАЙС.ОС** .

SELinux позволяет администраторам определять и применять **жёсткие политики доступа** , не зависящие от прав владельца файла или процесса. Это противостоит классической модели добровольного контроля доступа (DAC), в которой root может всё, а файлы доступны по правам `chmod` / `chown` .

По сравнению с другими механизмами Linux MAC:

- **AppArmor** — проще в настройке, но слабее по модели (путь-ориентированная, без тэгов контекста);
- **TOMOYO** — ориентирована на белые списки системных вызовов;
- **SMACK** — минималистичная и ориентирована на встроенные системы (включена в Tizen);
- **SELinux** — самая строгая и универсальная система, поддерживает роли, домены, контексты, уровни доступа (MLS).

🖊 Чем SELinux отличается от chmod + chown?

В Linux без SELinux доступ к файлу определяется его владельцем (`chown`) и правами доступа (`chmod`). Например, root может читать и писать любой файл.

С SELinux доступ регулируется **политикой безопасности** , где для каждого процесса и файла задан контекст (например: `system_u:system_r:sshd_t:s0`). Даже root-процесс не сможет прочитать файл другого домена, если политика это запрещает.

Это создаёт **изолированные домены безопасности** , где уязвимость в одном сервисе (например, nginx) не позволяет атакующему скомпрометировать другие части системы.

2. Почему SELinux критически важен для защищённой ОС

SELinux — это не просто средство усиления безопасности, а **ключевой компонент архитектуры защищённой операционной системы** , такой как НАЙС.ОС. Он реализует мандатную модель контроля доступа, при которой даже root не может нарушить заданную политику.

- **Изоляция процессов по доменам безопасности** — каждый системный компонент (служба, пользователь, daemon) работает в своём домене , что не позволяет эксплойту в одной части системы повлиять на другие. Например, скомпрометированный `nginx_t` не сможет читать файлы в `sshd_t` или выполнять shell-команды.
- **Защита от LPE (local privilege escalation)** — SELinux блокирует попытки повысить привилегии, даже если злоумышленнику удалось запустить код с правами пользователя. Без изменения контекста (что невозможно без политики) — это тупик.

- **Устойчивость к post-exploit persistence** — злоумышленник не сможет оставить бэкдор, если контексты запрещают доступ к конфигурационным файлам или cron.
- **Поддержка нормативных требований** ФСТЭК:
  - Модель нарушителя МИЗ;
  - Мандатная модель управления доступом;
  - Контролируемые отношения субъект-объект через теги и политики.
- **Особенно актуален** в системах:
  - электронного документооборота (ЭДО);
  - удостоверяющих центров (УЦ);
  - взаимодействия через СМЭВ и ГИС;
  - работы с ИСПДн (персональными данными).

Вывод: SELinux обеспечивает архитектурную устойчивость системы к широкому классу атак, и является основой для сертификации уровня НДВ, ОУ, УЗ1 и выше.

3. SELinux в НАЙС.ОС: активен по умолчанию

В дистрибутиве **НАЙС.ОС** SELinux включён **сразу после установки** — никакой ручной активации не требуется. Поддержка заложена на всех уровнях загрузки:

- `GRUB` передаёт параметр `selinux=1 enforcing=1` ядру Linux;
- `initrd` содержит начальные политики и монтирует корневую файловую систему с метками SELinux;
- `systemd` работает в контексте SELinux и запускает сервисы с доменными метками.

В зависимости от редакции ОС, по умолчанию применяется одна из политик:

- `targeted` — защита критичных служб (по умолчанию во всех редакциях);
- `mls` — многоуровневая политика (для редакций с УЗ1 / сертификацией ФСТЭК);

Уже встроены профили SELinux для ключевых компонентов:

- `sshd`, `sudo`, `gpg`, `tdnf` (пакетный менеджер);
- `systemd`, `journald` (инициализация и логирование);
- `nginx`, `OpenVPN`, `docker` и `podman`.

🛡️ **Бонус: auditd включён**

В системе предустановлены и активны **auditd** и **журналирование событий SELinux через `journald`**. Это позволяет отслеживать любые нарушения политик, попытки

обхода ограничений и потенциальные атаки в режиме реального времени.

Итог: SELinux не просто доступен в НАЙС.ОС — он является частью архитектуры безопасности «по умолчанию».

