

УДК 004.056:004.7

**МЕТОДИКА КОНФИГУРАЦИИ КОНТРОЛЛЕРА ДОМЕНА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ЛОКАЛЬНОЙ СЕТИ**

Григорян О.П., Пискунова Е.С.

зр.161401

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

Научный руководитель: Белоусова Е.С. – кандидат технических наук, доцент кафедры ЗИ

Аннотация. В материалах доклада рассматривается конфигурация контроллера домена на основе Active Directory, которое позволяет централизованно управлять пользователями, группами и компьютерами в сети. Реализация данной службы позволяет администраторам эффективно управлять безопасностью в сети, определяя права доступа пользователей к различным ресурсам

Ключевые слова: обеспечение безопасности, Active Directory, контроллеры доменов

Введение. С увеличением числа угроз кибербезопасности и развитием цифровых технологий обеспечение безопасности информации и сетей становится все более критически важным для организаций, поскольку утечка конфиденциальных данных или нарушения в работе сети могут повлечь серьезные последствия. Одним из фундаментальных элементов инфраструктуры сети в среде Windows Server является Active Directory, который обеспечивает централизованное управление и высокий уровень информационной безопасности сети.

Active Directory – это служба каталогов, которая используется для управления ресурсами в локальной сети организации. Другими словами, Active Directory – это центральная база данных, в которой хранится информация о пользователях, группах, компьютерах и других сетевых устройствах. Active Directory предоставляет службы аутентификации и авторизации, позволяя пользователям аутентифицироваться на устройствах и получать доступ к ресурсам в соответствии с их правами. Основными элементами структуры управления сети являются домены,

контроллеры доменов, деревья и леса доменов. Домены – это логические группы объектов, контроллеры доменов хранят информацию и управляют доступом к ресурсам, а деревья и леса доменов представляют собой иерархические структуры, объединяющие связанные домены и деревья в единую систему управления. В рамках сети, использующей Active Directory, серверы DHCP (Dynamic Host Configuration Protocol) и DNS (Domain Name System) играют важную роль в обеспечении бесперебойной работы сети. Сервер DHCP предназначен для автоматического назначения IP-адресов устройствам в сети, что упрощает доступ к сетевым ресурсам, в то время как сервер DNS отвечает за разрешение имен узлов в сети в IP-адреса, обеспечивая правильную адресацию и доступ к ресурсам.

Проведение научной работы по данной теме на практике позволит выявить оптимальные стратегии и методы обеспечения безопасности с использованием Active Directory. Это поможет организациям повысить уровень защиты своих данных и сетевой инфраструктуры, что является крайне актуальным в наше время.

Основная часть. Для реализации службы Active Directory в роли администратора используется виртуальная машина с серверной операционной системой Windows Server, а в роли пользователя – виртуальная машина с операционной системой Windows 10.

Для первоначальной конфигурации контроллера необходимо создать домен и обеспечить связь между администратором и пользователем. Для организации вычислительной сети установлены Active Directory Domain Service (AD DS), DHCP-сервер и DNS-сервер. На рисунке 1 изображена панель мониторинга всех установленных серверов.

