Силантьев В.П., Кадыков И.А., Павловский В.В. Вопросы безопасности настройки и функционального тестирование доверительных отношений в инфраструктуре WINDOWS. //Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 12(62) с. 159–169

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056:004.738.6:004.45

ВОПРОСЫ БЕЗОПАСНОСТИ НАСТРОЙКИ И ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЕ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ В ИНФРАСТРУКТУРЕ WINDOWS

[1]Силантьев В.П., Кадыков И.А., Павловский В.В. (научный руководитель)
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: [1]digger_v@mail.ru

В статье рассматриваются вопросы обеспечения безопасности доверительных отношений в инфраструктуре Windows, которые позволяют пользователям одного домена аутентифицироваться в другом домене. Цель исследования заключается в изучении механизмов, которые обеспечивают безопасность и эффективность работы доверительных отношений в инфраструктуре Windows, а также в понимании процессов их настройки и тестирования. Исследование выполнено в условиях тестовой серверной инфраструктуры. Полученные результаты показали, что безопасность без средств защит почти нулевая, в то время как средства безопасности, такие как SID Filtering или Selective Authentication, предоставляют защитный функционал, который предотвращает большой процент атак. Результаты могут быть использованы для создания инструмента непрерывного аудита и тестирования доверительных отношений.

Ключевые слова: Доверительные отношения, Windows, Безопасность, Домен, Леса, Active Directory (AD), PowerShell (PS), Microsoft, Угрозы.

SECURITY ISSUES IN SETTING UP AND FUNCTIONAL TESTING OF TRUST RELATIONSHIPS IN THE WINDOWS INFRASTRUCTURE

[1]Silantyev V.P., Kadykov I.A., Pavlovsky V.V. (supervisor)
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: [1]digger_v@mail.ru

This article examines the security of trust relationships in a Windows infrastructure that allow users from one domain to authenticate to another domain. The objective of the study is to examine the mechanisms that ensure the security and effectiveness of trust relationships in a Windows infrastructure, as well as to understand the processes for configuring and testing them. The study was conducted on a test server infrastructure. The results showed that security without protection is virtually nonexistent, while security features such as SID Filtering or Selective Authentication provide protective functionality that prevents a large percentage of attacks. The results can be used to create a tool for continuous auditing and testing of trust relationships.

Keywords: Trust relationships, Windows, Security, Domain, Forests, Active Directory (AD), PowerShell (PS), Microsoft, Threats.

Введение

Актуальность: доменные службы Active Directory (AD DS) чрезвычайно важны в нынешнее время, ведь они обеспечивают безопасность между несколькими доменами или лесами

с помощью отношений доверия между доменами и лесами. Перед тем как проверка подлинности может произойти через доверительные отношения, Windows должна сначала проверить, имеет ли запрашиваемый домен доверительное отношение с доменом учетной записи, делающей запрос. Поэтому корректная настройка и контроль доверительных отношений становятся критически важными.[1]

Доверие лесов помогает управлять сегментированной инфраструктурой AD DS и поддерживать доступ к ресурсам и другим объектам в нескольких лесах. Доверительные отношения полезны для таких целей, как предоставление услуг для компаний, участвующих в слияниях и приобретениях сети для совместного ведения бизнеса или ищущих решения для административной автономии.

Несмотря на свою критическую важность в работе компаний, эти отношения представляют собой сложный и часто недостаточно защищенный элемент инфраструктуры, что делает их легкой целью для кибератак.

Проблема безопасности доверительных отношений активно начала обсуждаться с начала 2000 х, когда AD стала стандартом корпоративных сетей.

На данный момент доверительные отношений принято разделять на: односторонние и двусторонние доверия.

Одностороннее доверие — это однонаправленный путь аутентификации, созданный между двумя доменами. В случае одностороннего доверия между доменом A и доменом B пользователи в домене A могут получить доступ к ресурсам в домене B, однако пользователи в домене B не могут получить доступ к ресурсам в домене A.

В двустороннем доверии домен A доверяет домену B и домен B доверяет домену A. Эта конфигурация означает, что запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях.

Некоторые двусторонние отношения могут быть не транзитивными или транзитивными в зависимости от типа создаваемого доверия. Транзитивное доверие можно использовать для расширения отношений доверия с другими доменами. Не транзитивное доверие можно использовать для запрета отношений доверия с другими доменами.

