Прокофьева Арина Сергеевна

Студент

РГУ нефти и газа (НИУ) имени И. М. Губкина

Прокофьева Мария Сергеевна

Студент

РГУ нефти и газа (НИУ) имени И. М. Губкина

ПРИМЕНЕНИЕ D-BUS ДЛЯ УПРАВЛЕНИЯ GNOME В ОС АЛЬТ. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация: Статья посвящена анализу применения механизма межпроцессного взаимодействия D-Bus для управления графической средой GNOME в операционной системе Альт. Рассматриваются возможности управления компонентами GNOME через сессионную шину D-Bus с использованием инструментов busctl, gsettings и dbus-monitor. Особое внимание уделено вопросам безопасности: анализируются стандартные политики доступа сессионной шины, выявляются потенциальные уязвимости (несанкционированное управление, spoofing сигналов, DoS-атаки, утечки информации) в многопользовательских сценариях и при интеграции с Alterator. Предложены практические рекомендации по повышению безопасности путём создания кастомных политик. Исследование проведено на ОС Альт Рабочая станция 11.0, подтверждены гипотезы об эффективности D-Bus и недостаточной строгости стандартных политик.

Ключевые слова: D-Bus, GNOME, ОС Альт, межпроцессное взаимодействие, сессионная шина, политики безопасности, уязвимости безопасности

Prokofieva A.S.

Student

Gubkin Russian State University of Oil and Gas

Prokofieva M.S.

Student

Gubkin Russian State University of Oil and Gas

USING D-BUS TO CONTROL GNOME IN ALT OS. SECURITY ISSUES

Annotation: *The article is devoted to the analysis of the use of the D-Bus interprocess communication mechanism for managing the GNOME graphical environment in the Alt operating system. The possibilities of controlling GNOME components through the session D-Bus are considered using tools such as busctl, gsettings, and dbus-monitor. Particular attention is paid to security issues: standard session bus access policies are analyzed, potential vulnerabilities (unauthorized control, signal spoofing, DoS attacks, information leakage) in multi-user scenarios and integration with Alterator are identified. Practical recommendations for improving security by creating custom policies. The study was conducted on Alt Workstation 11.0; the hypotheses about the effectiveness of D-Bus and the insufficient strictness of standard policies were confirmed.*

Keywords: D-Bus, GNOME, Alt Linux, interprocess communication, session bus, security policies, security vulnerabilities

Введение

В современных дистрибутивах Linux на базе графических сред рабочего стола, таких как GNOME, ключевую роль играет механизм межпроцессного взаимодействия (IPC). В операционной системе Альт (разработка компании BaseALT) GNOME является основной графической

оболочкой в редакциях Рабочая станция и Сервер с графическим интерфейсом. Здесь GNOME интегрируется с инструментами администрирования, включая Центр управления системой (Alterator на D-Bus).

D-Bus выступает стандартом де-факто для IPC в desktop-окружениях Linux, обеспечивая обмен сообщениями между компонентами GNOME (настройками, уведомлениями, расширениями, сессиями). Исследования разработчиков freedesktop.org и GNOME Foundation подтверждают эффективность D-Bus, но выявляют риски безопасности: слабые политики доступа в сессионной шине могут привести к несанкционированному управлению компонентами, эскалации привилегий или DoS-атакам.

D-Bus (Desktop Bus) представляет собой систему межпроцессной коммуникации (IPC), разработанную в рамках проекта freedesktop.org. Это механизм, позволяющий приложениям обмениваться сообщениями в низкозатратном и низкозадержанном режиме. D-Bus состоит из нескольких слоев: библиотеки для прямого соединения (libdbus), демона (dbus-daemon), который управляет обменом сообщениями, и спецификаций для интерфейсов. Стандарт D-Bus определяет формат сообщений, включая заголовки, типы данных и сигнатуры методов. Основные компоненты включают системную шину (system bus) для глобальных сервисов и сессионную шину (session bus) для пользовательских сессий. D-Bus широко используется в десктопных окружениях, таких как GNOME, для координации процессов, управления настройками и уведомлениями [2]. Спецификация D-Bus доступна на официальном сайте проекта, где описаны протоколы, типы сообщений и правила валидации [5].

