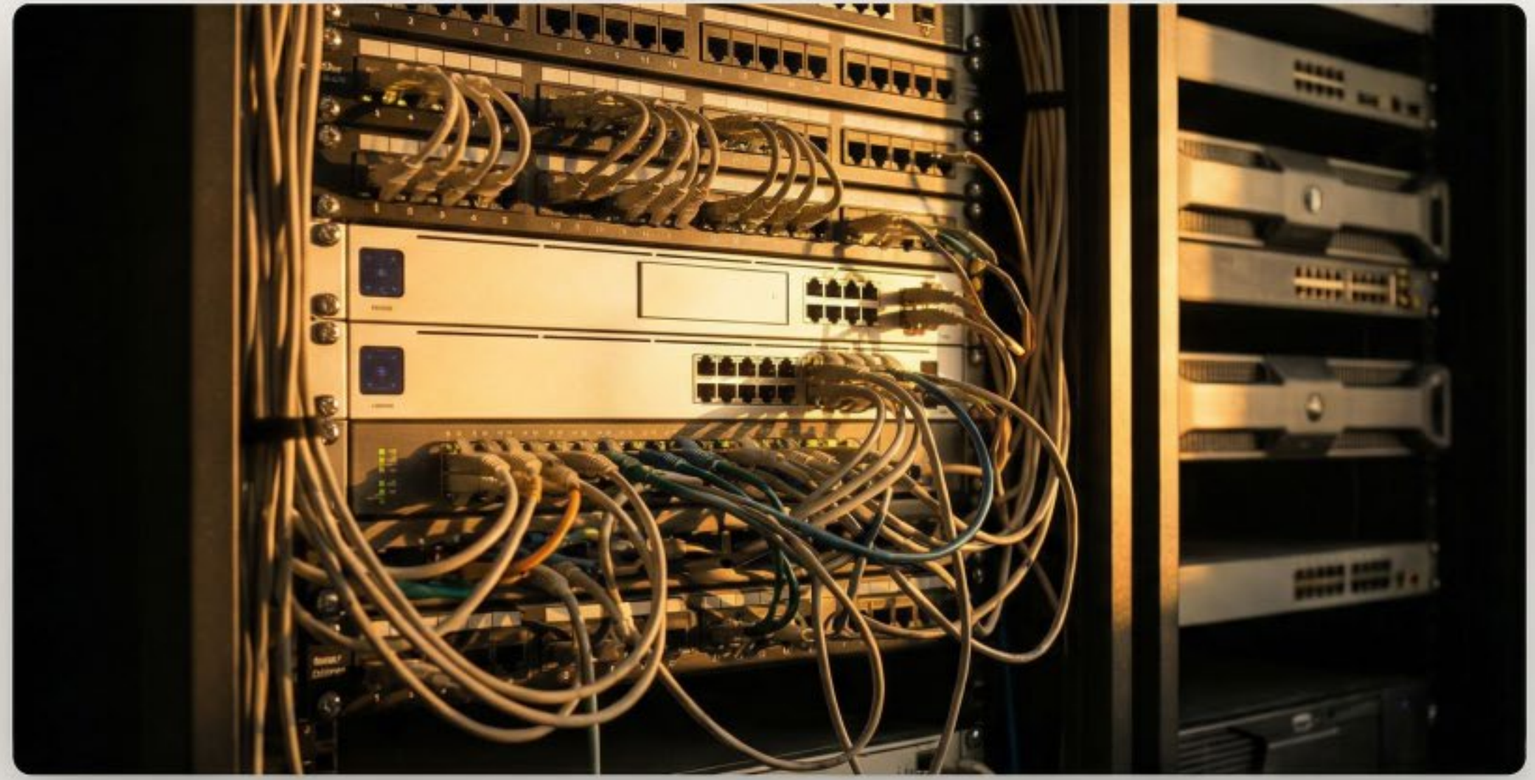


Факторы деградации архитектуры сегментации LAN: организационные барьеры, легаси-системы и проблемы управления политиками безопасности

Митрофанов М.В., Университет ИТМО | РусКрипто 2026 | Секция: Перспективные исследования в области кибербезопасности

Актуальность

- Рост сложности корпоративных сетей
- Противоречие: теоретическая модель сегментации vs. фактическое состояние
- Систематическое расхождение между декларируемой архитектурой и реальностью

Ключевой тезис:
сегментация деградирует во времени, что требует нового теоретического осмысления проблемы.