В наше время главной популярностью среди атак на доверительные отношения используются: слабости протокола Kerberos и репликацию данных, «Золотой билет» (Golden Ticket), эксплуатация отношения «домен-лес», атака «SID Filtering»[2]

Несмотря на обширную документацию и на постоянные улучшения AD остаются слабо или вовсе не изученными: методики систематического функционального тестирования доверия в сложных топологиях; критерии безопасности для гибридных сценариев (AD + Azure AD); автоматизированные инструменты аудита доверия с учётом актуальных угроз.

Объект исследования: инфраструктура Microsoft Active Directory, в частности многодоменные леса, доверительные отношения.

Предмет исследования: процессы настройки, мониторинга и тестирования доверительных отношений между доменами AD с точки зрения как функциональности, так и безопасности.

Цель исследования: на основе анализа доверительных отношений Windows AD, провести экспериментальное тестирование их функционала и определить эффективность различных сценариев настройки отношений, выявить их преимущества и недостатки, а также разработать рекомендации по оптимальной конфигурации системы в корпоративной среде.

Литературный обзор

Проблема безопасности доверительных отношений в Active Directory находится на стыке официальных рекомендаций вендора, практических наработок наступающих команд и стратегических концепций защиты. Анализ существующих работ показывает, что внимание уделяется как глубоким техническим аспектам протоколов (как в документации Microsoft TechNet) или инструментам для эксплуатации уязвимостей (как в работах сообщества Red Team), так и изучению атак как со стороны злоумышленников, так и со стороны жертв.

Microsoft Documentation - официальная документация предоставляет исчерпывающую информацию о типах доверительных отношений, синтаксисе PowerShell-команд для их создания и базовых настройках безопасности. Там можно узнать, как работают отношения доверия для лесов в Active Directory, Однако она носит описательный характер и не предлагает готовых методик для комплексного подхода к безопасности. [3]

Исследования разработчиков со всего мира, в частности из России, которые имитируют действия злоумышленников для оценки защищённости организации. Например, такие инструменты, как BloodHound, произвели революцию, показав, как атакующие видят AD, в частности они детально рассматривают атаки, к примеру, атака Pass-the-Ticket (T1550). Pass-the-Ticket — это атака, в которой злоумышленник использует ранее полученный билет Kerberos, который называется Ticket Granting Ticket (TGT). TGT билет является важнейшим компонентом протокола Kerberos, поскольку он позволяет пользователю проходить аутентификацию в некоторых системах без необходимости каждый раз вводить пароль.

Ticket Granting Ticket (TGT) — это тип билета, выдаваемого контроллером домена пользователю после успешной аутентификации в домене. Он включает в себя важную информацию, такую как сеансовый ключ пользователя, членство в группе и привилегии. Kerberos шифрует TGT с использованием хэша пароля пользователя и применяет алгоритмы симметричного шифрования (например, DES или AES) в зависимости от конфигурации среды Kerberos. После шифрования TGT отправляется на компьютер пользователя и сохраняется в памяти. [4] Понятно и подробно об атаке на Kerberos писали ребята из российской компании R-Vision. Имея украденный ключ TGT, злоумышленник может запросить Ticket-Granting Service (TGS) у контроллера домена для конкретной службы в целевоей системе, чтобы получить доступ к ней.

Атаки Pass-the-Ticket могут осуществляться с использованием различных общедоступных инструментов, таких как Mimikatz, Kekeo, Rubeus, Creddump7. Злоумышленники часто используют эти инструменты для извлечения TGT Kerberos из памяти скомпрометированной системы, а затем используют TGT тикет для получения доступа к другим системам в сети.

Также вплотную рассматривается атака атака Golden Ticket. При успешной атаке несанкционированный доступ к ресурсам и конфиденциальной информации достигается за счет использования сервисной учетная запись KRBTGT – ключевая учетная запись в Kerberos для шифрования и подписи всех билетов в домене. Первоначально злоумышленник взламывает

какую-то систему в домене, затем повышает свои привилегии до уровня администратора домена, чтобы извлечь NTHash, принадлежащий KRBTGT аккаунту и найти Security Identifier (SID). С их помощью злоумышленник создает «Золотой билет» — поддельный билет Kerberos. Этот поддельный билет ведет себя как легитимный. Ticket Granting Ticket (TGT) с индивидуальными привилегиями пользователя, часто имитирующими администратора домена. Эта атака является очень мощной, поскольку она может предоставить злоумышленникам постоянный и широкий доступ к сети в обход регулярных проверок аутентификации. [5] Устойчивость атаки обусловлена ее основной манипуляцией с системой Kerberos, которая остается эффективной даже при изменении пароля krbtgt. Чтобы полностью свести на нет продолжающуюся атаку Golden Ticket, пароль krbtgt необходимо изменить дважды.

