***Д. А. Искаков, А. М. Шабалин***
*Тюменский государственный университет, г. Тюмень*
**УДК 004.732, 004.722**

# РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СЛУЖБЫ КАТАЛОГОВ ALD PRO ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ С ФАЙЛОВЫМИ СИСТЕМАМИ

**Аннотация.** В работе были выявлены особенности использования отечественного программного обеспечения ALD Pro для управления доменной сетью на примере реальных случаев внедрения данного программного обеспечения, что позволило определить актуальные запросы пользователей. Кроме того был проанализирован продукт Microsoft Windows Server на предмет реализации мер защиты компьютерной сети, в результате чего были разработаны скрипты групповых политик и методология их применения.

**Ключевые слова:** домен, групповые политики, безопасность, автоматизация, Astra Linux, ALD Pro.

**Введение.** Обеспечение безопасности инфраструктуры — это неотъемлемая часть работы каждой организации. В последнее время (по причине ухода зарубежных вендоров с российского рынка) встал вопрос замещения программного обеспечения отечественными аналогами [1]. Соответственно, по этой причине многие организации занимаются миграцией своих систем на отечественное программное обеспечение [2, 3]. Многие российские разработчики предложили конкурентоспособные продукты, способные предоставить тот функционал, которого лишились предприятия.

Так, популярный программный продукт Windows Server, разработанный для управления доменом Active Directory уже можно заменить некоторыми отечественными продуктами, один из которых предложен группой компаний «Астра», ALD Pro [4]. Однако на данный момент, администраторы доменов на основе ALD Pro сталкиваются с проблемой нехватки штатных групповых политик, направленных на обеспечение безопасности инфраструктуры. Данный факт подтверждают пользователи в различных сообществах по технической поддержке продукта, в том числе администратор единого портала поддержки [5]. Это влечет за собой несоответствие требованиям регуляторов. Например, отсутствуют некоторые политики по обеспечению безопасности файловой системы, что приведет к реализации ряда угроз информационной безопасности [6].

Выбор в пользу ALD Pro был сделан нами после проведения анализа похожих открытых решений, которые в перспективе могли бы стать аналогом AD (см. табл. 1). Каждое из них выполняет требуемый функционал для обеспечения управления доменом. Все они предоставляют возможность управлять пользователями, подавляющее большинство продуктов поддерживает управление групповыми политиками и доверительные отношения с другими операционными системами. Однако решающим фактором выбора послужило наличие автоматизации процессов, что значительно упрощает работу администрирования.

**Проблема исследования.** В ходе исследования нами ставились следующие задачи:

1. Проанализировать случаи внедрения ALD Pro и определить актуальные запросы по разработке скриптов групповых политик;
2. Изучить методологию разработки скриптов для Unix-подобных систем;

3. Настроить модель сети предприятия в виртуальной среде для проведения тестов;
4. Разработать скрипты групповых политик;
5. Провести апробацию разработанных скриптов.

*Таблица 1*

**Сравнение программного обеспечения для управления службой каталога**

| *Критерий* | *ALD Pro* | *Samba DC* | *FreeIPA* | *OpenLDAP* |
|---|---|---|---|---|
| Наличие групповых политик | + | + | + | - |
| Управление пользователями | + | + | + | + |
| Автоматизация процессов | + | - | - | - |
| Миграция с Windows | + | + | + | - |

**Материалы и методы.** Методами данного исследования стали сравнение, анализ, моделирование. Апробация разработанных скриптов проводилась с использованием виртуального стенда в среде эмуляции GNS3.

**Результаты.** ALD Pro — это система для централизованного управления и автоматизации управления доменной сетью. На основании анализа программного продукта, ALD Pro обеспечивает снижение санкционных рисков и требований к квалификации персонала, так как данное решение обладает дружественным интерфейсом и позволяет выполнять задачи в среде Linux без обращения к интерфейсу командной строки. Помимо этого, уменьшается трудоемкость администрирования из-за гибкости настроек системы, автоматизации решения многих задач администратора и присутствия единой точки контроля и отчетности. При разработке ALD Pro использовались открытые программные компоненты, которые были выбраны в соответствии с такими критериями, как опыт масштабируемости, поддержка сообществом разработчиков, безопасность и скорость устранения уязвимостей, а также возможность интеграции в систему [1, 5].

