УДК 004.056.53

Заворотный Константин Александрович, студент РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва

Трегубов Демид Евгеньевич, студент РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва

ПОСТРОЕНИЕ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ FREEIPA

В статье рассматривается построение отказоустойчивой системы аутентификации на базе FreeIPA для обеспечения непрерывности бизнес-процессов. Описана архитектура высокодоступного домена с применением многомастерной репликации, распределенных служб Kerberos и избыточного DNS. Проведено моделирование отказов узлов в среде ОС ALT Linux,. Проверены механизмы защиты: LDAPS, TLS, алгоритмы Kerberos AES, ролевая модель доступа и GSS-TSIG. Результаты подтверждают эффективность конфигурации в минимизации простоев и обеспечении информационной безопасности. Полученные данные применимы при проектировании доменных решений в рамках стратегии импортозамещения.

The article examines the implementation of a fault-tolerant authentication system based on FreeIPA to ensure business continuity. It describes a high-availability domain architecture using multi-master replication, distributed Kerberos services, and redundant DNS. Failure modeling was conducted in the ALT Linux OS environment. Security mechanisms including LDAPS, TLS, Kerberos AES, RBAC, and GSS-TSIG were verified. The results confirm the configuration's effectiveness in minimizing downtime and ensuring information security. The findings are applicable for designing domain solutions within import substitution strategies.

Ключевые слова: FreeIPA, централизованная аутентификация, отказоустойчивость, Kerberos, LDAP.

Key words: FreeIPA, centralized authentication, fault-tolerance, Kerberos, LDAP.

Введение

Современные корпоративные инфраструктуры становятся всё более распределёнными, а количество сервисов, пользователей и точек доступа продолжает расти. В этих условиях надежная система централизованной аутентификации играет ключевую роль в обеспечении безопасности и доступности информационных ресурсов. Нарушение работы доменной инфраструктуры приводит к полной недоступности сервисов, остановке бизнес-процессов и риску компрометации данных. Требования регуляторов (ФЗ-152, GDPR, PCI DSS) диктуют необходимость создания отказоустойчивых и защищённых систем управления доступом.

При использовании традиционных схем сервер аутентификации становится критически важной точкой отказа: сбой оборудования, потеря сетевой связности или целевая атака на каталог могут сделать невозможной работу всех сервисов, зависящих от домена. Это повышает актуальность разработки отказоустойчивых конфигураций, основанных на открытом программном обеспечении, которое при правильной настройке способно обеспечивать функциональность, сопоставимую с коммерческими решениями. Одним из таких комплексных решений является FreeIPA, объединяющая LDAP-каталог, Kerberos, DNS, инфраструктуру сертификатов и механизмы административного контроля.

Несмотря на широкое распространение FreeIPA, вопросы её поведения в условиях отказов, корректной работы механизмов многомастерной репликации, автоматического переключения клиентов и обеспеченности требований безопасности в практических сценариях остаются недостаточно исследованными. Это делает актуальной задачу экспериментальной проверки устойчивости и надёжности доменной инфраструктуры, построенной на базе

FreeIPA, особенно при использовании отечественных дистрибутивов, таких как ALT Linux.

Целью данного исследования является оценка отказоустойчивости и защищённости высокодоступной конфигурации FreeIPA при моделировании отказов ключевых сервисов домена

Объектом исследования выступают системы централизованной аутентификации в корпоративных Linux-инфраструктурах.

Предметом исследования является высокодоступная архитектура FreeIPA, включающая многомастерную репликацию каталога, распределённые сервисы Kerberos, избыточный DNS, защищённые каналы LDAPS, криптографические механизмы аутентификации и административные политики безопасности.

Практическая значимость работы заключается в оценке показателей готовности системы к отказам и проверке защитных механизмов (TLS, Kerberos, RBAC, DNS), что позволяет использовать результаты при проектировании защищённых корпоративных доменных решений на основе открытого ПО.

Литературный обзор

Централизованная аутентификация является одним из фундаментальных механизмов обеспечения информационной безопасности, и её теоретические основы подробно описаны в ряде международных стандартов и спецификаций. Архитектура и криптографическая модель современных систем идентификации базируются на стандартах RFC 4120 (Kerberos) и RFC 4510 (LDAP).

Практические аспекты построения комплексных решений управления доступом нашли отражение в документации FreeIPA и Red Hat Identity Management (IdM). Эти источники описывают интеграцию LDAP, Kerberos, сертификатов X.509, DNS-сервисов и политик безопасности в единую административную среду. Отдельное внимание уделяется механизму

многомастерной репликации, обеспечивающему поддержку распределённых топологий и высокую степень отказоустойчивости. Руководства по Multi-Master Replication, SSSD failover и DNS SRV-механизмам приводят детальные рекомендации по построению надёжной и масштабируемой инфраструктуры.

Анализ угроз (атаки на билеты, MITM, незашифрованные соединения) обосновывает необходимость применения в Kerberos и LDAP механизмов pre-authentication, LDAPS/TLS и строгих политик доступа.