В ОС Альт D-Bus активно используется в Alterator для взаимодействия модулей в графической среде. Настоящее исследование анализирует применение D-Bus для управления GNOME в ОС Альт, детально рассматривает вопросы безопасности и предлагает рекомендации по минимизации рисков на основе практических примеров.

Объект, предмет и цель

Объект исследования — механизмы межпроцессного взаимодействия в графической среде GNOME операционной системы Альт.

Предмет исследования — применение шины D-Bus (сессионной и системной) для управления компонентами GNOME, включая конфигурацию политик доступа и потенциальные уязвимости безопасности.

Цель исследования — детально проанализировать возможности и практику применения D-Bus для управления GNOME в ОС Альт; выявить и классифицировать угрозы безопасности, связанные с политиками доступа и межпроцессным взаимодействием; предложить практические рекомендации по повышению безопасности на основе экспериментальных данных из среды ОС Альт; подтвердить или опровергнуть гипотезы о рисках в стандартной конфигурации.

Литературный обзор

D-Bus — система межпроцессного общения, разработанная в проекте freedesktop.org. Она включает системную шину (system bus) для глобальных событий и сессионную шину (session bus) для пользовательских сессий.

В GNOME D-Bus управляет настройками (org.gnome.desktop.interface), уведомлениями и расширениями. В ОС Альт D-Bus интегрирован в Alterator,

где модули обмениваются данными через шину для графического администрирования.

Анализ исследований (спецификация D-Bus, документация GNOME) показывает уязвимости:

- По умолчанию сессионная шина разрешает широкие права (allow own="", allow send_destination=""), что позволяет процессам одного пользователя влиять на другие в многопользовательских сценариях.
- Известны CVE (например, связанные с spoofing сигналов в GLib, утечками в gnome-remote-desktop, DoS через исчерпание FD).
- Политики доступа настраиваются в файлах /usr/share/dbus-1/session.conf и /etc/dbus-1/session.d/.

Публикации по использованию D-Bus для управления GNOME, особенно в контексте безопасности, охватывают введение в протокол, его интеграцию в десктопные окружения и потенциальные уязвимости. В статье "Введение в D-BUS" на OpenNET подчеркивается, что D-Bus заменяет более сложные системы вроде CORBA в GNOME, интегрируясь с HAL для управления оборудованием, и обсуждаются аспекты безопасности через политики доступа в конфигурационных файлах [3]. Статья "Тотальный контроль приложений с системой D-Bus" в журнале Хакер описывает, как D-Bus позволяет управлять приложениями в GNOME и KDE через команды вроде dbus-send, но предупреждает о рисках неавторизованного доступа и необходимости аутентификации для предотвращения уязвимостей в системах [4].

В контексте интеграции с systemd, публикация "GNOME адаптирован для управления через systemd" на OpenNET отмечает, что gnome-session

использует D-Bus для управления сессиями, что повышает безопасность через sandboxing, но требует systemd для полной функциональности [5]. По вопросам безопасности, статья на Linux.org.ru о семилетнем баге в Polkit (CVE-2021-3560) объясняет, как уязвимость позволяет эскалацию привилегий через D-Bus в GNOME, используя dbus-send для обхода аутентификации, что актуально для дистрибутивов вроде Ubuntu и потенциально ALT [6]. Аналогично, на Anti-Malware.ru обсуждается уязвимость в GNOME AccountsService (CVE-2021-3939), где через D-Bus можно получить root-доступ в Ubuntu, подчеркивая необходимость патчей для Linux-систем [7].