При развертывании домена встает вопрос о мерах защиты инфраструктуры для предотвращения воздействий злоумышленников, то есть нужно использовать определенные политики, процессы и элементы управления для защиты ключевых частей информационной системы от компрометации. Поскольку регуляторы определяют общие требования по безопасности информации, нами были рассмотрен ряд нормативно-правовых актов и федеральных законов РФ.

После анализа методов реализации требований регуляторов в Microsoft Active Directory применительно к реальным кейсам внедрения ALD Pro нами были выбраны следующие меры защиты, которые были реализованы с помощью скриптов:

1. Запрет использования съемных носителей;
2. Разграничение доступа к лояльным и сетевым ресурсам SMB с использованием мандатного управления доступом;
3. Разграничение доступа к локальным и сетевым ресурсам NFS с использованием мандатного контроля целостности;
4. Шифрование дисков.

Данные политики направлены на защиту файловой системы и выбраны нами из-за большого количества уязвимостей, которые могут быть реализованы в качестве угроз компьютерной сети. Представленные групповые политики способны снизить вероятность реализации следующих угроз:

1. Злоумышленники могут получить доступ к диску и внедрить вредоносное программное обеспечение, что может привести к недоступности системы или потере данных [6];

2. Несанкционированный доступ к дискам может привести к нарушению работы системы, если злоумышленники попытаются модифицировать или удалить файлы конфигурации и настройки;

3. Изменение данных, которые хранятся на диске, также может привести к рискам для пользователей, владельцев и операторов информационной системы; на носителях могут храниться критически важные данные, определяющие бизнес-процессы организации;

4. Нарушитель может заблокировать доступ к диску, перегружая его запросами или намеренно создавая сбои в работе, что приводит к недоступности данных для пользователей информационной системы или нарушению нормального функционирования [6].

Скрипты групповых политик разрабатывались с использованием языка программирования Python и системы управления конфигурациями и удаленного выполнения операций SaltStack. Для внедрения параметров в систему ALD Pro можно воспользоваться одним bash-скриптом, содержащим в себе обращение к коду каждого отдельного параметра групповой политики. После вызова утилиты policy.py происходит импорт групповой политики, которую можно использовать. Для импорта утилита обращается к программно-аппаратной части ALD Pro с использованием REST API.

В качестве примера групповой политики мы взяли запрещение использования съемных носителей. В Astra Linux можно использовать утилиту udev, создать правило, которое блокирует доступ к USB-устройствам, определяемым как съемные носители. Однако наличие такого параметра в разделе групповых политик сделает процесс запрета таких устройств легче. Администраторам не нужно будет настраивать подобные правила для каждого пользователя, что является достаточно ресурсоемким процессом.

