УДК 004.056

РАЗРАБОТКА ГРУППОВЫХ ПОЛИТИК АЛЬТ ДОМЕН НА БАЗЕ МЕХАНИЗМА SYSTEMD

Владимир Владимирович Павловский
преподаватель
Роман Романович Романов
студент
rrromanow@bk.ru
РГУ нефти и газа (НИУ) им. И. М. Губкина
Москва, Россия

Аннотация. В статье исследуется гибридный подход к управлению конфигурациями в доменной среде ОС Альт. Предлагается модель, преодолевающая ограничения стандартных групповых политик (GPO) путем их использования в качестве транспорта для доставки декларативных unit-файлов. Принудительное исполнение политик обеспечивается системным менеджером SystemD. Практически реализована и протестирована модель проактивной защиты, включающая службу-аудитор и механизм самовосстановления критически важных сервисов. Доказано, что синергия GPO и SystemD создает более надёжный и устойчивый контур безопасности.

Ключевые слова: Альт Домен, SystemD, групповые политики, GPO, централизованное управление, информационная безопасность, Linux, SambaDC, unit-файл, проактивная защита.

В условиях активного импортозамещения и построения суверенных IT-инфраструктур отечественные операционные системы, такие как ОС Альт, становятся основой для многих организаций. Ключевой задачей при этом является обеспечение эффективного и безопасного централизованного управления конфигурациями. Традиционным отраслевым стандартом для решения этой задачи в средах Microsoft является механизм групповых политик (GPO) Active Directory [3].

Отечественное решение Альт Домен, построенное на базе проекта с открытым кодом SambaDC, предоставляет схожий функционал, эмулируя подход Microsoft [7]. Однако стандартные средства зачастую выполняют роль императивного исполнителя сценариев. Такой подход имеет ограничения в контексте управления современными Linux-системами, где ключевую роль играет система инициализации SystemD [5]. Стандартные политики не способны гарантировать постоянное соблюдение требуемого состояния системных служб, оставляя возможность их несанкционированного изменения локальным администратором между циклами применения GPO.

Эта уязвимость формирует актуальность данной работы. Целью исследования стала разработка и практический анализ альтернативной модели управления, в которой групповые политики Альт Домен используются как транспорт для доставки декларативных конфигураций (unit-файлов), а их принудительное исполнение обеспечивается непосредственно системой инициализации SystemD. Такой подход переносит логику управления с периодически исполняемых скриптов на постоянно действующий механизм самой операционной системы, что позволяет создать более надёжный и устойчивый контур безопасности.

Для понимания предложенной модели необходимо рассмотреть три ключевые технологии: механизм GPO, архитектуру Альт Домен и систему инициализации SystemD.

Классическая модель работы GPO в Active Directory представляет собой декларативный подход. Администратор определяет желаемое состояние («что должно быть») в объекте групповой политики, а клиентская машина самостоятельно приводит себя в соответствие с этим состоянием.

Альт Домен является полнофункциональным контроллером домена на основе SambaDC, который технологически заменяет Microsoft Active Directory. Его архитектура включает службу каталогов на базе LDB, протокол аутентификации Kerberos и DNS-сервер. Для хранения файлов групповых политик используется сетевой каталог SYSVOL. Взаимодействие этих компонентов формирует стандартный механизм применения GPO в Альт Домен.

В свою очередь, SystemD является основным инструментом для управления службами и процессами в современных дистрибутивах GNU/Linux [8], включая ОС Альт. Его ключевое преимущество — декларативная модель управления. Администратор не описывает последовательность команд, а задаёт конечное желаемое состояние в специальных конфигурационных файлах — юнитах (units). Основными типами юнитов, используемыми в данной работе, являются «.service» (описывает, как управлять службой), «.path» (активирует службу при изменении файла или каталога) и drop-in файлы (дополняющие конфигурацию основного юнита). Общая схема работы Альт Домен и SystemD представлена на рисунке 1.