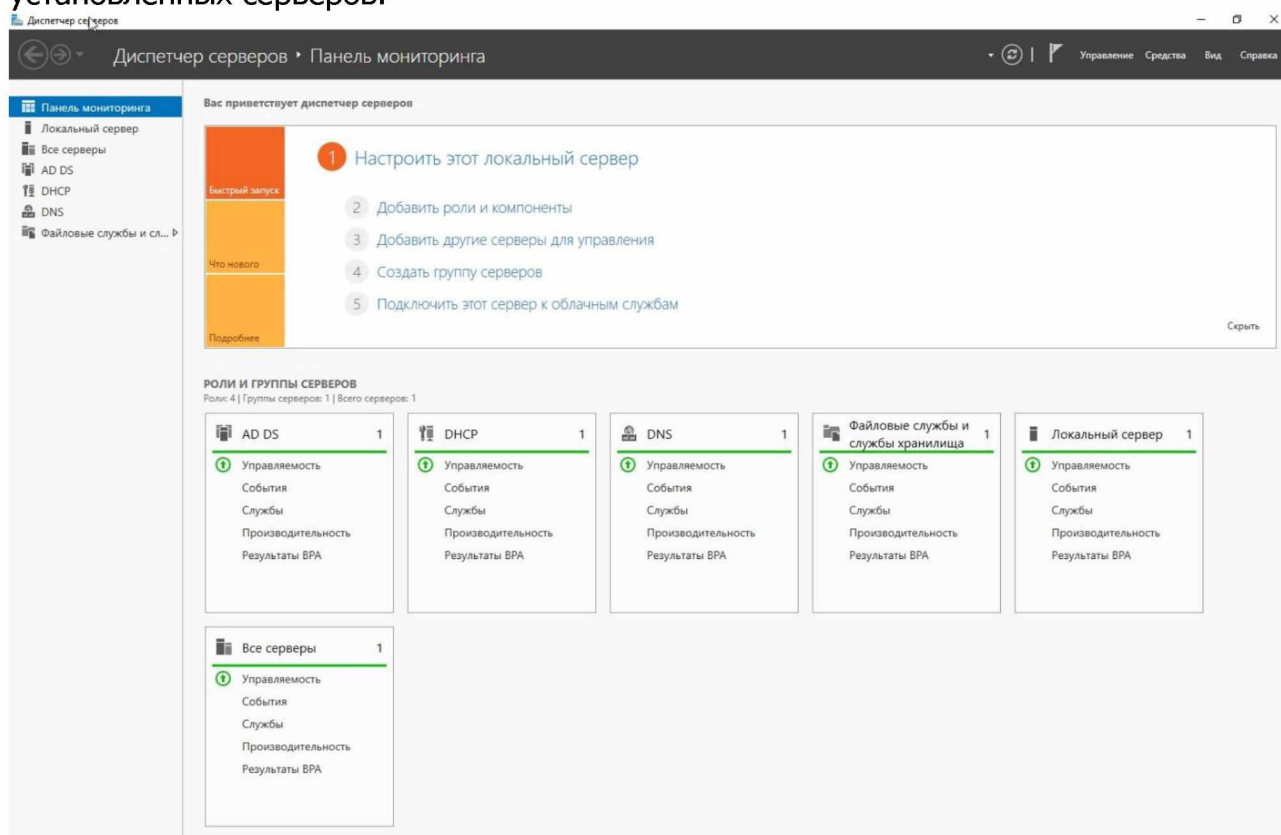


Рисунок 1 – Панель мониторинга установленных серверов

Следующий шаг настройки – добавление пользователей и разграничение их прав. На рисунке 2 представлена начальная страница входа в систему пользователя, где указан уже настроенный домен GP.

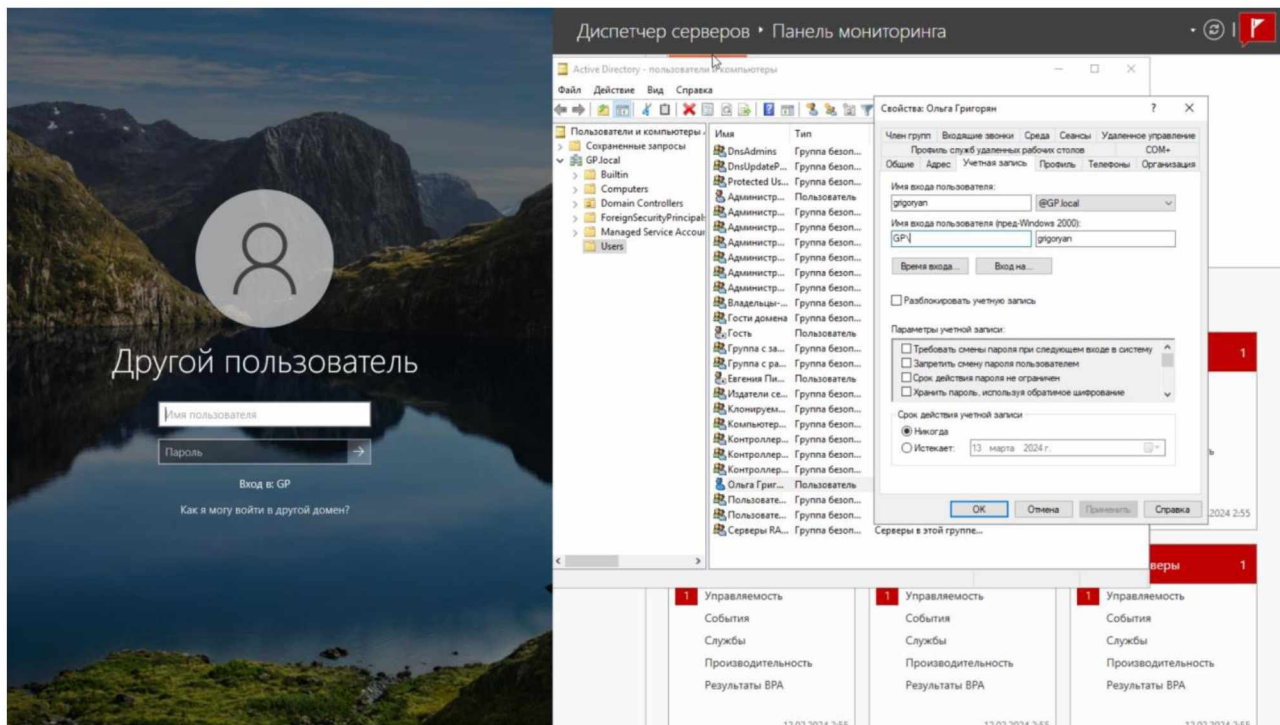


Рисунок 2 – Вход пользователя в домен

Также необходимо настроить раздачу IP-адресов по протоколу DHCP. На рисунке 3 отображен результат работы сервера.