пробел в исследованиях

M.V. Mitrofanov, ITMO University | RusCrypto 2026 | Cybersecurity Research

Ограниченный фокус

Фокус исключительно на технических аспектах VLAN и межсетевых экранов, игнорируя организационные факторы.

Нет оценки деградации

Отсутствие системной методологии и математического аппарата для моделирования деградации во времени.

Статический подход

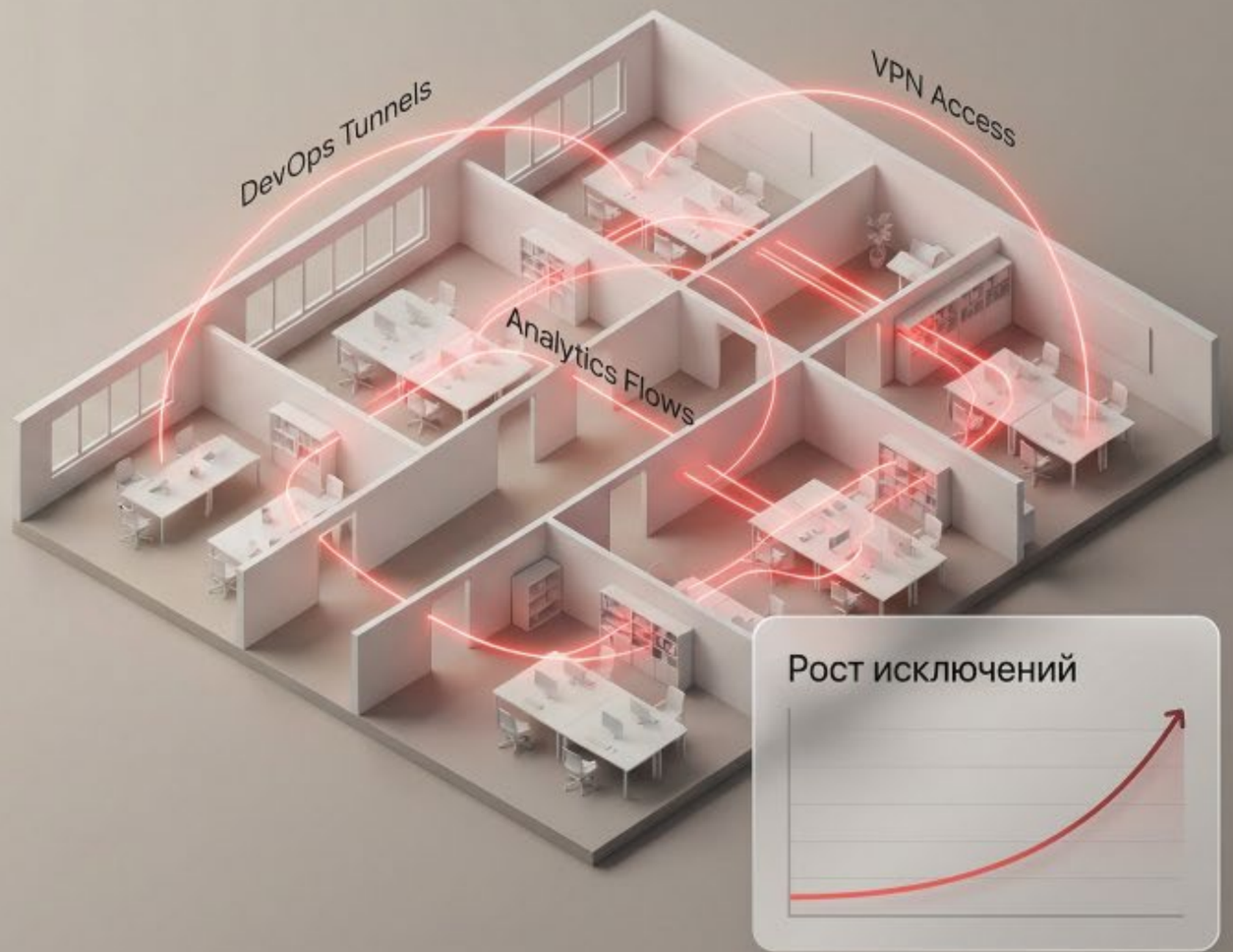
Игнорирование эволюционной природы архитектуры и динамики изменений межсегментной связности.