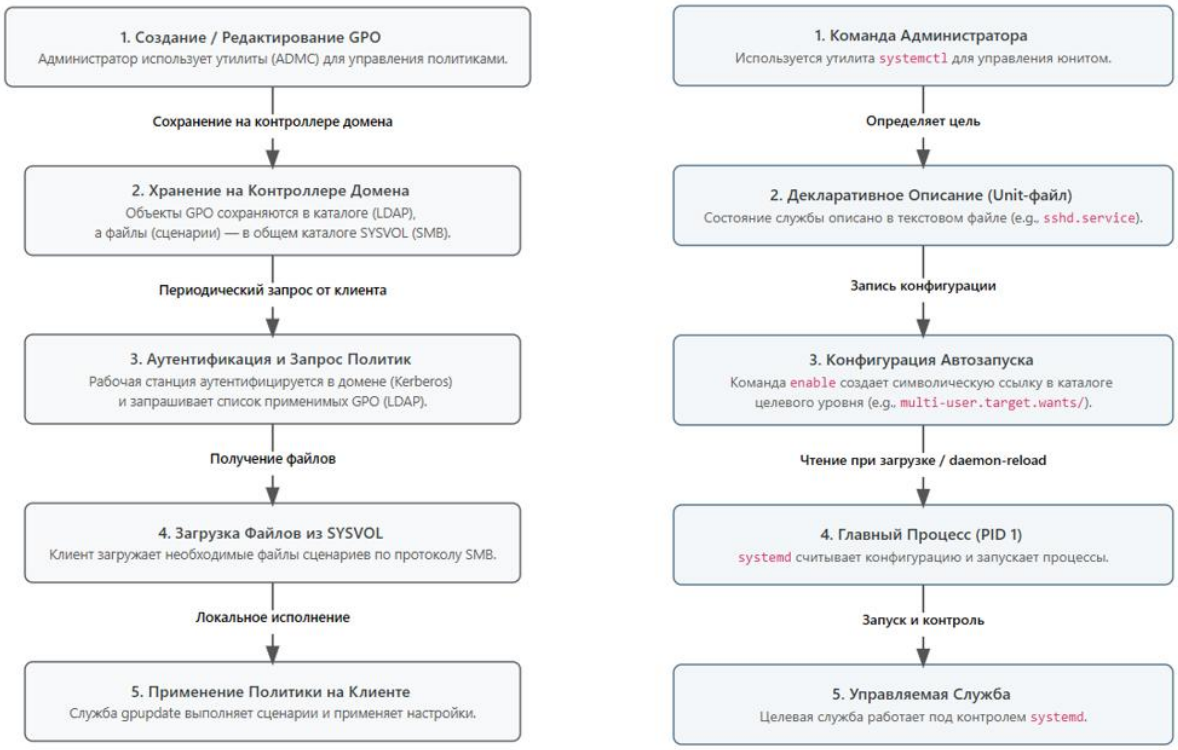

Рисунок 1 - Принцип работы GPO в Альт Домен и механизма SystemD по управлению службами

Ключевая проблема стандартного подхода заключается в том, что GPO в Альт Домен управляет Linux-клиентами через императивные сценарии, которые выполняются периодически службой «gpupdate». Это не позволяет обеспечить постоянный и неоспоримый контроль над состоянием служб, управляемых SystemD, создавая «окно уязвимости» между циклами обновления политик.

В практической реализации будет использоваться модель, где групповые политики – это транспорт для unit-файлов SystemD. Для этого был развёрнут виртуальный тестовый стенд (конфигурация которого представлена в таблице 1), имитирующий фрагмент корпоративной IT-инфраструктуры.

Стенд состоял из двух виртуальных машин: контроллера домена «dc1.corp.local» под управлением Альт Сервер 10.4 и клиентской рабочей станции «ws1.corp.local» под управлением Альт Рабочая станция 10.4. На контроллере домена с помощью утилиты «samba-tool» был развернут домен «corp.local», после чего рабочая станция была введена в домен [4].

Таблица 1

Конфигурация тестового стенда

Параметр	Контроллер домена	Клиентская рабочая станция
Роль	Сервер, контроллер домена Альт Домен	Клиент домена, управляемый хост
Имя хоста	dc1.corp.local	ws1.corp.local
Операционная система	Альт Сервер 10.4	Альт Рабочая станция 10.4
IP-адрес (статический)	192.168.56.10/24	192.168.56.100/24
DNS-сервер	127.0.0.1	192.168.56.10
Ключевое ПО (используемое на стендах)	samba (4.19.9-alt5), krb5-kinit (1.19.4-alt4), gpui (0.2.55-alt1), admc (0.18.0-alt1)	Служба gpupdate (0.12.2-alt1), alterator-auth (0.45-alt1)

Ключевым этапом исследования стала реализация модели, в которой GPO используется как транспорт для доставки нативных unit-файлов SystemD. Было разработано два сценария для демонстрации возможностей этого подхода.