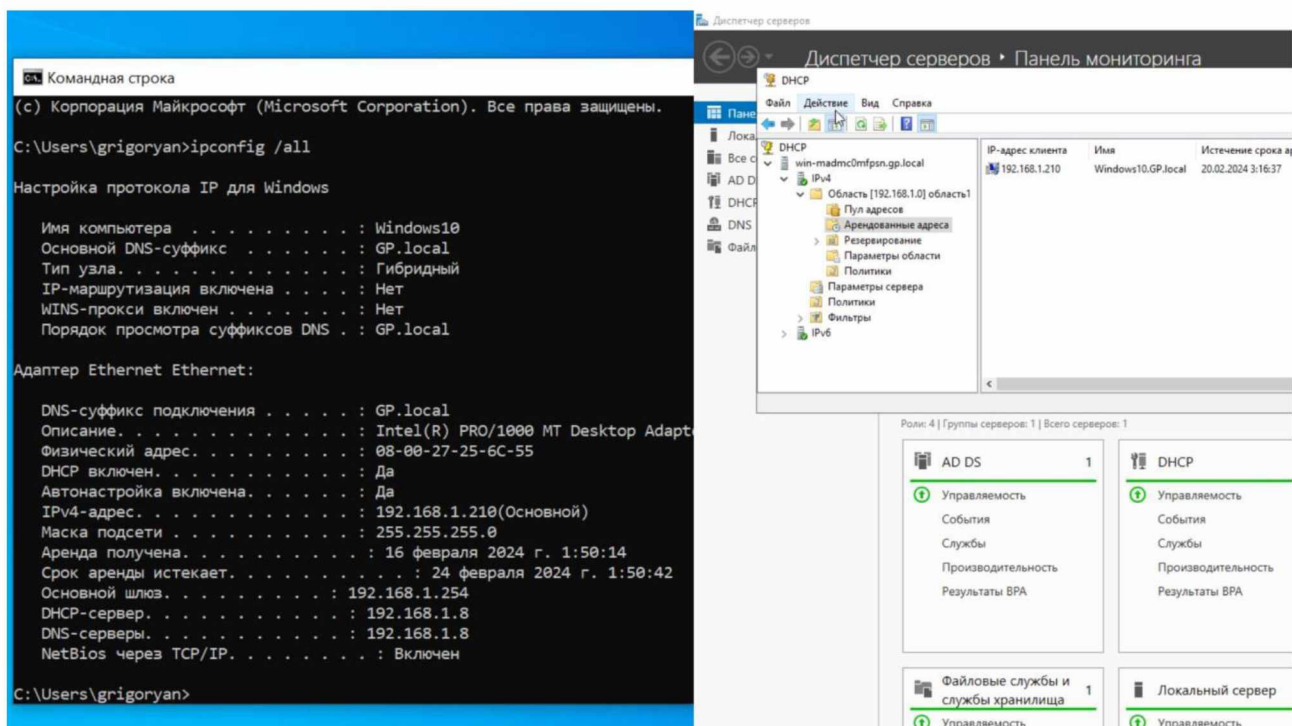


Рисунок 3 – Результат работы DHCP-сервера

Заключение. Применение методики конфигурации позволит повысить уровень безопасности локальной сети и защитить информационные ресурсы организации от угроз и атак. В дальнейшем планируется внедрение различных политик безопасности сети, а также добавление иных операционных систем в домен, что позволит

улучшить управление пользователями и ресурсами сети.

Список литературы

6. Active Directory и LDAP [Электронный ресурс]. – ISPsystem – 2023. – Режим доступа: <https://www.ispsystem.ru/news/active-directory-ldap/>. – Дата доступа: 16.02.2024.

UDC 004.056:004.7

DOMAIN CONTROLLER CONFIGURATION METHODOLOGY FOR SECURING THE LOCAL NETWORK

Grigoryan O.P., Piskunova E.S.

gr.161401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department

Annotation The article discusses the configuration of a domain controller based on Active Directory, which allows centralized management of users, groups and computers in the network. The implementation of this service allows administrators to effectively manage security in the network by defining user access rights to various resources

Keywords: security assurance, Active Directory, domain controllers