Отсутствие метрик

Нет формализованных метрик для количественной оценки эффективности изоляции и выявления деградации.

Фактор 1: Несоответствие модели реальным потокам

- **Противоречие:**
- Традиционная VLAN-сегментация vs. фактическая топология взаимодействий.
- **Конфликты реального мира:** Аналитические системы требуют доступа к базам данных; DevOps – к тестовым и прод-средам; VPN – к кросс-сегментным ресурсам.
- **Следствие:** Экспоненциальный рост исключений в политиках безопасности, превращающий сеть в "плоскую".



Фактор 2: Легаси-системы

- Унаследованные инфраструктуры с архитектурными ограничениями.
- Устаревшие ERP и базы данных из эпохи плоских сетей.
- Требуют широкополосного доступа, создавая обходные пути.
- Временные решения становятся постоянными и не удаляются.

Фактор 3: Отсутствие аудита

- Ad-hoc правила без документирования
- Отсутствие централизованного логирования
- Невозможность оценки фактического состояния
- Прогрессирующая эрозия изоляции, когда степень деградации становится неизмеримой

Фактор 4: Организационные барьеры

Конфликт: Скорость бизнеса vs. Безопасность

Давление на создание исключений

Коэффициент сопротивления C_{org}: Нежелание адаптации

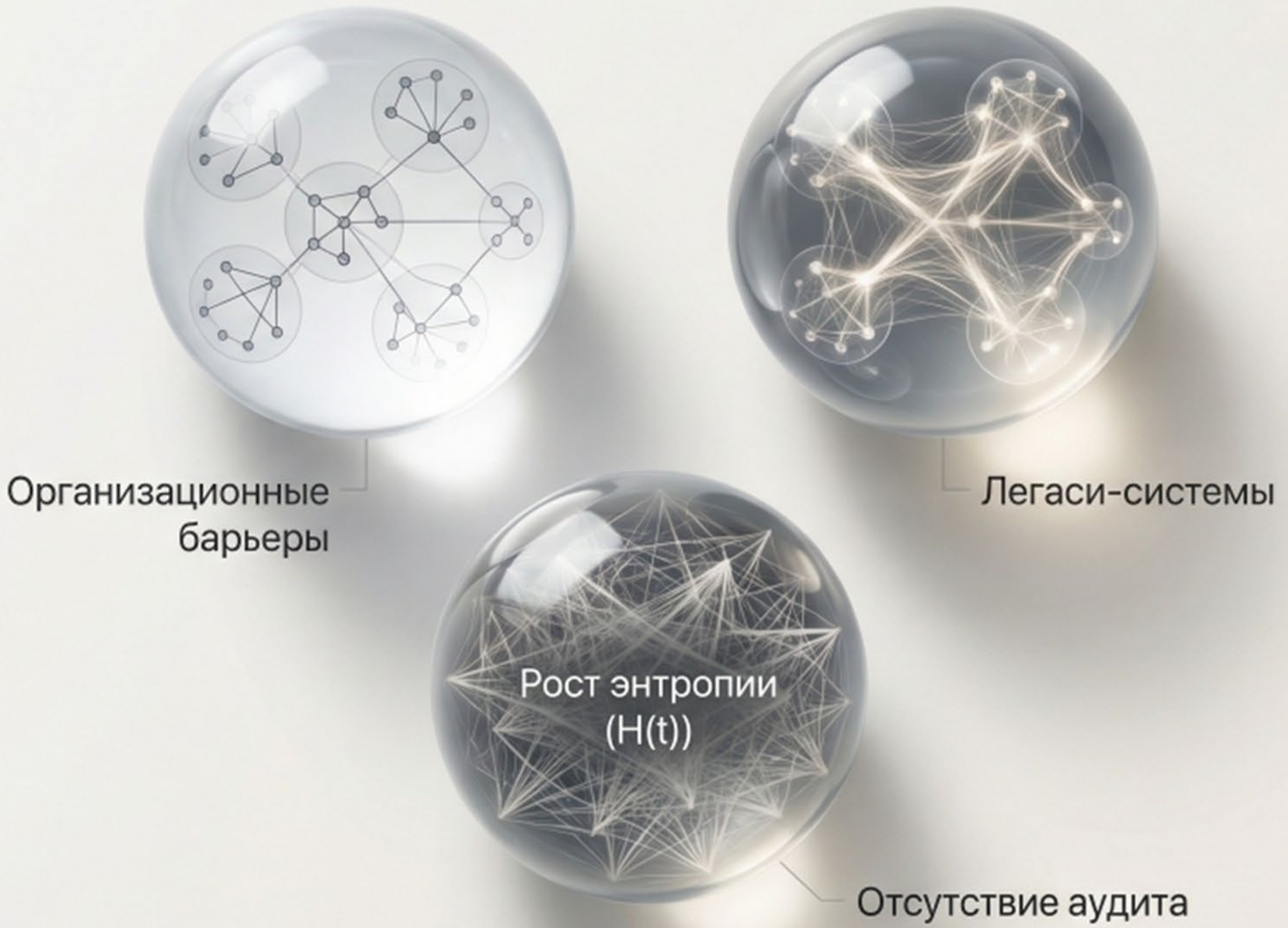
Порочный круг: Строже политика → Выше давление → Деградация