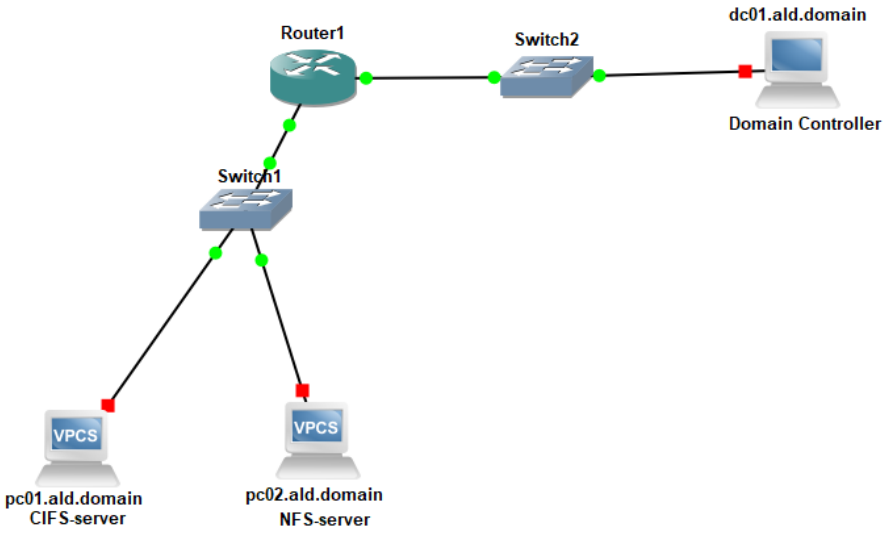


*Рис. 1.* Топология виртуального стенда

Для проведения тестов работоспособности разработанных скриптов использовался виртуальный стенд с развернутым контроллером домена и несколькими, введенными в домен, рабочими станциями (см. рис. 1).

При моделировании стенда использовался программный эмулятор сети GNS3 2.2.46 с подключением к среде виртуализации VMware Workstation Pro. Основные подсистемы, а именно: синхронизация времени, разрешение имен и служба каталогов — были развернуты на контроллере домена dc01.ald.domain (см. рис. 1). Кроме того, в работе использовались такие подсистемы, как CIFS/SMB и NFS, серверами для которых выступили pc01 и pc02 соответственно.

**Заключение.** В результате исследования было проведено сравнение отечественных программных решений для управления службой каталога и разработан набор скриптов, реализующих групповые политики для обеспечения безопасной работы пользователей с файловой системой. Также была смоделирована компьютерная сеть компании в современной среде виртуализации, где работа скриптов прошла успешную апробацию.

**СПИСОК ЛИТЕРАТУРЫ**


1. Ильенко В.О. Обоснование выбора средств развертывания доменной инфраструктуры телекоммуникационной системы на базе отечественного системного и прикладного программного обеспечения / В.О. Ильенко // III научно-педагогические чтения молодых ученых имени профессора С.В. Познышева: сборник материалов Всероссийской научно-практической конференции курсантов и студентов, Воронеж, 19 апреля 2023 года. — Воронеж: ФКОУ ВО Воронежский институт ФСИН России, 2023. — С. 53-55. — EDN LEWLRL. — URL: https://elibrary.ru/download/elibrary_60047288_35011422.pdf.
2. Указ Президента РФ от 30 марта 2022 г. — URL: https://publication.pravo.gov.ru/Document/View/0001202203300001.
3. Зыкин М.М. Отечественные операционные системы / М.М. Зыкин, В.А. Липатов // Российская наука в современном мире: сборник статей XXII международной научно-практической конференции, Москва, 31 мая 2019 года / Научно-издательский центр «Актуальность.РФ». Часть 1. — Москва: Общество с ограниченной ответственностью «Актуальность.РФ», 2019. — С. 128-129. — EDN ZRYLHF. — URL: https://elibrary.ru/download/elibrary_39148547_51798531.pdf.
4. Костин О.И. ALD Pro — для централизованного управления и автоматизации | Astra Linux / О.И. Костин // Математика и математическое моделирование: Сборник материалов XVII Всероссийской молодежной научно-инновационной школы, Саров, 05-07 апреля 2023 года. — Саров: Общество с ограниченной ответственностью «Интерконтакт», 2023. — С. 397-398. — EDN KCUGCN. — URL: https://elibrary.ru/item.asp?id=54187021.
5. Ильенко В.О. Анализ возможности практического применения программного комплекса ALD pro для централизованного управления / В.О. Ильенко, А.С. Кравченко // Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. — Воронеж: Издательско-полиграфический центр «Научная книга», 2022. — С. 90-92. — EDN JHVNLV. — URL: https://www.elibrary.ru/download/elibrary_50055600_11198556.pdf.
6. Добродеев А.Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности / А.Ю. Добродеев // Труды ЦНИИС. Санкт-Петербургский филиал. — 2020. — Т. 2, № 10. — С. 50-78. — EDN NRYSZL. — URL: https://elibrary.ru/download/elibrary_44547904_50419747.pdf.