Для ALT Linux, публикация "Опубликована одиннадцатая платформа ALT" на OpenNET упоминает интеграцию D-Bus в Alterator для системного управления, включая GNOME 46, с акцентом на безопасность через MAC и TLS в сервисах [8]. В целом, публикации подчеркивают полезность D-Bus для управления GNOME в ALT, но акцентируют внимание на настройке политик и обновлениях для минимизации рисков, с редкими упоминаниями иностранных источников для базовых спецификаций.

Гипотезы исследования:

1. D-Bus эффективно управляет GNOME в ОС Альт через инструменты вроде dbus-send и gsettings.
2. Стандартные политики сессионной шины в GNOME ОС Альт недостаточно строгие, создавая риски несанкционированного доступа.
3. Кастомные политики в /etc/dbus-1/session.d/ позволяют ограничить риски без потери функциональности.

Методы исследования

Тип исследования — прикладное экспериментальное, сочетающее анализ документации, конфигурационных файлов и практическое тестирование команд в реальной среде.

Характеристика выборки — исследование проводилось на операционной системе Альт Рабочая станция версии 11.0 (актуальной на дату исследования) с установленной графической средой GNOME по умолчанию. Тестирование выполнялось в одиночной и имитированной многопользовательской сессии (с несколькими пользователями).

Цель исследования (детализация в контексте методов): достижение цели осуществляется через последовательные этапы — от анализа стандартной конфигурации D-Bus и GNOME до тестирования управления компонентами, выявления уязвимостей и применения мер защиты. Это позволяет не только описать функциональность, но и количественно/качественно оценить риски безопасности.

Методы сбора данных:

- Анализ официальной документации ОС Альт (разделы по Alterator на D-Bus и GNOME).
- Осмотр конфигурационных файлов D-Bus (/usr/share/dbus-1/session.conf, /etc/dbus-1/session.d/).
- Использование утилит: busctl --user, dbus-send, gdbus, dbus-monitor для просмотра и взаимодействия с шиной.

Описание процедуры проведения исследования:

1. Установка и запуск ОС Альт Рабочая станция с GNOME.
2. Запуск GNOME-сессии, проверка наличия сессионной шины (echo $DBUS_SESSION_BUS_ADDRESS).

3. Просмотр активных сервисов: busctl --user tree.
4. Тестирование управления: изменение настроек GNOME через D-Bus (gdbus call).
5. Анализ стандартных политик: cat /usr/share/dbus-1/session.conf.
6. Симуляция угроз: попытки отправки сообщений от одного пользователя к сервисам другого (в многопользовательском режиме).
7. Применение кастомных политик: создание файла в /etc/dbus-1/session.d/, перезапуск сессии, верификация ограничений.
8. Мониторинг событий: dbus-monitor --session.

Методы обработки данных — качественный анализ вывода команд, интерпретация политик доступа, сравнение поведения до и после применения ограничений.

Результаты исследования

В ОС Альт GNOME полностью зависит от сессионной шины D-Bus. Практические примеры управления:

1. Просмотр сервисов:

busctl --user tree

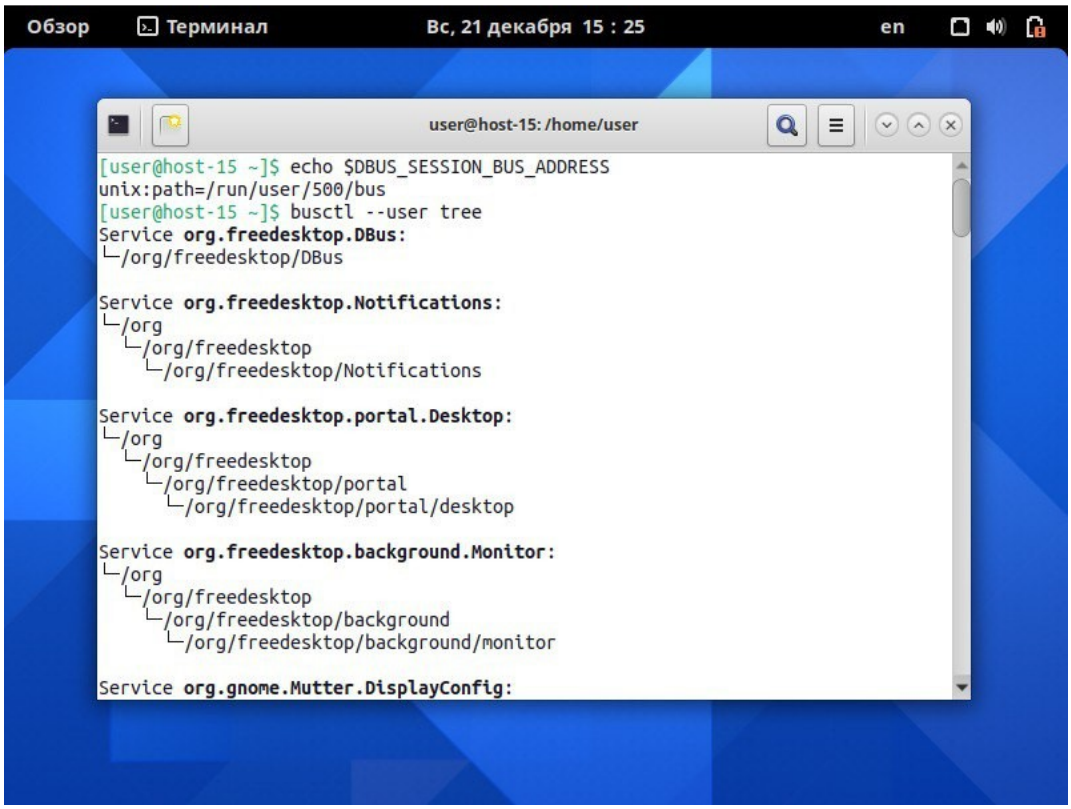

Рисунок 1 – Просмотр сервисов

Вывод включает org.gnome.Shell (управление оболочкой), org.gnome.SettingsDaemon (настройки), org.gnome.Mutter (оконный менеджер), org.freedesktop.portal.Desktop (порталы для sandbox).

2. Изменение настроек:

gsettings set org.gnome.desktop.interface gtk-theme 'Adwaita-dark'