Был создан проактивный механизм защиты, предназначенный для автоматического обнаружения и удаления неавторизованных системных служб на примере каталога «/etc/systemd/system». Модель состоит из трех компонентов, содержимое которых представлено на рисунке 2. Первый - сценарий аудита «unit-audit.sh», это исполняемый скрипт, который сверяет все unit-файлы в системном каталоге «/etc/systemd/system» с «белым списком» разрешенных служб. Любой юнит, не входящий в список, считается неавторизованным, отключается и удаляется, а событие регистрируется в лог-файле. Второй - сервисный юнит «unit-audit.service» - декларативный файл, описывающий, как запустить сценарий аудита. И, наконец, третий компонент - path-юнит «unit-audit.path», активирующий «unit-audit.service» каждый раз, когда в каталоге «/etc/systemd/system/» происходят изменения.

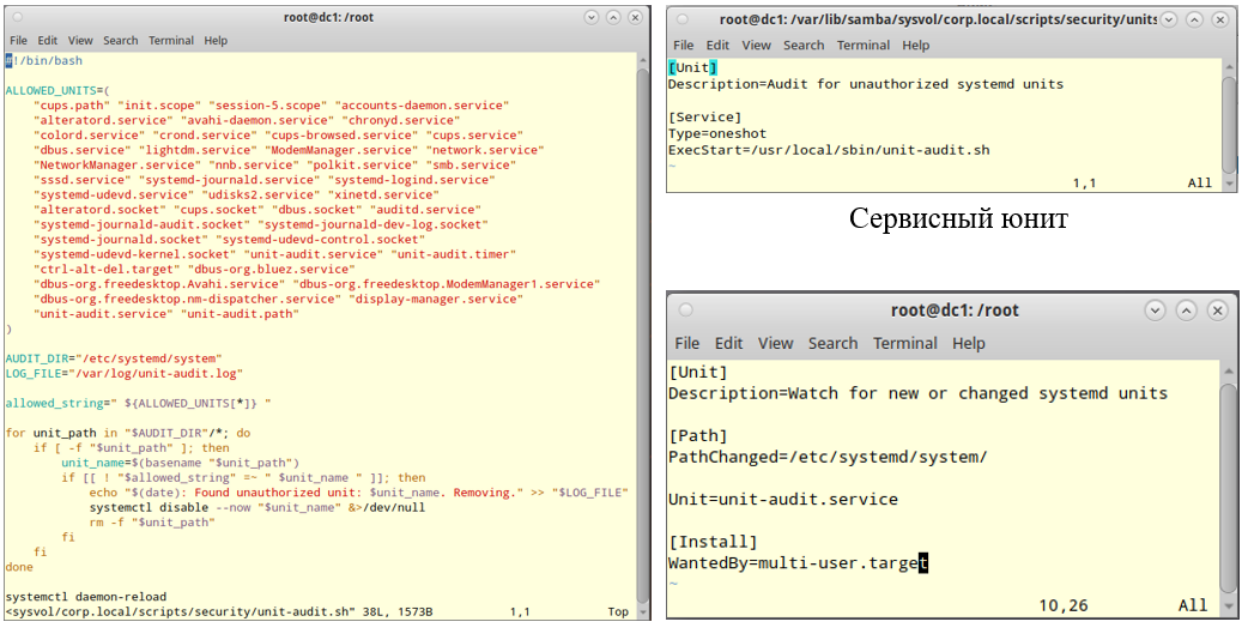

Рисунок 2 - Компоненты службы-аудитора

Второй же сценарий демонстрирует принудительное обеспечение работы компонента. В качестве примера была выбрана служба системного аудита auditd. Для этого был использован гибкий механизм SystemD — drop-in файл. Создан файл «/etc/systemd/system/auditd.service.d/override.conf» (рисунок 3), который переопределяет параметры запуска службы «auditd», добавляя директивы «Restart=always» и «RestartSec=2». Эти параметры заставляют SystemD автоматически перезапускать службу через 2 секунды в случае ее остановки, включая принудительное завершение через «kill -9».