С точки зрения операционной и нормативной практики особую роль играют требования стандартов и регуляторов — ФЗ-152, GDPR, PCI DSS, рекомендаций регуляторов по защите персональных данных. Эти документы определяют необходимость обеспечения непрерывности сервисов аутентификации, применения криптографических протоколов и защиты административных операций. В среде российских Linux-дистрибутивов практические руководства ALT Linux предоставляют рекомендации по настройке FreeIPA, DNS, Kerberos, TLS и политик аутентификации с учётом требований промышленной эксплуатации.

Таким образом, доступная литература и нормативные источники формируют широкую теоретическую и методическую основу для изучения механизмов аутентификации и построения отказоустойчивых инфраструктур. Однако большинство работ охватывают протоколы, архитектуры и методики защиты, в то время как практическая оценка отказоустойчивости конкретных реализаций — особенно в открытых системах — остаётся недостаточно представленной. Это определяет необходимость проведения экспериментального исследования устойчивости FreeIPA в реальных сценариях отказов и подтверждает актуальность настоящей работы.

Методы исследования

Исследование проводилось методом экспериментального моделирования в изолированной виртуализированной среде, построенной на базе дистрибутивов ALT Linux 11 (Server и Workstation). В экспериментальной инфраструктуре были развернуты два серверных узла FreeIPA,

функционирующих в режиме многомастерной репликации, и один клиентский узел, использующий динамическое обнаружение сервисов домена через SRV-записи DNS. Логическая схема используемой топологии представлена на рисунке 1.

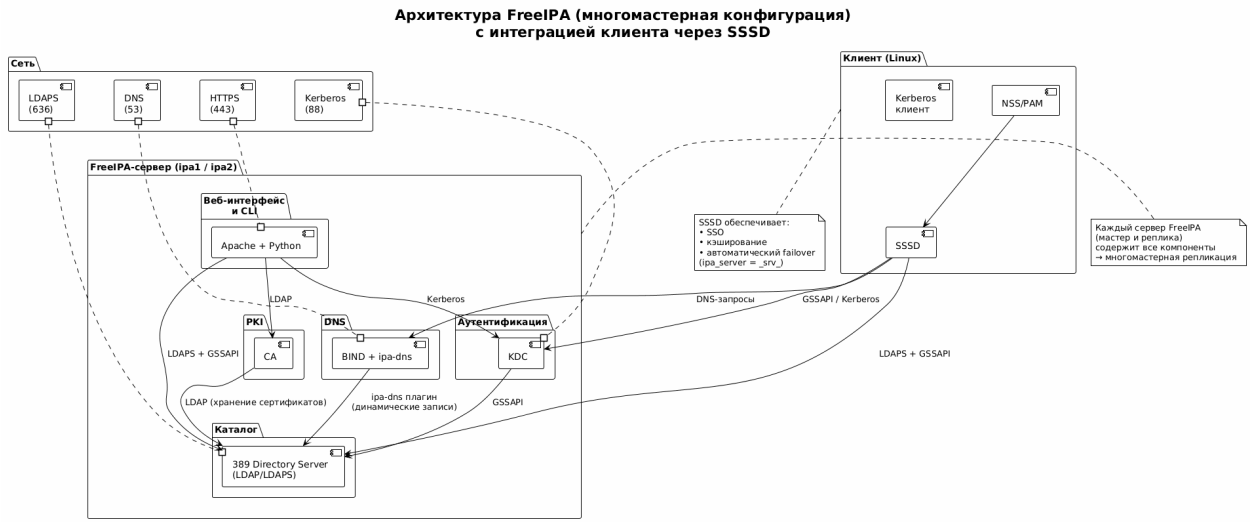

Рисунок 1 – Архитектура FreeIPA

Проверка корректности топологии выполнялась с помощью стандартных инструментов FreeIPA для просмотра репликационных сегментов.

Экспериментальная часть исследования включала моделирование нескольких типов отказов, типичных для корпоративной инфраструктуры: отключение мастер-сервера, недоступность DNS-службы, остановка KDC, временная потеря сетевой связности и проверка отказоустойчивости клиентского поведения при использовании механизма _srv_.

Отдельным направлением стала проверка мер безопасности (LDAPS, TLS, алгоритмы Kerberos, политики паролей, RBAC, GSS-TSIG) встроенными средствами FreeIPA и инструментами ALT Linux для оценки соответствия конфигурации установленным требованиям.

Результаты исследования

Экспериментальная оценка отказоустойчивости двухузловой системы FreeIPA показала, что механизмы многомастерной репликации, избыточности DNS и распределённых KDC обеспечивают высокую устойчивость службы

аутентификации к отказам отдельных узлов. Репликация данных каталога между мастер-сервером и репликой функционировала в обоих направлениях, что подтвердило корректность настройки и синхронизации пользовательских записей, политик доступа и сертификатов.