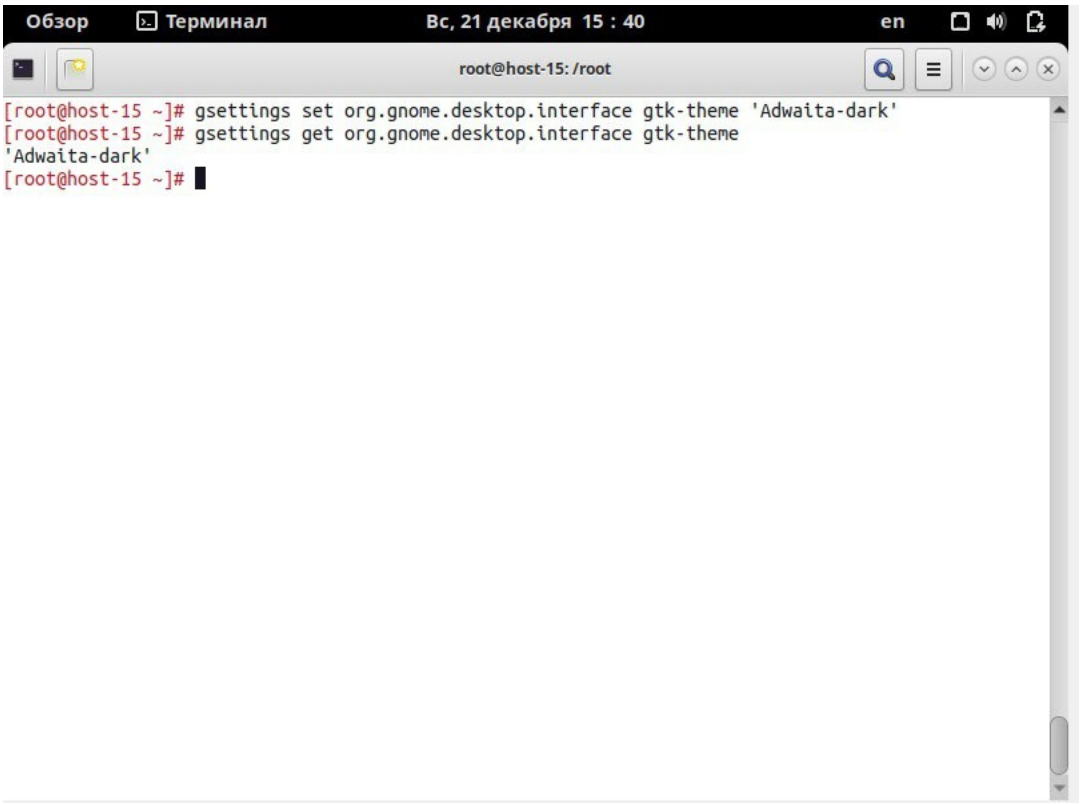

Рисунок 2 – Изменение настроек

Применяет тёмную тему; эквивалент через gdbus для свойств; также включение night-light: gsettings set org.gnome.settings-daemon.plugins.color night-light-enabled true.

3. Мониторинг:

dbus-monitor --session interface='org.gnome.SettingsDaemon'

Рисунок 3 - Монитринг

Позволяет наблюдать сигналы изменений (громкость, питание); busctl --user monitor для конкретных сервисов.

Вопросы безопасности:

Стандартная конфигурация сессионной шины (файл /usr/share/dbus-1/session.conf) содержит permissive-политики:

– <allow own=""/> — любой процесс может владеть именем.
– <allow send_destination=""/> — свободная отправка сообщений.