Сегментация только на уровне документации

Гипотеза исследования

Центральное утверждение:
эффективность сегментации
характеризуется временной деградацией.
Три фактора детерминируют процесс:
организационные барьеры,
архитектурные ограничения легаси-
систем и недостаточность аудита.

Рост энтропии межсегментных связей
ведет к снижению
эффективной изоляции,
потенциально конвергируя
сеть в плоскую топологию.



Цель и задачи исследования

Цель: Разработать математическую модель для количественной оценки деградации сегментации LAN и прогнозирования критических состояний.

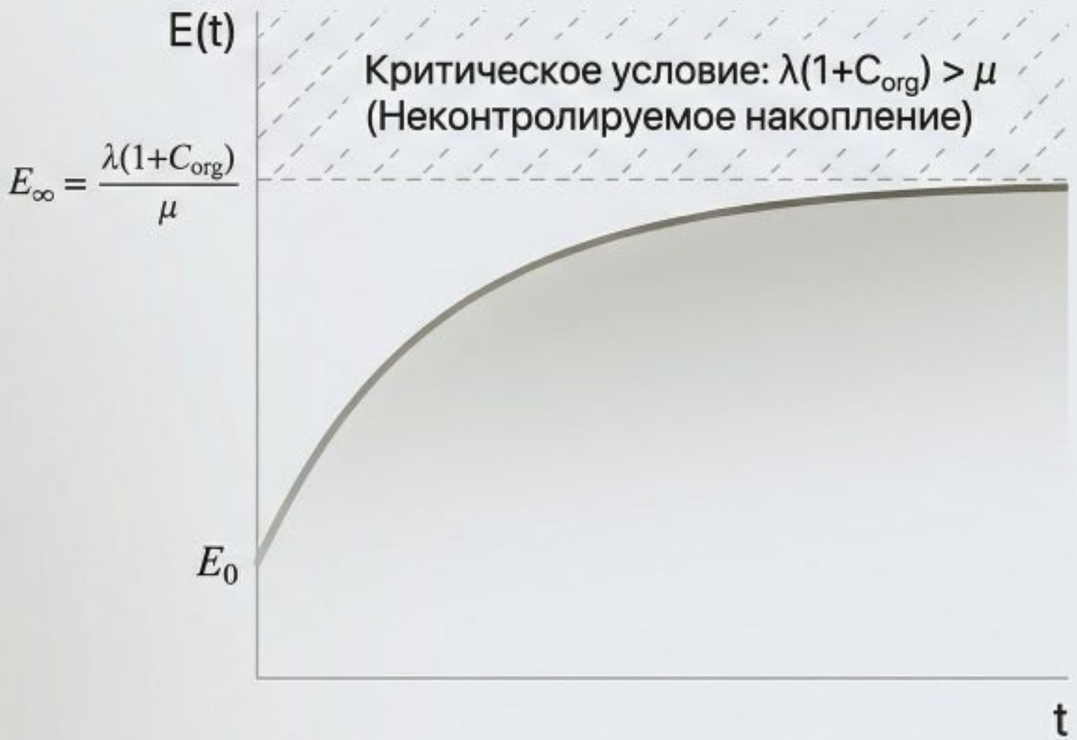
1. Формализация метрик эффективности сегментации.
2. Моделирование накопления политик-исключений.
3. Оценка влияния легаси-систем на деградацию.
4. Интеграция моделей в единую систему уравнений.
5. Проведение вычислительного эксперимента.