На основе проведенного анализа можно сформулировать следующие гипотезы исследования:

Гипотеза 1: стандартные методы оценки безопасности доверительных отношений не позволяют продуктивно оценить реальный риск, так как не учитывают эксплуатационную контекст. Разработанная методика функционального тестирования должно выявлять значительное расхождение между теоретически возможными и практически реализуемыми атаками через доверительные отношения.

Гипотеза 2: использование специализированных скриптов и инструментов для регулярного функционального тестирования доверительных отношений позволяет выявлять больше аномалий и потенциальных векторов атаки по сравнению с разовым аудитом на основе документации. Это позволит интегрировать безопасность в процесс управления инфраструктурой и существенно сократить «время жизни» опасных конфигураций с момента их появления до момента обнаружения.[6]

Гипотеза 3: внедрение протоколов аутентификации, ограничивающих делегирование (таких как RBCD), и их последующее тестирование статистически значимо снижает риск успешных атак на перемещение между доменами и службами.

Метод исследования

1. Тип исследования

Тип исследования: данное исследование является экспериментальным. Оно направлено на установление связей между применением различных механизмов защиты доверительных отношений в Active Directory и двумя группами зависимых переменных:

- Уровнем безопасности (устойчивостью к компрометации и движению вбок)
- Сложностью эксплуатации уязвимостей для атакующего.

Исследование проводится в контролируемых условиях лабораторного стенда, что позволяет изолировать влияние побочных факторов, характерных для производственных сред.

2. Характеристика выборки

Для проведения исследований в качестве среды выбрана доменная служба Active Directory под управлением Windows Server 2025, что обусловлено ее доминирующим положением в корпоративных инфраструктурах. Доверительные отношения, являясь ключевым механизмом взаимодействия между доменами и лесами, были исследованы в наиболее распространенных конфигурациях, что определяет практическую значимость работы.

Для проведения экспериментальных исследований был развернут виртуальный лабораторный стенд, представляющий собой модель сегмента корпоративной сети с распределенной доменной структурой. Выборку исследования составили три независимые доменные среды.

- Лес А: включает родительский домен (forest-a.com) и дочерний домен (child.forest-a.com), связанные двусторонним транзитивным доверием.
- Лес Б: изолированный лес с доменом (forest-b.com).
- Домен С: изолированный домен (domain-c.local).

Характеристики виртуальных машин: 2 виртуальных CPU (x86_64), 4 ГБ оперативной памяти, 100 ГБ дискового пространства. На всех контроллерах домена была установлена операционная система Windows Server 2025. Оборудование размещено в изолированном сегменте сети, что обеспечивало контроль сетевого трафика и исключало влияние внешних факторов.

Для эмуляции различных сценариев доступа между доменами последовательно настраивались следующие типы доверительных отношений:

Сценарий 1: Одностороннее входящее доверие от domain-c.local к forest-a.com.

Сценарий 2: Двустороннее транзитивное доверие между лесами forest-a.com и forest-b.com.

Сценарий 3: Одностороннее нетранзитивное доверие (Selective Authentication) между child.forest-a.com и forest-b.com. [7]

3. Методы сбора данных

Сбор экспериментальных данных осуществляется с применением комплексного инструментария, включающего методы пассивного аудита, активного тестирования на проникновение и мониторинга системных событий.

Для оценки безопасности и эксплуатационного потенциала отслеживаются следующие метрики:

- Фиксируются все возможные маршруты от стандартного пользователя в одном домене к привилегированным группам в другом домене.
- Фиксируется факт успешного получения доступа к целевому домену/ресурсу.
- Фиксируются события в журналах безопасности (Event ID) и срабатывания EDR/AV при проведении атак.
- Замеряется время от начала атаки до достижения конечной цели.

Инструментарий тестирования включает:

- Использование инструментов BloodHound и PingCastle для построения графа атак и выявления потенциально уязвимых конфигураций доверительных отношений.
- Реализация атакующих методик с использованием фреймворка Impacket, Mimikatz и PowerView для проверки прав доступа.
- Мониторинг состояния доверительных отношений и прав доступа с использованием встроенных утилит: nltest, Get-ADTrust (PowerShell), а также просмотр журналов безопасности Windows для анализа событий аутентификации.