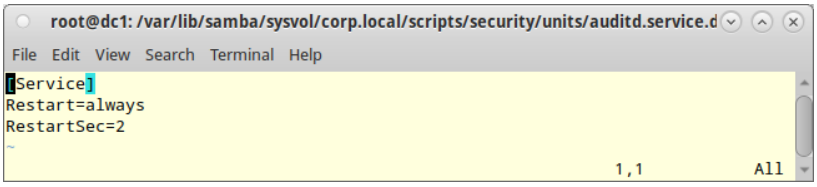

Рисунок 3 - Содержимое drop-in файла

После подготовки unit-файлов на контроллере домена был настроен механизм их централизованной доставки и активации. С помощью утилиты ADMC была создана групповая политика «Proactive Security Policy», привязанная к подразделению (OU) с рабочими станциями.

Настройка GPO проходила в два этапа. Сначала, в редакторе GPO (gpui) по пути «Machine → Preferences → System Settings → Files» были созданы правила, которые копируют четыре подготовленных файла (скрипт, два юнита и drop-in файл) из общего ресурса SYSVOL в их целевые каталоги на клиентской машине. Для каждого правила было выбрано действие «Replace», чтобы гарантировать обновление файлов на клиентах при их изменении на сервере.

Второй этап - активация службы. По пути «Machine → Preferences → System Settings → Scripts → Startup» был настроен сценарий запуска (рисунок 4). Он последовательно выполняет две команды: «systemctl daemon-reload», чтобы SystemD перечитал конфигурацию и «увидел» новые юниты, и «systemctl enable --now unit-audit.path», чтобы включить и немедленно запустить path-юнит аудитора.

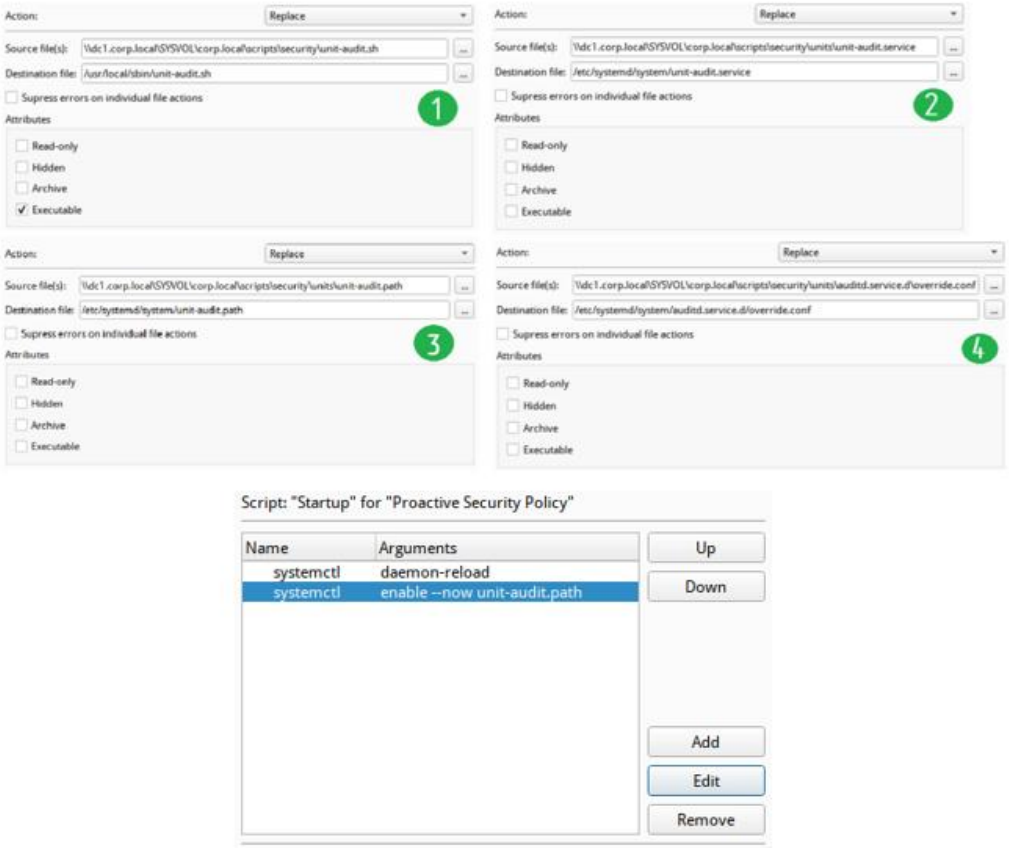

Рисунок 4 - Настройка GPO

После развертывания политик было проведено тестирование для проверки их эффективности. Сначала - попытка изменения защищённого каталога. На клиентской машине была совершена попытка создать точку постоянного

