КОНФИДЕНЦИАЛЬНО

АУДИТ ИТ-ИНФРАСТРУКТУРЫ · 2026

Сеть, которую *видно.*

Отчёт по итогам обследования сети и серверной инфраструктуры ООО «Северный продукт»: шесть площадок, производство и розница.

6	47	12	3
ПЛОЩАДОК	УСТРОЙСТВ	НАХОДОК	КРИТИЧНЫЕ

Илья Шаповалов
сетевой инженер · Zabbix, MikroTik, SNMP
t.me/ilik_1

обследование 12–15 октября 2026
отчёт от 16 октября 2026
версия 1.0

ДЕМОНСТРАЦИОННЫЙ ОБРАЗЕЦ. Компания и данные вымышлены; структура, характер находок и оформление — такие же, как в реальном отчёте.

ЧТО ВНУТРИ

Десять минут вместо *полугода догадок*

Отчёт отвечает на три вопроса: что у вас есть, что из этого сломается первым и что делать в первую очередь. Без пересказа конфигураций — только то, что влияет на простой.

Резюме для руководителя 03
главное на одной странице

Границы и методика 04
что проверено, чего не касались

Карта сети 05
как всё связано на самом деле

Критичные находки (P1) 06
ломается уже сейчас

Существенные находки (P2) 07
авария станет дороже

Гигиена и порядок (P3) 08
не горит, но мешает

Наблюдаемость 09
что видно без мониторинга и что — с ним

План на 30 и 90 дней 10
по приоритетам и стоимости

КАК ЧИТАТЬ ПРИОРИТЕТЫ

P1 — угрожает остановкой работы сегодня. P2 — увеличивает цену и длительность аварии. P3 — порядок, который экономит время в будущем. Все оценки сделаны по результатам опроса, конфигураций и 72-часового наблюдения.

РЕЗЮМЕ ДЛЯ РУКОВОДИТЕЛЯ

Сеть держится на *одном человеке* и одном канале

4 ч 40 м
ПРОСТОЙ ЗА КВАРТАЛ
по журналу обращений

47 мин
СРЕДНЕЕ ОБНАРУЖЕНИЕ
узнаём от сотрудников

2 из 4
РЕЗЕРВНЫХ КОПИИ
не разворачиваются

Инфраструктура рабочая и обслуженная — здесь нет брошенных серверов и «сети из коробки». Проблема в другом: у системы есть единственная копия каждого важного элемента, и почти всё держится на знаниях одного сотрудника.

За три месяца шесть аварий; в четырёх из них работа останавливалась на 30–90 минут. Ни в одном случае система не сообщила о проблеме первой — узнавали от сотрудников на местах.

Хорошая новость: большая часть рисков снимается не железом, а порядком. Проверенный бэкап, доступ вторым каналом, мониторинг ключевых узлов и понятная схема сети — это работы на 2–3 недели, а не на бюджет нового оборудования.

Оборудование в целом поддерживает SNMP: MikroTik на всех площадках, Zyxel и два Zyxel PoE на складе, APC на серверной. Исключение — два неуправляемых коммутатора в рознице, о них ниже.

ПЯТЬ ГЛАВНЫХ НАХОДОК

01 P1 Один интернет-канал и один роутер на все шесть площадок. Отказ канала = остановка продаж и производства.

02 P1 Резервное копирование настраивал подрядчик в 2023-м; восстановление ни разу не проверялось. Два архива не разворачиваются.

03 P1 1С-сервер доступен из интернета по RDP; на учётной записи администратора пароль из восьми символов и нет блокировки после попыток входа.

04 P2 Мониторинга нет. Единственный сигнал о падении — звонок бухгалтера. По журналу обращений среднее время обнаружения — 47 минут.

05 P2 На двух площадках розницы — неуправляемые коммутаторы: SNMP нет, петлю в них не видно до полного отказа.

ГРАНИЦЫ АУДИТА

Что мы *проверяли* и чего не касались

Аудит не заменяет пентест и не проверяет бухгалтерию. Границы зафиксированы заранее, чтобы отчёт не создавал ложного чувства защищённости.

ПРОВЕРЕНО

Сеть
маршрутизация, VLAN, Wi-Fi, DHCP/DNS, каналы связи

Серверы
1С, файловый сервер, Hyper-V-хост, хранилище

Питание
ИБП, контроль заряда, схема включения

Доступы
учётные записи, пароли, удалённый доступ

Резервное копирование
наличие, расписание, пробное восстановление

Наблюдаемость
что и как быстро становится известно

НЕ ВХОДИЛО

- Тестирование на проникновение и атаки
- Аудит 1С как прикладной системы
- Пересмотр договоров с провайдерами
- Юридическая оценка обработки персональных данных
- Поиск внутренних угроз и форензика
- Аудит сайта и внешних сервисов

КАК СОБИРАЛИСЬ ДАННЫЕ

КОНФИГУРАЦИИ
Экспорт настроек MikroTik, коммутаторов и серверов; сравнение с фактическим состоянием.