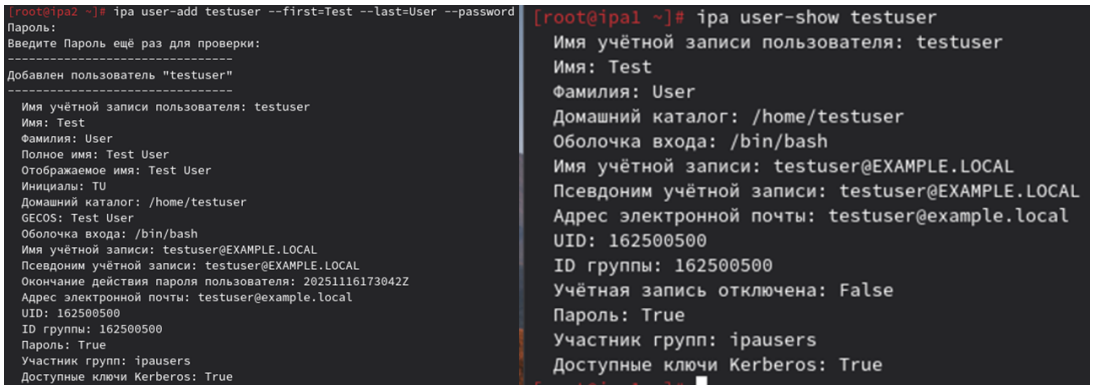

Рисунок 2 — Подтверждение корректной репликации данных между узлами FreeIPA.

В ходе экспериментов был проведён тест полного отключения мастер-узла. После искусственного прекращения работы сервера клиенты сохранили возможность аутентификации и продолжили получать информацию из домена без задержек.

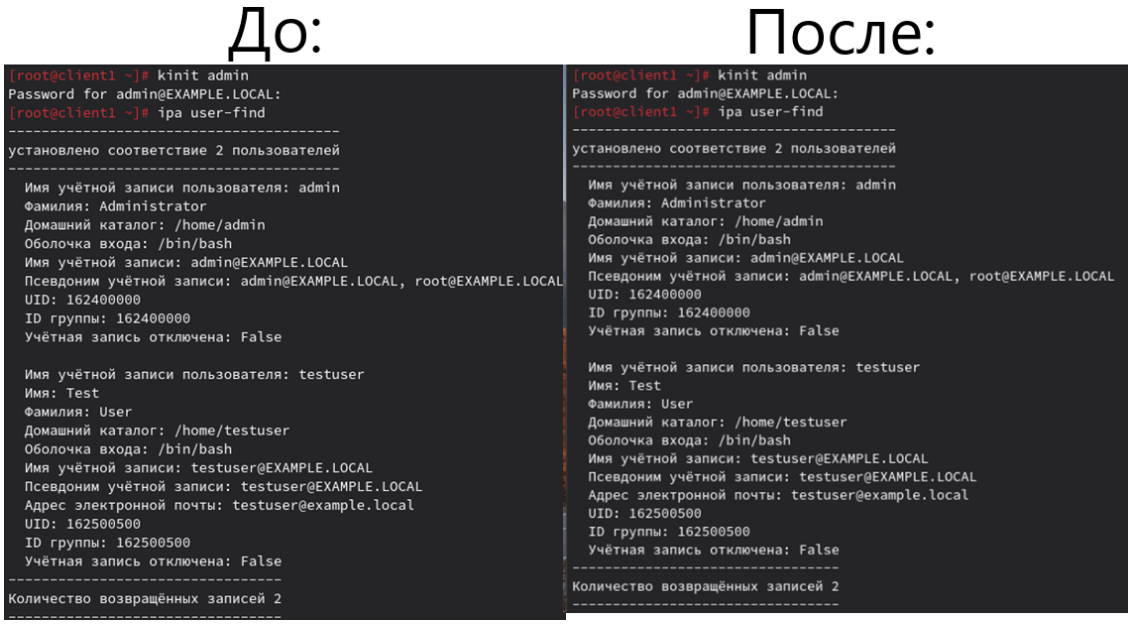

Рисунок 3 — Работа клиента FreeIPA до и после отключения мастер-сервера.

Переключение на реплику происходило автоматически благодаря использованию SRV-записей Kerberos и LDAP, а также конфигурации клиента с динамическим поиском доступных серверов через srv-механизм SSSD.

Время восстановления обслуживания не превысило нескольких секунд, что соответствует требованиям к высокодоступным системам аутентификации.