присутствия путём размещения собственного unit-файла «malware.service» в системном каталоге. Сразу после создания файла сработал «unit-audit.path», запустил службу «unit-audit.service», которая в свою очередь запустила сценарий для проверки каталога, описанный ранее. Сценарий обнаружил неавторизованный юнит и немедленно его удалил (рисунок 5).

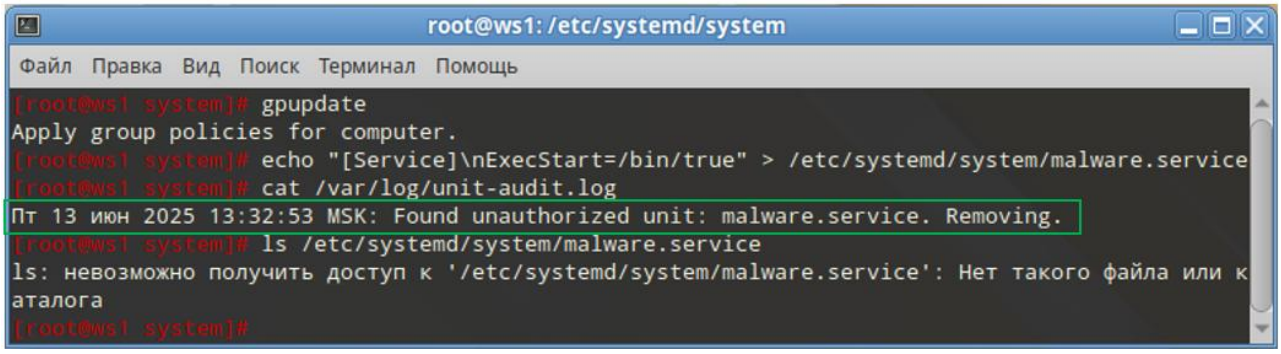

Рисунок 5 - Тестирование удаления посторонних служб

Далее был сделан второй тест - проверка механизма самовосстановления службы. Была предпринята попытка вручную остановить службу «auditd». Процесс был завершён принудительно командой «kill -9». Благодаря доставленному через GPO drop-in файлу, SystemD немедленно перезапустил службу «auditd», восстановив ее работоспособность в течение 2 секунд (рисунок 6).

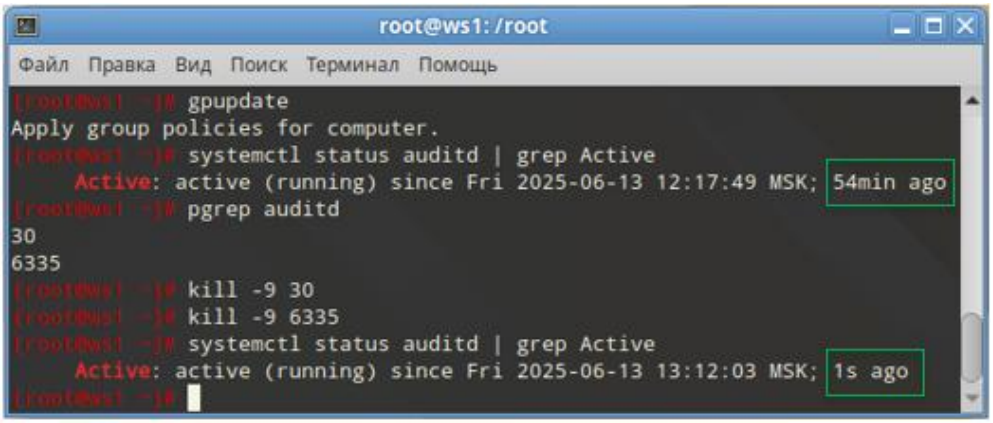

Рисунок 6 - Демонстрация немедленного запуска службы

Проведённые эксперименты позволили свести результаты в итоговую таблицу 2.