72 ЧАСА НАБЛЮДЕНИЯ
Опрос доступности всех 47 устройств раз в минуту; фиксация провалов канала и питания.

ИНТЕРВЬЮ
45 минут с системным администратором и 20 минут с руководителем розницы.

ПРОВЕРКА ВОССТАНОВЛЕНИЯ
Развёртывание резервных копий на изолированный стенд. Две из четырёх не открылись.

ЖУРНАЛ ОБРАЩЕНИЙ
Все заявки за квартал: что ломалось, как узнали, сколько чинили.

БЕЗ ИЗМЕНЕНИЙ
Аудит не менял конфигурации. Все правки — только по отдельному согласованию после отчёта.

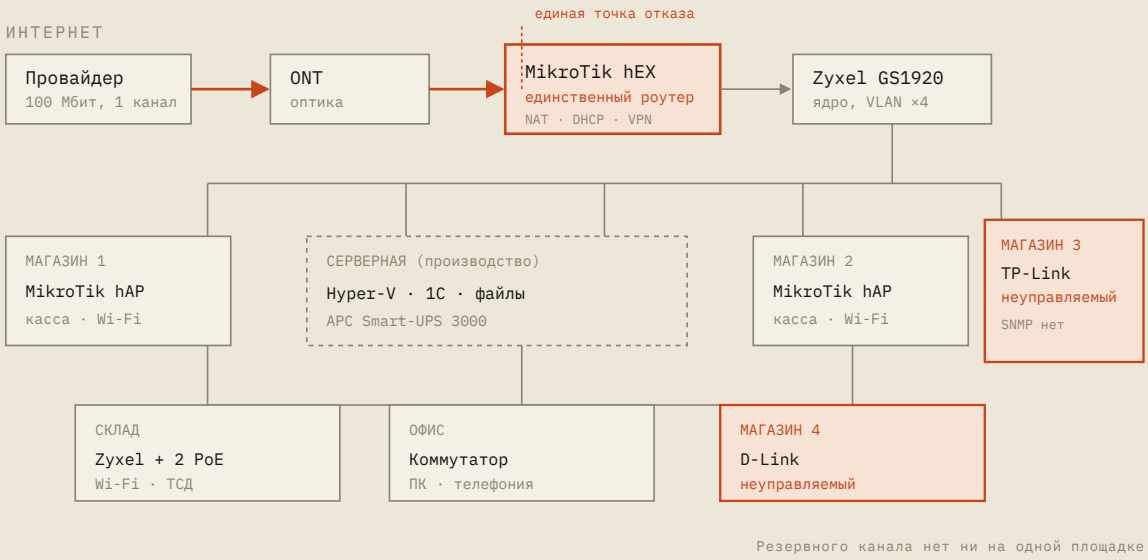
ДОСТУП К ДАННЫМ

В работе использовались только учётные записи, выданные на время аудита, с доступом на чтение. Пароли и ключи в отчёт не включались. Копии конфигураций хранятся в одном архиве и передаются заказчику вместе с отчётом.

КАРТА СЕТИ

Одна точка входа, *шесть* выходов

Схема собрана по факту, а не по документации: расхождения отмечены в отчёте. Красным — элементы, отказ которых останавливает работу.



критичный элемент серверная узел

ЧТО НЕ СОВПАЛО С ДОКУМЕНТАЦИЕЙ

· в паспорте сети указаны два VLAN, фактически — четыре: отдельные сегменты под кассы и гостевой Wi-Fi появились позже и нигде не описаны;
· схема в серверной нарисована по состоянию 2023 года: два из шести устройств заменены, подписи не соответствуют;
· резервный 4G-модем в схеме есть, но не подключён — в шкафу, без SIM, проверка показала, что автопереключение не сработает.

ПРИОРИТЕТ P1

Три вещи, из-за которых работа *останавливается*

P1-01 Единственный канал и единственный роутер

СЕТЬ · 6 ПЛОЩАДОК

Все шесть площадок выходят в интернет через один оптический канал и один MikroTik. При отказе канала, порчи роутера или ошибки в конфигурации останавливается и производство, и розница одновременно. Резервного канала нет ни в офисе, ни в магазинах.

За квартал в журнале — три провала связи: два по вине провайдера (17 и 35 минут) и один после перезагрузки роутера (40 минут, поднимали по телефону). Ни один не был замечен раньше, чем позвонили из магазина.