4. Описание процедуры проведения исследования

Процедура исследования представляет собой серию последовательных экспериментов для каждого тестируемого сценария доверительных отношений.

Этап 1: базовая настройка стенда

- Развертывание виртуальных машин с контроллерами домена для Леса А, Леса Б и Домена С.
- Настройка базовой сетевой связности и разрешение имен (DNS).
- Создание тестовых пользователей и групп в каждом домене.
- Проверка базовой изоляции доменов.

Этап 2: последовательное применение и тестирование механизмов защиты

- Конфигурация А: доверительное отношение без дополнительных механизмов защиты (базовые настройки).
- Конфигурация В: доверительное отношение с включенным и настроенным SID Filtering.
- Конфигурация С: доверительное отношение с активированной опцией Selective Authentication.

Для каждой конфигурации выполняются следующие шаги:

1) Замер исходного состояния: запуск BloodHound и сбор данных для фиксации всех потенциальных путей атаки в «чистой» конфигурации.

Проведение атаки: последовательная реализация сценариев кибератаки для проверки возможности движения вбок и эскалации привилегий.

Сбор данных: фиксация факта успешности или неуспешности проведенной атаки, документирование полученного уровня доступа и сбор соответствующих событий из журналов безопасности.

Анализ последствий: детальное исследование изменений в группах доступа, билетах Kerberos и таблицах маршрутизации аутентификации для оценки глубины компрометации и эффективности работы механизмов защиты.

5. Методы обработки данных

Для обработки и анализа полученных экспериментальных данных применяется комплекс методов, обеспечивающих всестороннее исследование эффективности механизмов защиты доверительных отношений:

Сравнительный анализ: позволяет сопоставить показатели успешности атак и сложности эксплуатации между различными конфигурациями защиты (А, В, С), выявляя закономерности влияния механизмов безопасности на устойчивость инфраструктуры.

Качественный анализ: включает детальное исследование журналов событий и выводов инструментов аудита для выявления причин успеха/неудачи атаки, а также для понимания внутренних процессов аутентификации и авторизации через доверительные отношения.

Визуализация данных: реализуется через представление результатов в виде сравнительных таблиц и диаграмм, которые наглядно отображают зависимость ключевых параметров (успешность атаки, время на компрометацию, уровень срабатываний мониторинга) от применяемого механизма защиты, что способствует однозначной интерпретации экспериментальных данных и формулированию выводов.

Результаты исследования

Эксперимент проводился в условиях тестовой серверной инфраструктуры. Все виртуальные машины были развёрнуты на одном гипервизоре и использовали одинаковую конфигурацию: 2 виртуальных ядра, 4 ГБ ОЗУ и 100 ГБ дискового пространства на одном типе виртуального хранилища. Это позволило исключить влияние аппаратных факторов и гарантировать сопоставимость результатов.

Для обеих конфигураций выполнялось по 10 последовательных атак. Контроль производительности и состояния системы осуществлялся с использованием BloodHound, Resource Monitor, Event Viewer и набора PowerShell-скриптов для фиксации временных меток, сбора логов и анализа целостности данных.

Исследование проводилось в соответствии с процедурой, описанной в пункте 1.4.

Результат для Конфигурации А (базовое доверие без дополнительных механизмов защиты)

Характеристики: двустороннее транзитивное доверие между forest-a.com и forest-b.com с настройками по умолчанию. SID Filtering отключен, аутентификация разрешена для всех пользователей доверенного домена.

Результаты тестирования:

- Успешность атак - 100% (10 из 10 попыток). Все сценарии, включая для дочернего домена и перемещение в целевой лес через уязвимые сервисные аккаунты, завершились успешно.
- Среднее время от начала атаки до получения прав Admin в целевом лесе составило 8,2 минуты. Низкое время обусловлено прямыми путями атаки.
- Журналы безопасности (Event ID 4769, 4672) фиксировали аномальные действия. EDR-системы сработали только в 2 случаях из 10, что демонстрирует низкую детекцию комплексных атак на доверие.
- Наиболее эффективным вектором оказалась эксплуатация SID History. Атакующий из домена forest-a.com, добавив SID группы «Domain Admins» целевого леса в свой токен, получил полный административный доступ в forest-b.com без необходимости взлома паролей.

Вывод: Настройки доверия по умолчанию создают критически опасную и уязвимую среду. Доверие является фактически полным, позволяя осуществлять быструю эскалацию привилегий и боковое перемещение между лесами. Данная конфигурация неприемлема для рабочих сред компаний.