4. Как это работает в реальности

SELinux применяет **жёсткие правила разграничения доступа** , которые действуют даже при наличии root-прав. Ниже — реальные сценарии, как это защищает систему в повседневной работе:

📌 Пример 1: изоляция сервисов

Даже если злоумышленник получил доступ к оболочке под доменом `sshd_t` (например, через SSH), он **не сможет запустить nginx** напрямую:

```
$ sudo systemctl start nginx
Failed to start nginx.service: Access denied by SELinux policy.
```

Это происходит потому, что домен `sshd_t` не имеет права перехода в `nginx_t` . Таким образом, SELinux **блокирует горизонтальное перемещение** между сервисами.

📌 Пример 2: контроль доступа к файлам

Даже если процесс nginx запущен, он не сможет прочитать файлы пользователя:

```
[error] [client 127.0.0.1] (13)Permission denied: access to /home/user/file.txt denied
```

SELinux проверяет не только владельца и права файла, но и **метку безопасности** . Только файлы с меткой `httpd_sys_content_t` могут быть обслужены nginx.

🛡️ Пример 3: защита даже при root-доступе

Если атакующий получил shell под root, он всё равно ограничен. В режиме `MLS` и `RBAC` (Role-Based Access Control) SELinux запрещает доступ root-пользователю к данным и сервисам за пределами назначенного контекста:

```
root: read access to /var/secrets denied by policy (mls/role violation)
```

Это делает SELinux ключевым компонентом архитектурной защиты, предотвращая эскалацию и закрепление атаки даже в случае успешной компрометации.

Итог: SELinux в НАЙС.ОС — это не «дополнение», а полноценная система контроля, которая обеспечивает изоляцию и безопасность на каждом уровне.

5. Метки безопасности (labels) в НАЙС.ОС

В SELinux **всё имеет метку безопасности** — файлы, процессы, сокеты и даже устройства. Эти метки (или контексты) определяют, какие действия допустимы между субъектами и объектами. НАЙС.ОС поставляется с готовыми профилями и утилитами для работы с метками.

🗎 Метки файлов

Посмотреть метку файла можно командой:

```
$ ls -Z /var/www/html/index.html
system_u:object_r:httpd_sys_content_t:s0
```

Изменить временно — через `chcon`:

```
$ chcon -t httpd_sys_content_t file.txt
```

Восстановить правильную метку по шаблону — через `restorecon`:

```
$ restorecon -Rv /var/www/
```

Метки процессов

Для процессов используется команда `ps -eZ`:

```
$ ps -eZ | grep nginx
system_u:system_r:nginx_t:s0 1234 ? 00:00:01 nginx
```

Это позволяет чётко понимать, какой домен безопасности у каждого процесса.

Профили и шаблоны

- Все шаблоны меток хранятся в: `/etc/selinux/targeted/contexts/`
- Для создания пользовательских политик используются утилиты из пакета `policycoreutils`.

📝 Контексты в 3-х строках: `user:role:type:level`

- **user** : субъект SELinux (например, `system_u`, `unconfined_u`)
- **role** : роль (например, `system_r`, `staff_r`)
- **type** : ключевой элемент — определяет разрешения (например, `nginx_t`, `ssh_t`)
- **level** : уровень конфиденциальности (например, `s0`, `s0-s15:c0.c1023`)

И именно **type** управляет политикой доступа: кто и что может делать.

6. SELinux для администратора

SELinux может показаться сложным, но в НАЙС.ОС он сопровождается удобным набором инструментов для администрирования. Ниже — основные команды для проверки статуса, диагностики проблем и настройки политик.

🔍 Проверка состояния SELinux

- `getenforce` — выводит текущий режим: `Enforcing`, `Permissive` или `Disabled`.

```
$ getenforce
Enforcing
```

- `sestatus` — подробная информация о политике, режимах и статусе загрузки:

```
$ sestatus
SELinux status:                 enabled
Policy name:                    targeted
Current mode:                   enforcing
```

- `audit2why` — анализ причин отказа на основе журналов `/var/log/audit/audit.log`.

🚨 Устранение блокировок

Когда SELinux блокирует действия, сообщения попадают в системный журнал. Их можно увидеть через:

```
$ journalctl -t setroubleshoot
```

Для генерации временного разрешения можно использовать:

```
$ grep AVC /var/log/audit/audit.log | audit2allow -M myfix
$ semodule -i myfix.pp
```

⚠️ **Важно:** использовать `audit2allow` нужно осознанно — лучше временно включить `Permissive`-режим для тестирования.