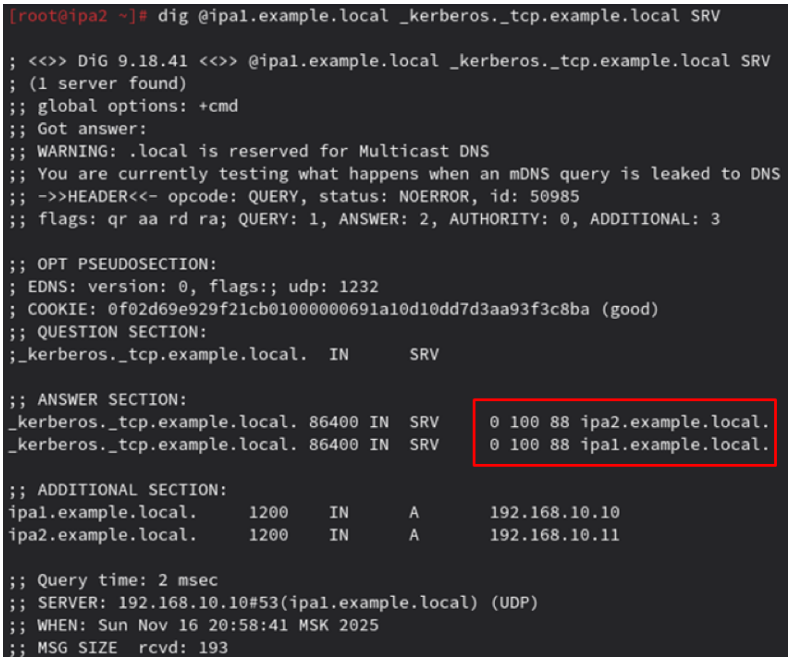

Рисунок 4 — SRV-записи Kerberos, используемые клиентами для автоматического выбора доступного KDC.

Тестирование отказоустойчивого DNS также подтвердило корректность работы. При недоступности основного DNS-сервера клиенты успешно переключались на вторую зону, что обеспечило непрерывное разрешение имён для Kerberos, LDAP и внутренних сервисов FreeIPA. Работа SSSD-кэша позволила сохранить работоспособность механизма входа в систему даже при кратковременных потерях связи.

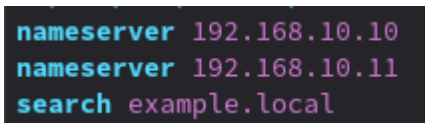

Рисунок 5 — Конфигурация клиента с двумя DNS-серверами для обеспечения отказоустойчивости.

Анализ журналов подтвердил отсутствие конфликтов и целостность данных после восстановления мастер-сервера.

```
[root@ipa1 ~]# ipa topologysegment-find ca
--------------------------------
установлено соответствие 1 сегмента
--------------------------------
  Имя сегмента: ipa1.example.local-to-ipa2.example.local
  Левый узел: ipa1.example.local
  Правый узел: ipa2.example.local
  Возможность подключения: both
--------------------------------
Количество возвращённых записей 1
--------------------------------
```

Рисунок 6 — Состояние репликационных сегментов между серверами FreeIPA.

Анализ конфигурации FreeIPA показал, что служба LDAP доступна по защищённому порту 636.

```
[root@ipa1 ~]# ss -tulnp | grep 636
tcp   LISTEN 0      128                                *:636              *:*    users:(("ns-slapd",pid=1235,fd=9))
```

Рисунок 7 – Подтверждение слушания порта 636

Трафик-анализ подтвердил использование LDAPS: TLS-шифрование исключает перехват учетных данных в открытом виде.

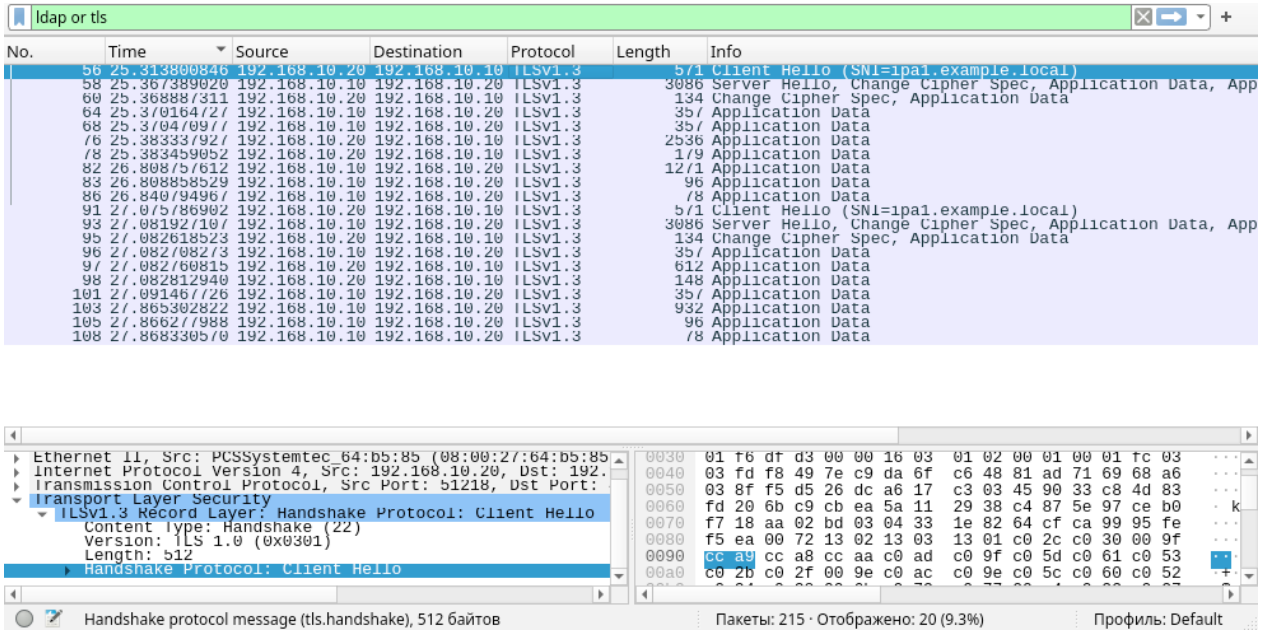

Рисунок 8 — Анализ трафика при нормальной работе клиента

Для подтверждения корректности настроек безопасности доменной инфраструктуры были проанализированы параметры Kerberos и LDAPS. Проверка показала, что KDC использует современные алгоритмы шифрования AES, для пользователей корректно применяется ролевая модель RBAC, максимальный срок жизни билета составляет один день, что соответствует рекомендациям по обеспечению безопасности, а LDAPS-сертификат

находится в состоянии MONITORING, что означает его автоматическое отслеживание и продление службой certmonger.