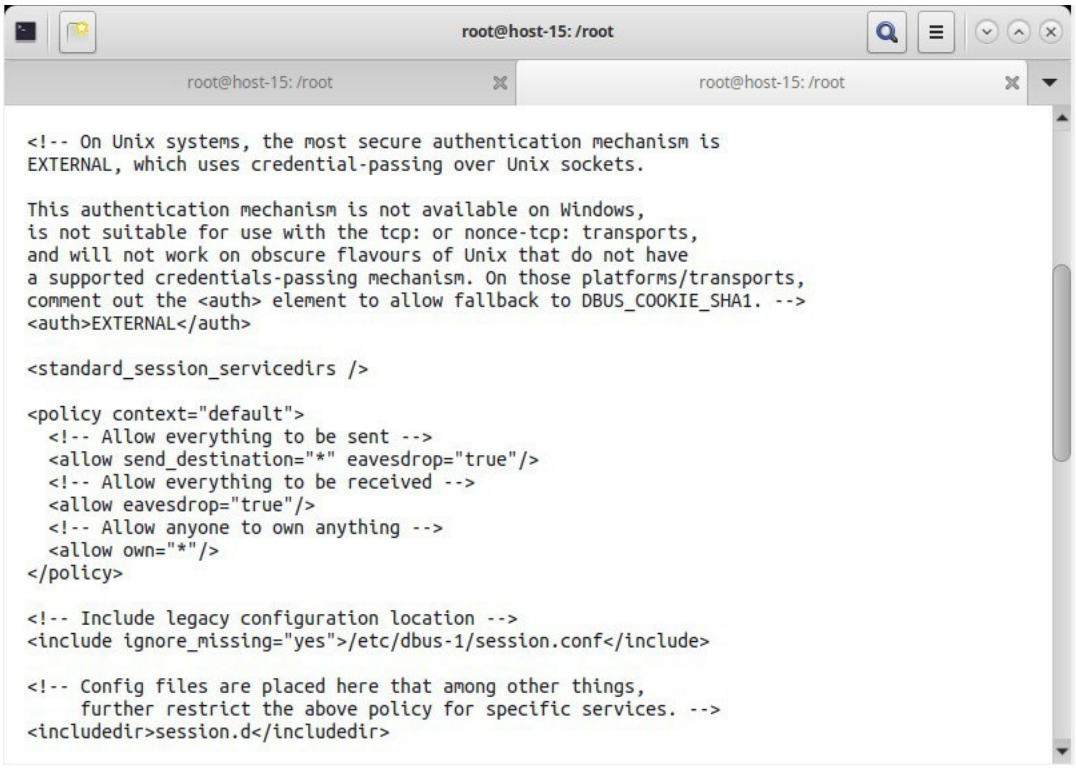

Рисунок 4 – Стандартная конфигурация сессионной шины

Это создает риски:

- Несанкционированное управление: В многопользовательской системе (несколько пользователей на одном ПК) процесс одного пользователя может отправлять сообщения сервисам GNOME другого, изменяя настройки или инъектируя события.
- Spoofing сигналов: Вредоносное приложение может эмулировать сигналы от trusted-сервисов (известно по CVE в GLib/GDBus).
- DoS: Исчерпание file descriptors или соединений.
- Утечки информации: В некоторых расширениях GNOME (например, remote desktop) возможны утечки через неавторизованные интерфейсы.

В ОС Альт риски аналогичны стандартному GNOME, но усиливаются интеграцией с Alterator на D-Bus: несанкционированный доступ к модулям администрирования возможен в сессии.

Рекомендации по защите:

Создать файл /etc/dbus-1/session.d/gnome-restrict.conf, с содержимым:

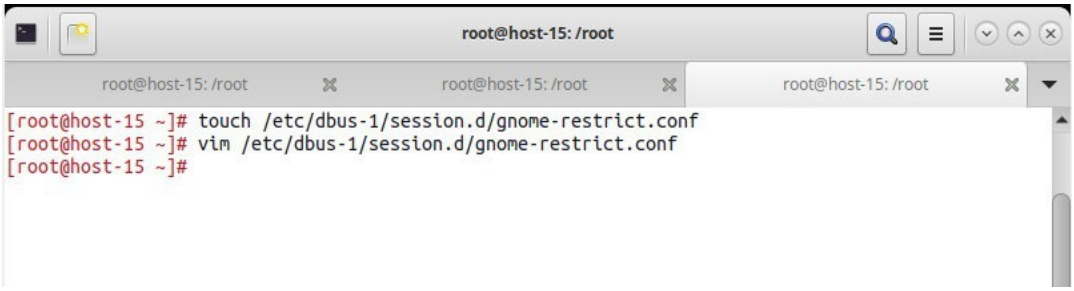

Рисунок 5 – Создание файла политик безопасности

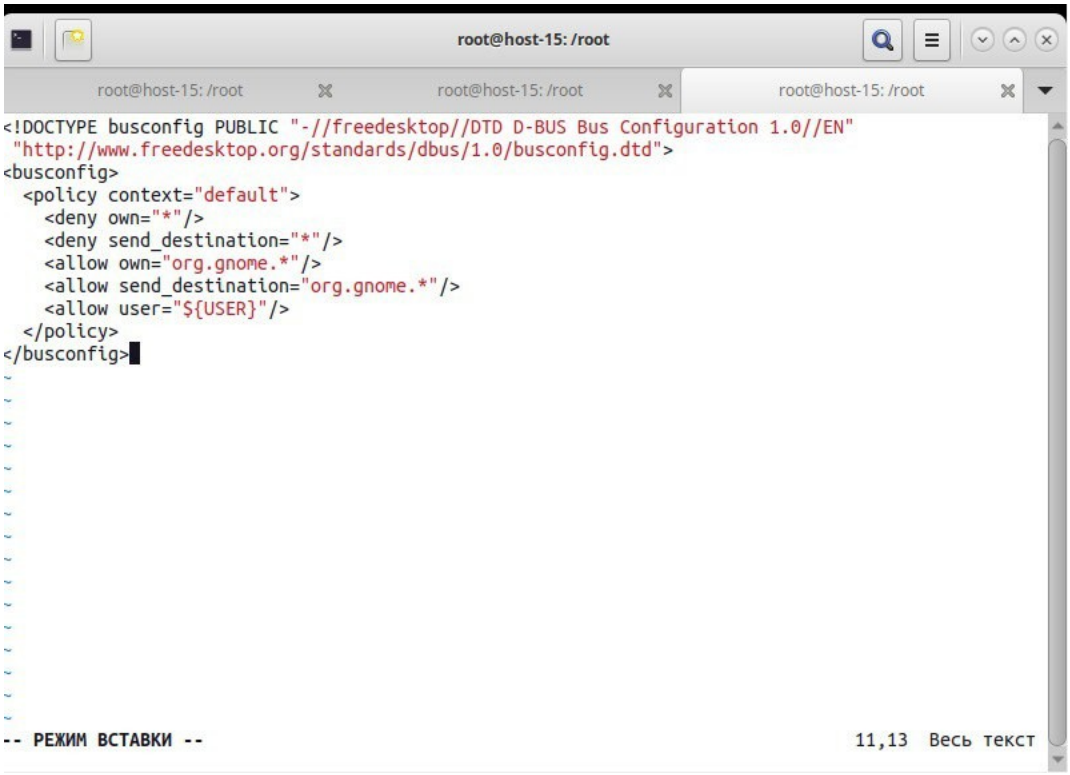

Рисунок 6 – Содержимое файла политик безопасности

После перезапуска GNOME ограничения применяются, блокируя внешний доступ при сохранении функциональности.

Обзор функционала управления

В GNOME D-Bus используется для экспозиции интерфейсов различных компонентов. Основные включают:

- org.gnome.SessionManager: Управление сессией, включая logout, shutdown и inhibit (блокировку) screensaver.
- org.gnome.SettingsDaemon: Настройки, такие как клавиатура, мышь, энергопотребление и темы.
- org.gnome.Mutter: Управление окнами (window manager), включая фокус и геометрию.
- org.freedesktop.Notifications: Уведомления.
- org.freedesktop.UPower: Управление питанием.

В Alt Linux эти компоненты доступны через системный или сессионный bus, интегрированные в пакеты gnome-session и gnome-settings-daemon [1].

Для поиска компонентов используйте инструменты introspection. Команда:

gdbus introspect --session --dest org.gnome.SessionManager --object-path /org/gnome/SessionManager

перечисляет методы и свойства интерфейса [4]. Чтобы получить список всех сервисов:

gdbus call --session --dest org.freedesktop.DBus --object-path /org/freedesktop/DBus --method org.freedesktop.DBus.ListNames.

Графический инструмент D-Feet позволяет визуально просматривать шины и интерфейсы. В Alt Linux эти инструменты доступны в пакете gdbus (из glib2) и d-feet.

Для просмотра сообщений используйте

dbus-monitor --session или *--system*,

который отображает трафик в реальном времени [3]. Чтобы вызвать метод:

dbus-send --session --dest=org.gnome.SessionManager --type=method_call --print-reply /org/gnome/SessionManager org.gnome.SessionManager.Logout uint32:1.

Для более удобного вызова применяйте gdbus call. В GNOME файлы интерфейсов хранятся в /usr/share/dbus-1/interfaces/ [2].

Права определяются через конфигурационные файлы D-Bus (/etc/dbus-1/*.conf) и интеграцию с Polkit. Polkit проверяет авторизацию для привилегированных действий, таких как shutdown. Файлы политик Polkit находятся в /usr/share/polkit-1/actions/, например, org.gnome.settings-daemon.plugins.power.policy. Чтобы проверить: используйте

pkcheck --action-id org.freedesktop.upower.hibernate --process $$.