Таблица 2

Сводные результаты тестирования

№	Проведённый тест	Наблюдаемый результат	Вывод об эффективности
1	Попытка изменения содержимого защищённого каталога	Служба-аудитор, доставленная через GPO, успешно обнаружила и удалила неразрешённый unit-файл.	Модель позволяет создавать и централизованно развертывать проактивные механизмы безопасности, работающие на уровне подсистемы инициализации.
2	Попытка ручной остановки службы	Прямое "убийство" процесса (kill -9) привело к его немедленному автоматическому перезапуску.	Доставленный drop-in файл успешно успешно предотвратил остановку службы, что позволило сохранить стабильность и непрерывность работы системы.

В ходе выполнения работы была исследована и практически реализована модель централизованного управления конфигурациями в доменной инфраструктуре на базе ОС Альт. Проведённый анализ показал, что стандартные подходы к применению GPO, основанные на императивных сценариях, не обеспечивают постоянный контроль над низкоуровневыми компонентами Linux.

Целесообразность использования модели, где GPO выступает в роли транспорта для доставки декларативных unit-файлов SystemD, была полностью подтверждена. Практическая реализация и тестирование модели доказали её высокую эффективность, надёжность и устойчивость к попыткам несанкционированного изменения конфигурации.

Таким образом, было доказано, что синергия штатных инструментов доставки GPO в Альт Домен и декларативной мощи системы инициализации SystemD является высокоэффективным решением для построения эшелонированной и самовосстанавливающейся системы безопасности. Предложенная модель позволяет повысить уровень контроля и управляемости рабочих станций в доменной сети на базе ОС Альт. Результаты данной работы могут служить методическим материалом для системных администраторов при построении защищённых IT-инфраструктур на базе отечественных операционных систем.

Список литературы:

1. Уймин А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 /3-е изд., стер. СПб.: Лань, 2022. 480 с. ISBN 978-5-8114-9255-8.

2. Alt Linux Wiki – URL: https://www.altlinux.org/Главная_страница

3. Microsoft Learn – URL: https://learn.microsoft.com

4. Руководство по ALT домену. Версия 1.1 // ООО «Базальт СПО». Москва: Базальт СПО, 2023. – URL: https://www.basealt.ru/fileadmin/user_upload/manual/ALT_Domain_guide.pdf

5. System and Service Manager (systemd). – https://systemd.io/ (Дата обращения: 07.06.2025).

6. Николаев А. М., Савицкий Д. Д. Анализ и сравнение популярных гипервизоров // Молодой ученый. 2023. № 24 (471). С. 23–26. ISSN: 2072–0297; eISSN: 2077–8295.

7. The Official Samba HOWTO and Reference Guide. Version 4.18 // The Samba Team. – [S.l.]: The Samba Team, 2023. – URL: https://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf

8. Кофлер М. Linux. Установка, настройка, администрирование // Пер. с нем. 4-е изд., перераб. и доп. Санкт-Петербург: БХВ-Петербург, 2016. 976 с.

9. Nemeth, Evi, Garth Snyder, Trent R. Hein, Ben Whaley, and Dan Mackin. UNIX and Linux System Administration Handbook. 5th ed., Pearson Education, Inc., 2018. (ISBN-13: 978-0134277554)

UDC 004.056

DEVELOPING ALT DOMAIN GROUP POLICIES BASED ON THE SYSTEMD MECHANISM

Vladimir V. Pavlovskij
lecturer
Roman R. Romanov
student
rrromanow@bk.ru
Gubkin Russian State University of Oil and Gas
Moscow, Russia

Abstract. This article explores a hybrid approach to configuration management within the Alt OS domain environment. It proposes a model that overcomes the limitations of standard Group Policy Objects (GPO) by using them as a transport mechanism for delivering declarative unit-files. The enforcement of these policies is handled by the SystemD system manager. A proactive security model, including an auditor service and a self-healing mechanism for critical services, was implemented and tested. The results prove that the synergy of GPO and SystemD creates a more reliable and resilient security perimeter.

Keywords: Alt Domain, SystemD, Group Policy, GPO, centralized management, information security, Linux, SambaDC, unit-file, proactive security.

Статья поступила в редакцию 10.05.2025; одобрена после рецензирования 20.06.2025; принята к публикации 30.06.2025.

The article was submitted 10.05.2025; approved after reviewing 20.06.2025; accepted for publication 30.06.2025.