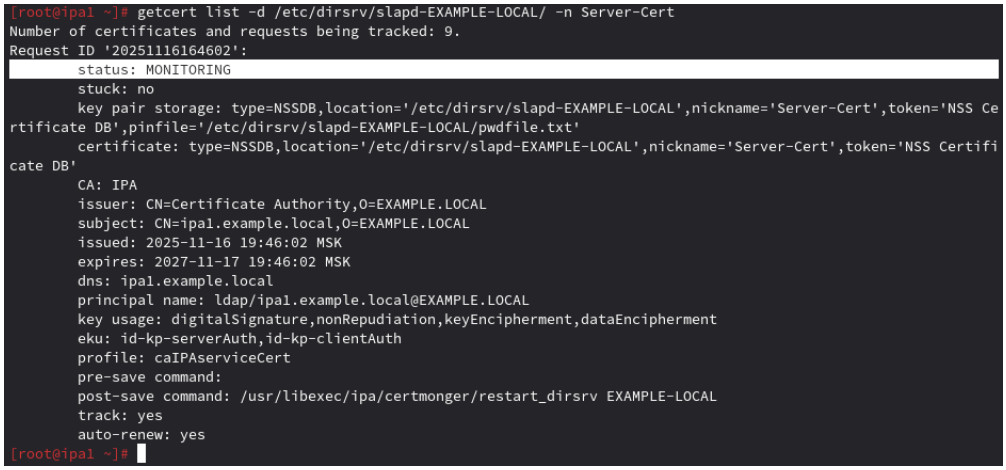

Рисунок 9 — Подтверждение работы LDAPS и корректного TLS-сертификата FreeIPA

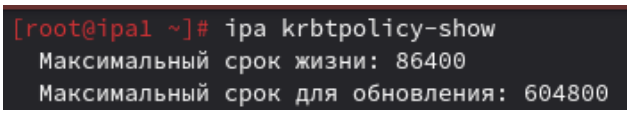

Рисунок 10 – Проверка сроков жизни билетов

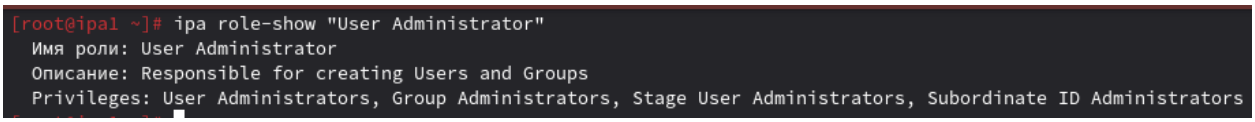

Рисунок 11 – Проверка роли User Administrator

Рисунок 12 — Разрешённые криптографические алгоритмы Kerberos

Проверка протокола Kerberos подтвердила корректный обмен сообщениями AS-REQ и AS-REP между клиентом и контроллером домена. Передача ключевого материала и служебных данных осуществляется в зашифрованном виде, что соответствует требованиям безопасной аутентификации.