⚙️ Управление политиками

- `semanage` — универсальный инструмент для настройки портов, типов, логинов и прочего:

  ```
  $ semanage port -l | grep http
  http_port_t                    tcp      80, 443
  ```

- `setsebool` — включает/отключает boolean-переменные (условия доступа):

  ```
  $ setsebool -P httpd_can_network_connect on
  ```

- `checkmodule` и `semodule` — сборка и установка кастомных политик.
- `seinfo` — просмотр политик и объектов безопасности (требуется пакет `setools`).

Все эти инструменты предустановлены в административных сборках НАЙС.ОС и интегрированы с `auditd` и `journalctl` для облегчённой диагностики.

7. Как писать и отлаживать свои SELinux-профили

В НАЙС.ОС вы можете создавать собственные модули SELinux для поддержки новых служб или приложений. Это особенно важно для безопасной интеграции нестандартных компонентов в систему с мандатным контролем доступа.

🛠️ Минимальный профиль: структура

Стандартный модуль SELinux состоит из трёх файлов:

- `myservice.te` — политика (type, allow, переходы);
- `myservice.fc` — файлы и их контексты;
- `myservice.if` — интерфейсы (необязательно для модульного переиспользования).

Пример `.te`-файла для системной службы:

```
policy_module(myservice, 1.0)

type myservice_t;
init_daemon_domain(myservice_t, myservice_exec_t)

allow myservice_t self:process { fork transition };
allow myservice_t var_log_t:dir { read write search };
```

🎁 Сборка и установка

Для компиляции и установки своего профиля используйте:

```
$ checkmodule -M -m -o myservice.mod myservice.te
$ semodule_package -o myservice.pp -m myservice.mod -f myservice.fc
$ semodule -i myservice.pp
```

Отладка и тестирование

- Используйте `audit2allow` на этапе разработки, чтобы находить пропущенные разрешения.
- Временно переведите домен в *permissive*-режим:

  ```
  $ semanage permissive -a myservice_t
  ```

- Просматривайте логи отказов:

  ```
  $ journalctl -t setroubleshoot
  $ ausearch -m avc -ts recent
  ```

- Используйте `seinfo` и `sesearch` (из пакета `setools`) для анализа взаимодействий

между доменами.

🔄 Обновление и удаление

- `semodule -r myservice` — удалить модуль;
- `semodule -l` — список установленных модулей;
- `semodule -u myservice.pp` — обновить модуль без удаления.

В НАЙС.ОС локальные политики помещаются в `/etc/selinux/local`, а профили прошли валидацию на совместимость с `mls`-режимом.

💡 **Советы:**

- Не давайте службам `unconfined_t` — это нарушает модель SELinux.
- Изучите существующие .te-файлы в `/usr/share/selinux/targeted/` для шаблонов.
- Не забывайте про `restorecon` после установки контекстов.

8. Поддержка в системных пакетах

В НАЙС.ОС SELinux поддерживается на уровне системной сборки — все ключевые компоненты системы поставляются с корректно прописанными SELinux-контекстами и необходимыми правилами.

- **Все базовые системные службы** собраны с поддержкой SELinux: установлены корректные типы (`systemd_t`, `initrc_t`, `unconfined_t`), контексты файлов, а также policy-файлы.
- В систему включены **модули SELinux-политик** для популярных сервисов:
  - `nginx` — ограничение доступа к контенту, сокетам, модулям;
  - `postgresql` — безопасная работа базы данных без доступа к пользовательским данным;
  - `dnf` / `tdnf` — только чтение репозиториев и запись во временные каталоги;
  - `podman` / `docker` — отдельные домены для контейнеров (контейнер isolation);
  - `usbguard` — контроль правил и правил авторизации устройств;
  - `usbmon` — безопасный доступ к системным трассировщикам USB;
  - `crond` — контроль запуска скриптов с правильным типом пользователя.
- **Спецификации RPM-пакетов** адаптированы: секции `%filecontext` и `%post` устанавливают нужные метки через `restorecon`.
- Все профили проходят автоматическую валидацию в CI при сборке: используется `checkmodule`, `sepolgen` и `selinux-lint`.

Это гарантирует, что из коробки сервисы работают в изолированных доменах, и даже при наличии уязвимости в коде вредоносный процесс **не сможет выйти за пределы своей зоны ответственности** .

✔ **Пример: nginx**

В НАЙС.ОС `nginx` работает в домене `httpd_t` , имеет доступ только к `/var/www` и сокетам, при этом не может читать содержимое `/home` или файлов других служб.

Это предотвращает утечки конфиденциальных данных даже при эксплуатации RCE-уязвимостей.