Результат для Конфигурации В (доверие с включенным SID Filtering)

Характеристики: на базовое доверие применен механизм SID Filtering. Данная настройка фильтрует «чужие» SID (включая SID History) из токенов аутентификации, поступающих из доверенного леса.

Результаты тестирования:

- Успешность атак - 30% (3 из 10 попыток). Провалились все атаки, основанные на эксплуатации SID History и прямой эскалации через встроенные группы.

Успешными остались только атаки, основанные на компрометации конкретных учетных данных пользователей, имеющих права в целевом домене.

- Среднее время для успешных атак возросло до 22,5 минут. Увеличение связано с необходимостью этапа сбора и взлома хэшей Kerberos, что усложнило процесс.
- Активность, связанная с попытками использования отфильтрованных SID, генерировала события отказа в доступе (Event ID 4771). EDR-системы зафиксировали 7 срабатываний на подозрительные действия PowerShell и сетевые аномалии, что улучшило видимость атаки.
- Основным вектором осталась уязвимость сервисных аккаунтов. SID Filtering эффективно блокирует наиболее опасные пути атаки, но не защищает от компрометации учетных записей, которым предоставлены права.

Вывод: механизм SID Filtering является высокоэффективным барьером против сложных атак, направленных на эскалацию привилегий через свойства доверия. Он снижает поверхность атаки, переводя угрозу в плоскость защиты конкретных учетных данных. Это необходимый минимум для настройки любого межлесного доверия.

Результат для Конфигурации С (Доверие с Selective Authentication)

Характеристики: одностороннее нетранзитивное доверие между child.forest-a.com и forest-b.com с включенной опцией Selective Authentication. Доступ к ресурсам разрешен только тем пользователям, которым явно назначено право «Allowed to Authenticate» на конкретных компьютерах в целевом домене.

Результаты тестирования:

- Успешность атак - 10% (1 из 10 попыток). Единственная успешная атака стала возможной из-за ошибки конфигурации: право «Allowed to Authenticate» было ошибочно назначено не на конкретный сервер, а на весь узел домена (Domain Controllers OU), что предоставило избыточный доступ.
- Для единственной успешной атаки время составило 35,8 минут. Большая часть времени ушла на рекогносцировку и выявление ошибки в разграничении прав.
- Наблюдалась наибольшая активность систем защиты. Все попытки несанкционированной аутентификации четко фиксировались в журналах безопасности (Event ID 4771, 4625). EDR-системы сработали 12 раз, блокируя попытки выполнения скриптов и неавторизованный доступ к сетевым ресурсам.
- Главная ошибка - человеческий фактор и ошибки администрирования в совокупности. Принцип наименьших привилегий, лежащий в основе Selective Authentication, сам по себе надежен, но его некорректная реализация сводит защиту на нет.

Вывод: Selective Authentication является наиболее безопасной моделью доверия, превращая его из «доверия между доменами» в «точечный доступ для конкретных пользователей к конкретным ресурсам». Она максимально усложняет жизнь атакующему, но требует сложных процессов управления доступом и тщательного аудита.

Общий вывод по результатам исследования

Существует прямая зависимость между жесткостью механизмов защиты и устойчивостью доверительных отношений к атакам. Путь от конфигурации А к конфигурации С доказывает, что настройки по умолчанию неприменимы в реальных условиях, а дополнительные механизмы (SID Filtering, Selective Authentication) критически важны.

Ни один механизм не является 100% надежным. SID Filtering не спасает от компрометации учетных данных, а Selective Authentication уязвима к ошибкам конфигурации. Эффективная безопасность достигается только их комбинацией и многоуровневым контролем.

Автоматизированное тестирование незаменимо. Регулярная проверка с помощью инструментов вроде BloodHound и специализированных скриптов позволила не только подтвердить уязвимости, но и выявить ошибки в развертывании защитных мер (как в Конфигурации С), что невозможно при разовом документационном аудите.

Сложность эксплуатации для атакующего растет нелинейно. Введение каждого нового механизма защиты (от А к В, от В к С) не просто снижает процент успешных атак, но качественно меняет тактику атакующего, заставляя его совершать больше продуманных и явных действий, что значительно повышает шансы на обнаружение.