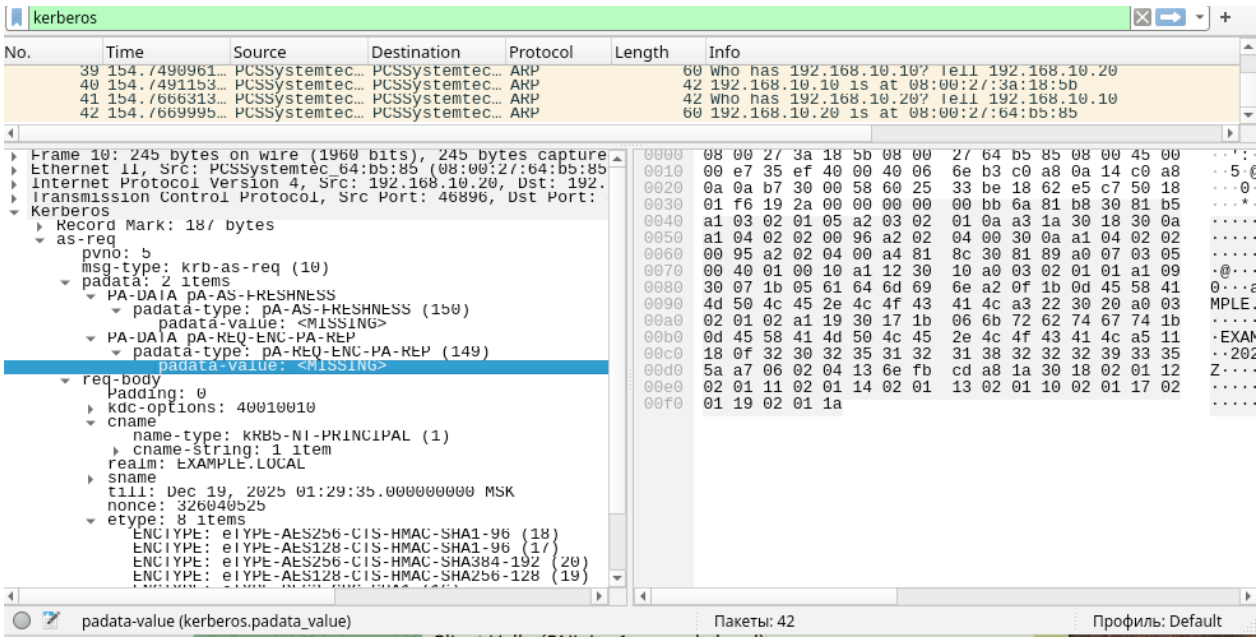

Рисунок 13 — Трафик Kerberos при kinit admin

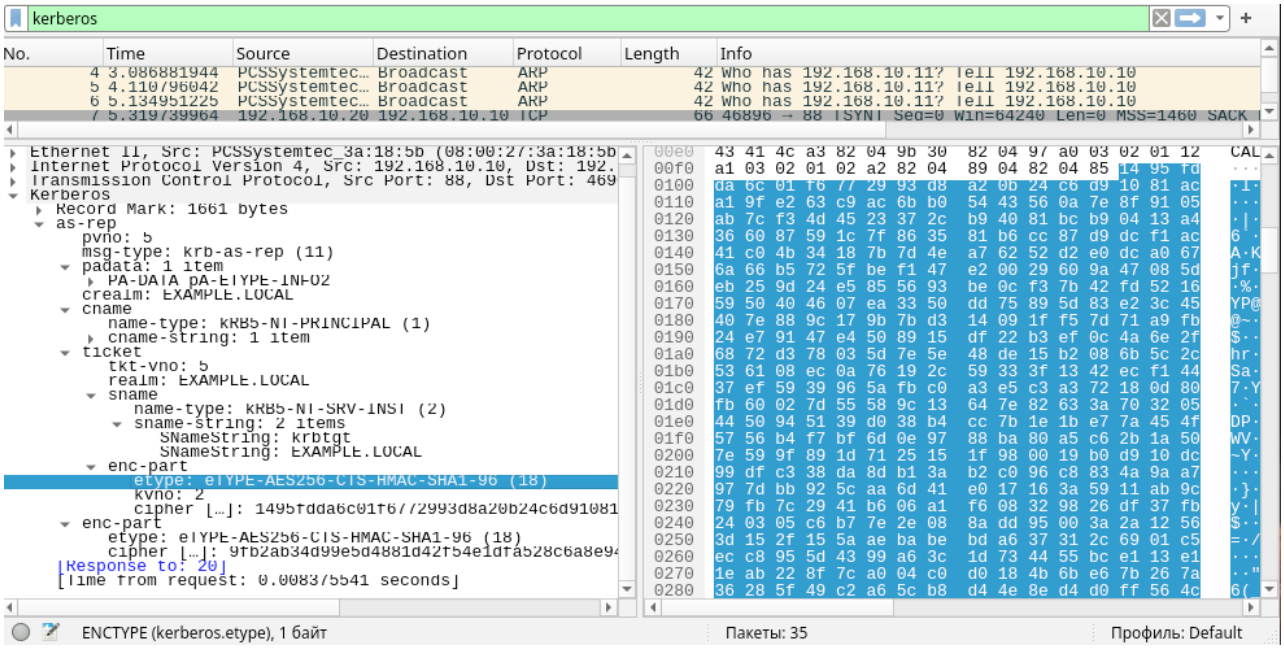

Рисунок 14 — Трафик Kerberos при kinit admin

Примененная политика паролей (длина, сложность, блокировка) минимизирует риски подбора и соответствует стандартам безопасности.

```
[root@ipa1 ~]# ipa pwpolicy-mod global_policy \
  --maxlife=60 \
  --minlife=24 --history=24 \
  --minclasses=3 \
  --minlength=12 \
  --maxfail=3 \
  --failinterval=60 \
  --lockouttime=900 \
  --grace=5
  Группа: global_policy
  Максимальный срок действия (в днях): 60
  Минимальный срок действия (в часах): 24
  Размер журнала : 24
  Классы символов: 3
  Минимальная длина: 12
  Максимальное количество ошибок: 3
  Интервал сброса ошибок: 60
  Длительность блокировки: 900
  Grace login limit: 5
```

Рисунок 15 — Настройки политики паролей FreeIPA

При попытках перебора паролей механизм аутентификации корректно реагирует на подозрительную активность. После превышения допустимого числа неудачных попыток входа учётная запись переводится в заблокированное состояние, а дальнейшие запросы аутентификации отклоняются сервером, что подтверждает эффективность защиты от атак типа brute force.