Динамика накопления исключений

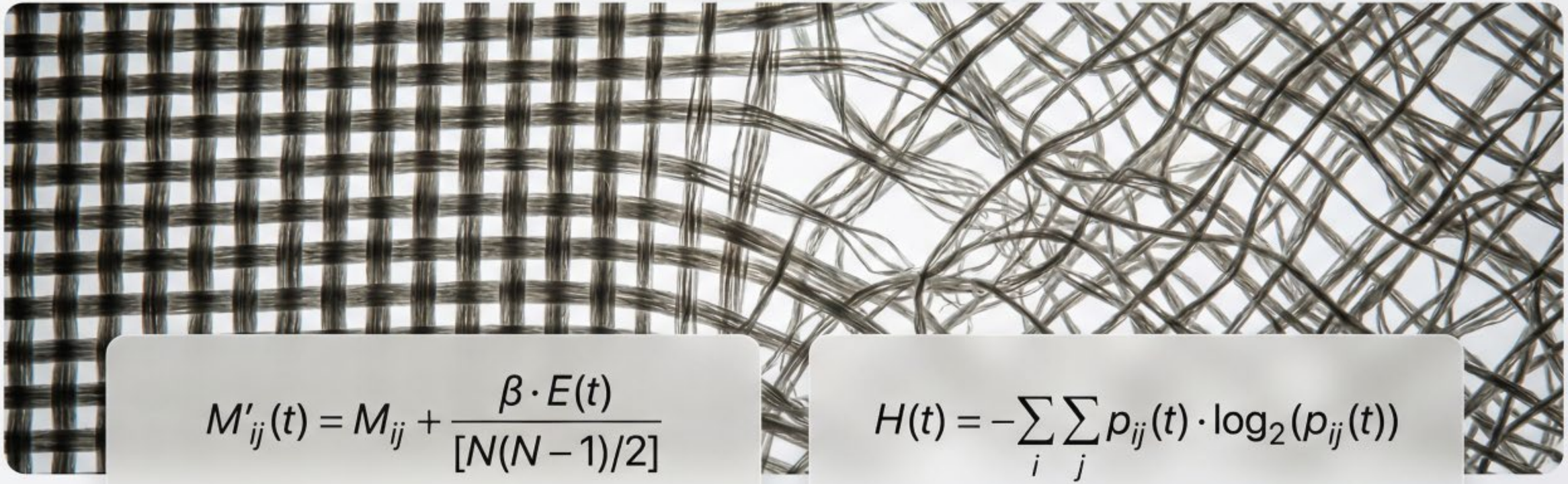
$$\frac{dE(t)}{dt} = \lambda(1 + C_{org}) - \mu \cdot E(t)$$

$$E(t) = \frac{\lambda(1 + C_{org})}{\mu}(1 - e^{-\mu t}) + E_0 \cdot e^{-\mu t}$$