Таким образом, гипотезы исследования подтвердились: стандартные настройки небезопасны, регулярное тестирование выявляет больше рисков, а внедрение строгих механизмов защиты (SID Filtering, Selective Authentication) в рамках комплексной методики статистически значимо снижает успешность атак и повышает контролируемость инфраструктуры доверительных отношений.

Заключение

Проведённое исследование было направлено на разработку комплексной методики настройки и тестирования доверительных отношений в инфраструктуре Windows Active Directory. Эксперименты проводились на лабораторном стенде с использованием современных инструментов аудита в трёх различных конфигурациях доверия. Все гипотезы подтверждены. Цель достигнута.

Стандартные методы оценки безопасности действительно не отражают реальный эксплуатационный контекст. Разработанная методика выявила значительный разрыв между теоретически возможными и практически реализуемыми атаками, особенно в конфигурациях с SID Filtering и Selective Authentication. Регулярное автоматизированное тестирование с использованием скриптов PowerShell позволило выявить в несколько раз больше аномалий и векторов атаки по сравнению с разовым аудитом, что доказывает его эффективность для сокращения времени жизни опасных конфигураций. Внедрение ограничивающих механизмов (на примере Selective Authentication) статистически значимо снизило риск успешных атак. Интеграция статического анализа, динамического тестирования и оценки контрмер в единую методику доказала свою эффективность, обеспечив не только обнаружение уязвимостей, но и проактивную оценку рисков при изменении конфигурации.

Практическая значимость работы заключается в предоставлении инженерам безопасности и системным администраторам структурированного, воспроизводимого подхода к настройке и постоянному контролю одного из наиболее уязвимых элементов корпоративной инфраструктуры — доверительных отношений Active Directory.

Список литературы

1. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Компоненты доверия. — Введ. 2014-06-01. — М.: Стандартинформ, 2014. — 165 с. — (Система стандартов по информации, библиотечному и издательскому делу).
2. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Руководство по менеджменту безопасности информационных и телекоммуникационных технологий. Часть 5: Руководство по сетевой безопасности. — Введ. 2007-07-01. — М.: Стандартинформ, 2007. — 89 с. — (Система стандартов по информации, библиотечному и издательскому делу).
3. Kerberoasting [Электронный ресурс]. — URL: https://habr.com/ru/articles/875694/ (дата обращения: 01.12.2025).
4. Microsoft Learn. Как работают отношения доверия для лесов в Active Directory [Электронный ресурс]. — https://learn.microsoft.com/ru-ru/entra/identity/domain-services/concepts-forest-trust (дата обращения: 01.12.2025).
5. Настройка доверительных отношений между доменами Active Directory [Электронный ресурс]. — URL: https://dmosk.ru/ (дата обращения: 07.12.2025).
6. SpecterOps Team. BloodHound: Six Degrees of Domain Admin [Электронный ресурс]. — URL: https://github.com/BloodHoundAD/BloodHound (дата обращения: 01.12.2025).
7. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1: учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург: Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8.

References

1. GOST R ISO/IEC 15408-3-2013 Information technology. Security methods and tools. Information technology security evaluation criteria. Part 3: Assurance components. — Introduction. 2014-06-01. — Moscow: Standartinform, 2014. — p.165— (System of standards on information, librarianship and publishing).
2. GOST R ISO/IEC TO 13335-5-2006 Information technology. Security methods and tools. Information and telecommunication technology security management guide. Part 5: Network security guide. — Introduction. 2007-07-01. — Moscow: Standartinform, 2007. — 89 p. — (System of standards on information, librarianship and publishing).
3. Kerberoasting [Electronic resource]. URL: https://habr.com/ru/articles/875694/ (accessed: 01.12.2025).
4. Microsoft Learn. How Forest Trusts Work in Active Directory [Electronic resource]. URL: https://learn.microsoft.com/ru-ru/entra/identity/domain-services/concepts-forest-trust (accessed: 01.12.2025).
5. Configuring Trust Relationships Between Active Directory Domains [Electronic resource]. URL: https://dmosk.ru/ (accessed: 07.12.2025).
6. SpecterOps Team. BloodHound: Six Degrees of Domain Admin [Electronic resource]. URL: https://github.com/BloodHoundAD/BloodHound (accessed: 01.12.2025).

7. Uymin, A. G. Network and System Administration. Demonstration Exam CODE 1.1: A Study Guide for Secondary Vocational Education / A. G. Uymin. – 3rd edition, standardized. – St. Petersburg: Lan Publishing House, 2022. – p.480– ISBN 978-5-8114-9255-8.