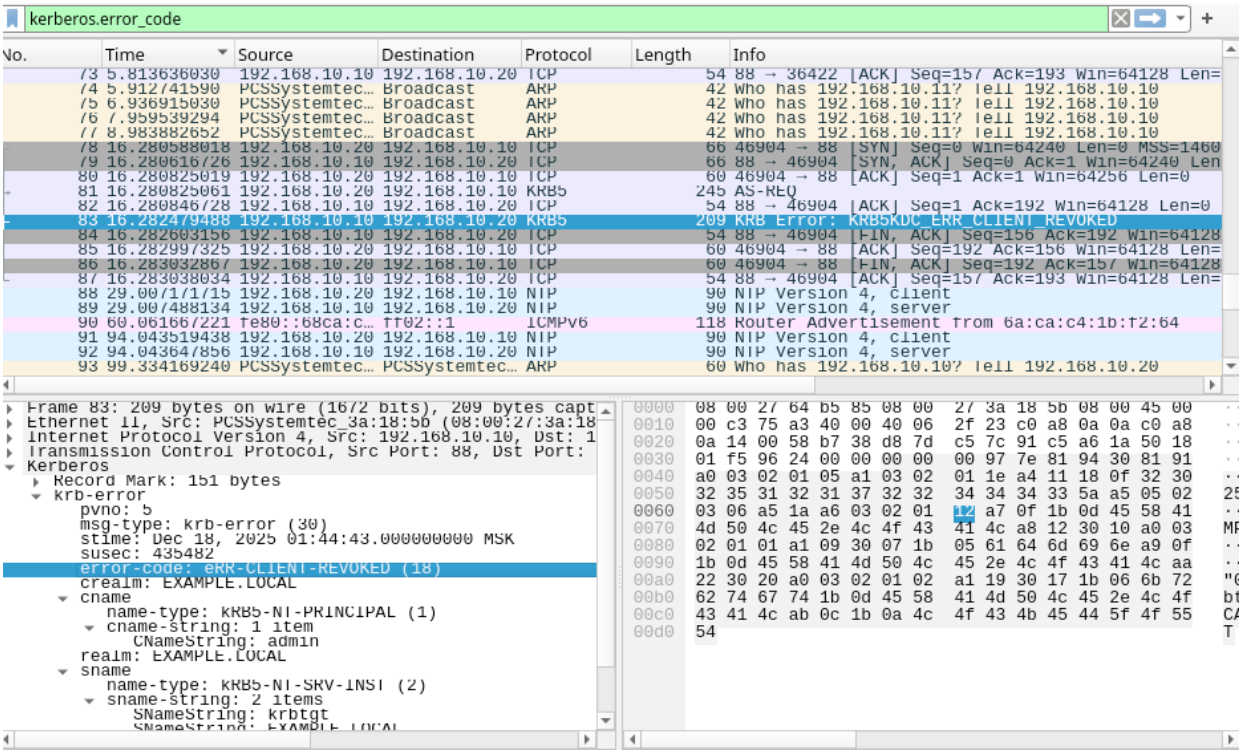

Рисунок 16 — Анализ брутфорс атаки на Kerberos

Проверка механизма защиты DNS показала, что зона example.local защищена с помощью GSS-TSIG. Это исключает возможность внесения

изменений в DNS-записи неавторизованными клиентами и предотвращает атаки подмены записей.

```
[root@ipa1 ~]# ipa dnszone-show example.local
  Имя зоны: example.local.
  Активная зона: True
  Полномочный сервер имён: ipa1.example.local.
  Адрес электронной почты администратора: hostmaster.example.local.
  Номер SOA: 1764935309
  Обновление SOA: 3600
  Повторный запрос SOA: 900
  Окончание действия SOA: 1209600
  Минимальный срок жизни SOA: 3600
  Политика обновления BIND: grant EXAMPLE.LOCAL krb5-self * A; grant EXAMPLE.LOCAL krb5-self * AAAA; grant EXAMPLE.LOCAL
                            krb5-self * SSHFP;
  Динамическое обновление: True
  Разрешить запрос: any;
  Разрешить перенос: none;
```