В Alt Linux Polkit интегрирован с D-Bus для GNOME, обеспечивая, что неавторизованные вызовы отклоняются [6]. Для сэндбоксов (Flatpak) права на D-Bus задаются в манифесте, ограничивая доступ к определенным интерфейсам [8].

Заключение

Исследование подтвердило эффективность D-Bus для управления GNOME в ОС Альт, но выявило значительные риски безопасности в стандартной конфигурации сессионной шины.

Гипотезы подтверждены: управление возможно и удобно, но default-политики слабы; кастомные файлы политик эффективно минимизируют риски.

D-Bus позволяет эффективно управлять GNOME в ОС Альт, предоставляя инструменты для автоматизации задач, таких как изменение настроек, управление сессией и уведомлениями. Можно вызывать методы для повседневных операций, например, блокировки экрана или изменения яркости, без root-прав, если Polkit разрешает (для активного пользователя). Однако нельзя выполнять привилегированные действия (например, системный shutdown) без аутентификации, чтобы избежать эскалации привилегий. Работа строится на модели шины: приложения регистрируют сервисы, экспонируют интерфейсы, и общаются через dbus-daemon с проверкой политик.

С точки зрения безопасности, D-Bus работает надежно при правильной настройке, но уязвим к атакам, таким как подмена сообщений или эксплуатация незащищенных интерфейсов (например, в AccountsService). Рекомендуется использовать сэндбоксы, мониторить трафик и обновлять пакеты для устранения известных уязвимостей [7]. В Alt Linux интеграция D-Bus с GNOME усиливает безопасность через российские стандарты (например, Мандатный контроль доступа), но требует осторожности в корпоративных средах.

Рекомендуется обязательная настройка ограничений в корпоративных и многопользовательских deployment. Дальнейшие исследования: анализ системной шины в серверных редакциях Альт, интеграция с Polkit и SELinux/AppArmor для усиления защиты.

Список литературы

1. ALT Linux (дистрибутив Linux) [Электронный ресурс] // Википедия. — URL: https://ru.wikipedia.org/wiki/ALT_Linux_(дистрибутив_Linux) (дата обращения: 21.12.2025).
2. D-Bus Tutorial [Электронный ресурс] // freedesktop.org. — URL: https://dbus.freedesktop.org/doc/dbus-tutorial.html (дата обращения: 21.12.2025).
3. Введение в D-BUS - OpenNET. https://www.opennet.ru/base/sys/dbus_intro.txt.html (дата обращения: 21.12.2025).
4. Тотальный контроль приложений с системой D-Bus - Хакер. https://xakep.ru/2011/02/16/54722 (дата обращения: 21.12.2025).
5. GNOME адаптирован для управления через systemd - OpenNET. https://opennet.ru/51601-gnome (дата обращения: 21.12.2025).
6. Семилетний баг в Polkit, позволяющий получить права root - Linux.org.ru. https://www.linux.org.ru/news/security/16368036/page2 (дата обращения: 21.12.2025).
7. Атакующие могут получить root в Ubuntu, положив службу AccountsService - Anti-Malware.ru. https://www.anti-malware.ru/news/2021-12-14-111332/37737 (дата обращения: 21.12.2025).

8. Опубликована одиннадцатая платформа ALT - OpenNET. https://www.opennet.ru/opennews/art.shtml?num=61282 (дата обращения: 21.12.2025).
9. Документация GNOME по D-Bus интеграции // developer.gnome.org. URL: https://developer.gnome.org/ (дата обращения: 21.12.2025).
10. Запуск центра управления системой в графической среде // Документация Альт Сервер 11.0. URL: https://docs.altlinux.org/ru-RU/alt-server/11.0/html/alt-server/acc-start.html (дата обращения: 21.12.2025).
11. Спецификация D-Bus // freedesktop.org. URL: https://dbus.freedesktop.org/doc/dbus-specification.html (дата обращения: 21.12.2025).
12. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