9. Мандатный контроль (MLS): опционально

В дополнение к стандартной политике SELinux, в НАЙС.ОС предусмотрена **опциональная поддержка мандатного разграничения доступа по уровням конфиденциальности (MLS — Multi-Level Security)** . Эта модель применяется в высокозащищённых системах, где необходимо строгое соблюдение правил доступа между субъектами и объектами в зависимости от их уровня секретности.

🏢 Особенности MLS в НАЙС.ОС

- Используется ядро с поддержкой `mls_policy.ko` , активируется при установке соответствующей редакции системы (например, редакция «Госзащита»).
- **Контексты безопасности** включают уровень секретности, например: `system_u:system_r:sshd_t:s0-s15:c0.c255`
- Поддерживается создание политик с уровнями `unclassified` , `confidential` , `secret` , `topsecret` , с обязательной маркировкой процессов и данных.
- Пользователи не могут самостоятельно повысить уровень доступа — это исключает несанкционированный доступ к более защищённым данным.
- **Встроенные роли** и правила передачи информации соответствуют требованиям ФСТЭК РФ для систем КС3/КС4 и классов защищённости 1Г/1Д.

📚 Применение в реальных системах

- ЦОД и виртуализированные среды с несколькими уровнями доступа;
- ИТ-системы в госсекторе и силовых структурах;
- Системы электронного документооборота (ЭДО) с допуском по уровню секретности;

- Удостоверяющие центры (УЦ) с требованиями по разграничению операторов.

🖊 Что даёт MLS по сравнению с обычным SELinux?

Обычный SELinux разделяет доступ между доменами процессов. MLS добавляет **иерархию уровней конфиденциальности** , которые нельзя пересечь без явного разрешения политики. Это особенно важно там, где необходимо исключить даже случайную утечку секретной информации.

10. Что дальше / Дорожная карта

SELinux в НАЙС.ОС уже обеспечивает мощный уровень изоляции и мандатного контроля доступа, но развитие продолжается. Ниже — ключевые направления развития SELinux-инфраструктуры в рамках будущих релизов дистрибутива.

🔗 Включение полной политики MLS по умолчанию

В редакции **ГОСТ.ОС** запланировано **включение полноценной политики `mls` по умолчанию** . Это позволит реализовать полное разграничение доступа по уровням секретности и категориям — в соответствии с требованиями к ИБ классов КС3/КС4 и ГОСТ Р 56939.

В рамках этой инициативы:

- Все системные службы и пользовательские процессы будут запускаться в доменах с соответствующими **уровнями и категориями** .
- Будут добавлены **механизмы автоматического назначения контекстов** для критичных данных при установке и конфигурировании.
- Расширится **набор политик для системных ролей** : администратор ИБ, оператор УЦ, модератор СМЭВ и т.д.

🛠 Расширение SELinux-инструментария

В планах — поставка встроенного графического средства для просмотра и редактирования политик SELinux (на базе `sepolicy` и `audit2why`), а также **веб-интерфейса для анализа SELinux-лога** и генерации временных правил.

Интеграция с сертификацией

В целях получения соответствия требованиям ФСТЭК и Минобороны, вся инфраструктура SELinux в НАЙС.ОС будет:

- включена в состав технической документации;
- проверена на корректную реализацию мандатной модели;
- включена в процессы сертификационного тестирования как механизм мандатного контроля доступа.

Итог: SELinux будет оставаться неотъемлемой частью архитектуры безопасности НАЙС.ОС, обеспечивая предсказуемую, управляемую и подтверждаемую защиту критичных процессов и данных.

Заключение

SELinux в НАЙС.ОС — это не дополнение, а **фундаментальный компонент безопасности** , встроенный на всех уровнях: от загрузки системы до пользовательских процессов.

Его наличие позволяет защитить систему даже от **компрометации root-пользователя** , за счёт мандатной модели доступа, строгих политик и изоляции по доменам безопасности.

Если вы создаёте или администрируете критически важные сервисы — **освойте SELinux** . Это не сложно: документации и инструментов предостаточно, а выгода — огромна: защита ядра, системных демонов, пользовательских данных и инфраструктурных компонентов от широкого спектра атак.

В НАЙС.ОС SELinux включён и настроен **по умолчанию** . Не выключайте его — используйте его возможности. А если вам нужно больше — подключайтесь к разработке, предлагайте свои профили и правила. Мы открыты к сотрудничеству.

🛡️ **SELinux — это простая, но мощная защита, которую нельзя игнорировать.**