Рисунок 17 — Состояние DNS-зоны example.local

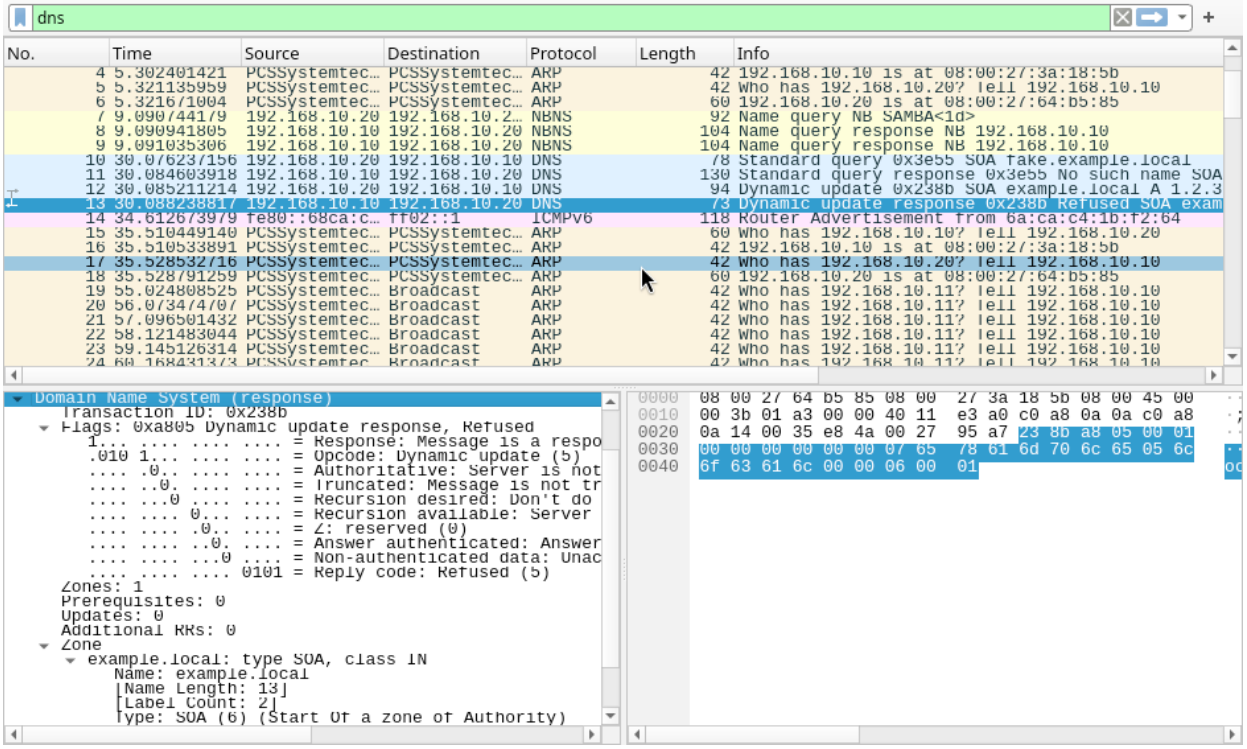

Рисунок 18 — Анализ трафика при попытке DNS-spoofing

Результаты тестирования, включая анализ сетевого трафика, подтвердили корректную работу механизмов защиты — TLS/LDAPS, криптографических алгоритмов Kerberos, ролевого разграничения прав, политик паролей и защиты DNS-зоны, что свидетельствует о соответствии предложенной конфигурации современным требованиям информационной безопасности.

Заключение

Экспериментальные результаты показали, что двухузловая конфигурация с многомастерной репликацией обеспечивает непрерывность процессов аутентификации при недоступности одного из узлов, переключение клиентов происходит автоматически, а потеря данных отсутствует.

Дополнительно проведённая проверка мер безопасности, в том числе с использованием анализа сетевого трафика, продемонстрировала корректность применения защищённого канала LDAPS, использование современных криптографических алгоритмов Kerberos, работу усиленных политик паролей и защиту DNS-зоны с использованием GSS-TSIG. Это подтверждает, что предложенная архитектура обеспечивает не только отказоустойчивость, но и соответствие актуальным требованиям информационной безопасности и промышленной эксплуатации.

Таким образом, полученные данные могут быть использованы при разработке и внедрении доменных решений на базе открытого программного обеспечения, а также служить основой для дальнейших исследований масштабируемости, распределённых топологий и интеграции с внешними системами федерации идентичности.

Список использованных источников

1. FreeIPA в ОС ALT Linux: установка сервера, настройка репликации и клиентской части [Электронный ресурс] // ALT Linux Wiki. – URL: https://www.altlinux.org/FreeIPA (дата обращения: 17.11.2025).

2. FreeIPA Project Documentation: Multi-Master Replication, Backup and Restore [Electronic resource] // FreeIPA Project Official Website. – URL: https://www.freeipa.org/page/Documentation (дата обращения: 17.11.2025).

3. Man-страницы ipa-server-install, ipa-replica-install, ipa-backup [Электронный ресурс] // Linux man pages online. — Режим доступа: https://man7.org/linux/man-pages/. — Дата обращения: 17.11.2025.

4. SSSD Configuration — ipa_server parameter [Электронный ресурс] // SSSD Documentation. — Режим доступа:

https://sssd.io/docs/design_pages/ipa_failover.html. — Дата обращения: 17.11.2025.

5. RFC 4120: Kerberos V5 / RFC 4510: LDAP Technical Specification [Electronic resource] // IETF Datatracker. – URL: https://datatracker.ietf.org/ (дата обращения: 17.11.2025).

6. ЦИФРОВЫЕ ДВОЙНИКИ СЕТЕВЫХ ИНФРАСТРУКТУР: ТОЧНОСТЬ, МЕТОДЫ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ Уймин А.Г. Радиотехнические и телекоммуникационные системы. 2023. № 3 (51). С. 44-52.