Модель роста исключений с учетом организационного сопротивления



Эволюция матрицы связности и энтропия



$$M'_{ij}(t) = M_{ij} + \frac{\beta \cdot E(t)}{[N(N-1)/2]}$$

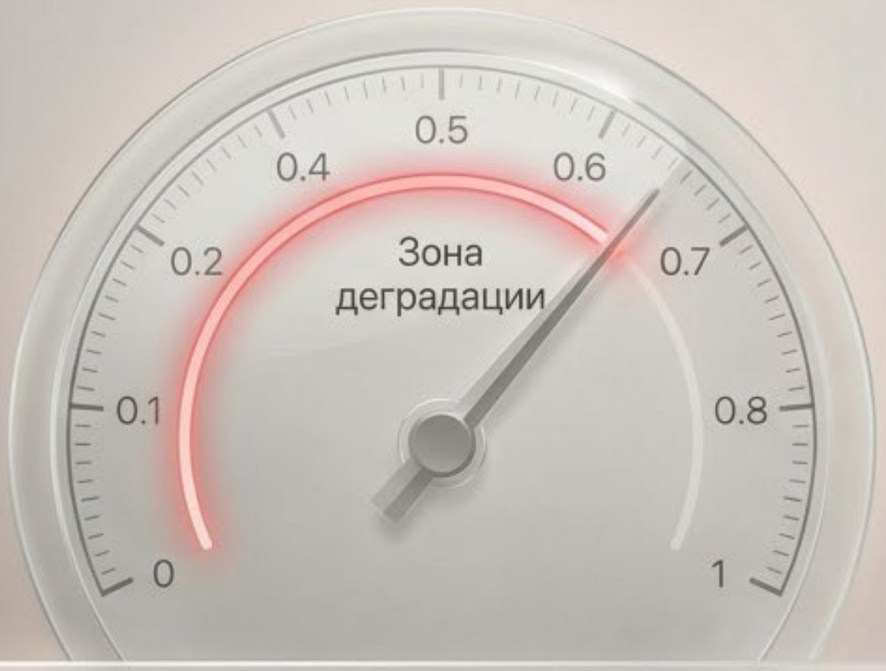
Эволюция матрицы связности под влиянием накопленных исключений

$$H(t) = -\sum_i \sum_j p_{ij}(t) \cdot \log_2(p_{ij}(t))$$

Энтропия Шеннона: количественная оценка структурного хаоса

Рост энтропии сигнализирует о переходе от структурированной архитектуры с выделенными изолированными зонами к хаотической топологии с практически равновероятными связями между всеми сегментами.

Коэффициент эффективной изоляции (IEI)



$$IEI(t) = 1 - [\sum_{i \neq j} M'_{ij}(t)]/[\sum_{i \neq j} M^*_{ij}]$$

- Диапазон значений: [0, 1] (1 = идеальная изоляция)
- Пороговое значение: IEI = 0.7 (критическая граница)
- Время полуразрушения T_{deg}: момент, когда $IEI(T_{deg}) = 0.5$

Влияние легаси-систем и эффективность аудита

Идеальная Сегментация

$$P_{degrad}(i) \approx 0$$

Деградация от Легаси

Неконтролируемый экспоненциальный рост исключений

$$P_{degrad}(i) = 1 - \prod_{k=1}^{L}(1 - \gamma_k \cdot d_{ik})$$

Эффективность Аудита:

$$A_{eff} = \mu/[\lambda(1+C_{org})]$$

Критическое условие стабильности: $A_{eff} \geq 1$

Параметры вычислительного эксперимента

Сегменты сети (N):	12 (Бухгалтерия, Маркетинг, Серверная, Разработка, Тест, Аналитика, Гостевой, IoT, Админ, DMZ, Резерв, Управление)
Исходная Матрица Связности	Строгая изоляция, 18/66 возможных связей (только смежные зоны)
Интенсивность требований (λ):	8 запросов/месяц
Коэффициент сопротивления (C_org):	0.5
Интенсивность аудита (μ):	0.1 правил/месяц
Коэффициент влияния исключений (β):	0.3
Начальные исключения (E_0):	5
Легаси-системы (L):	3

Результаты базового сценария

- Стационарное количество исключений
  $E_\infty = 120$ правил
- Эффективность аудита
  $A_{eff} \approx 0.0083 < 1$
  (Критическое условие)
- Фактическая связность
  $M'_{ij}(24) \approx M_{ij} + 0.498$
- Индекс легаси-влияния
  $\Psi_{legacy} \approx 0.56$

Сценарии корректирующих мер

Сравнение стратегий управления сегментацией. Комбинированная стратегия обеспечивает возвращение IEI к приемлемому уровню (>0.7). Изолированные меры недостаточны.

Базовый сценарий: IEI=0.365 | Снижение сопротивления: IEI=0.422 | Усиленный аудит: IEI=0.582 | Комбинированная стратегия: IEI=0.706 (+ΔIEI)

Выводы и практические рекомендации

Ключевые выводы

- Эмпирическое подтверждение деградации сегментации во времени.
- Сегментация – динамический процесс, требующий непрерывного мониторинга.
- Критическая важность баланса $A_{eff} \geq 1$.

Практические рекомендации

- Внедрение систем непрерывного мониторинга IEI, H(t), A_{eff}.
- Автоматизация выявления и деактивации неиспользуемых правил.
- Поэтапная миграция легаси-систем на современные платформы.
- Организационные политики с указанием срока действия исключений.