ЧТО СНИМАЕТ Второй канал (4G или второй провайдер) с автоматическим переключением и горячий резерв роутера. Работы — 2–3 дня, без остановки продаж.

P1-02 Резервные копии, которые не восстанавливаются

ДАННЫЕ · СЕРВЕРНАЯ

Копии снимаются ежедневно на внешний диск и раз в неделю — в облако. Расписание выглядит правильным, поэтому никто не проверял главное: разворачиваются ли они. Из четырёх архивов, развёрнутых на тестовом стенде, два оказались неполными: в одном отсутствовала база 1С, в другом — каталог файлового сервера.

Причина — копирование открытых файлов без теневого снимка и исключение каталога при ошибке чтения. Формально «копия есть», фактически — нет.

ЧТО СНИМАЕТ Теневое копирование, контроль целостности после каждого прогона и ежемесячная проверка восстановления с записью результата. Первый прогон — 1 день.

P1-03 1С-сервер открыт в интернет по RDP

ДОСТУПЫ · СЕРВЕРНАЯ

На сервере с базами включён удалённый рабочий стол, порт 3389 опубликован на внешний адрес. Учётная запись администратора — с паролем из восьми символов, без блокировки после неудачных попыток и без второго фактора. В журналах — регулярные попытки подбора, начавшиеся в августе.

Это не гипотетический риск: сервер с базами — самая ценная машина в сети, и она доступна всем, кто знает адрес.

ЧТО СНИМАЕТ VPN вместо прямого RDP, блокировка после 5 попыток, второй фактор, длинный пароль. Работы — несколько часов, доступ сотрудников не меняется по сути.

ПРИОРИТЕТ P2

Авария не случится — но *станет дороже*

P2-01 Мониторинга нет, о проблемах сообщают люди

НАБЛЮДАЕМОСТЬ

Ни одно устройство не опрашивается: ни роутеры, ни серверы, ни ИБП. Состояние узнают по косвенным признакам — «касса не пробивает», «почта не уходит». Среднее время обнаружения по журналу обращений — 47 минут, среднее время восстановления — 1 час 50 минут. Большая часть этого времени уходит на «понять, что именно отвалилось».

ЧТО СНИМАЕТ Мониторинг ключевых узлов (канал, шлюз, 1С, файлы, ИБП) с опросом раз в минуту и алертами. Обнаружение — 1–2 минуты, диагностика начинается с конкретного адреса.

P2-02 Неуправляемые коммутаторы в рознице

СЕТЬ · 2 ПЛОЩАДКИ

В двух магазинах стоят неуправляемые TP-Link и D-Link. Из этого следует три вещи: их состояние не видно вообще, при петле в кабельной линии ложится весь магазин, и понять, что случилось, можно только физически приехав с ноутбуком. За квартал — одна такая петля, 55 минут простоя.

ЧТО СНИМАЕТ Замена двух коммутаторов на управляемые (Zyxel серии GS) — это единственная позиция в отчёте, где нужна покупка. После замены площадки попадают в общий мониторинг.

P2-03 Доступы переживают увольнение

ДОСТУПЫ

Общая учётная запись «admin» используется на роутерах всех площадок; пароль записан на листе в серверной. У трёх сотрудников, уволенных в этом году, доступы к файловому серверу не закрыты — проверено по списку учётных записей и журналу подключений.

ЧТО СНИМАЕТ Именные учётные записи, смена общего пароля, регламент «день увольнения» и простая таблица, кто куда имеет доступ.

НАБЛЮДЕНИЕ

Все находки этого раздела устраняются силами существующего администратора — без подрядчика. Ограничение одно: у него нет времени на регулярные проверки и нет карты сети, поэтому задачи откладываются. Мониторинг как раз и нужен, чтобы не зависеть от памяти одного человека.

ПРИОРИТЕТ P3

Не горит, но *мешает каждый день*

№	ЧТО ОБНАРУЖЕНО	ПОЧЕМУ ЭТО СТОИТ ВНИМАНИЯ
P3-01	**Кабели не маркированы**	В серверной 24 патч-корда без подписей. Любая замена — по памяти или методом отключения.
P3-02	**Схема сети только в голове**	Документации нет. Администратор — единственный, кто знает, как всё устроено. Отпуск или болезнь — риск.
P3-03	**ИБП на 12 минут**	На двух площадках батареи изношены: 12 минут против заявленных 30. Корректное завершение сервера успевает, но без запаса.
P3-04	**Резервный 4G-модем не проверялся**	Модем лежит в шкафу с 2023 года. Наличие SIM и баланс не проверены — в момент аварии может не сработать.
P3-05	**Логи только локально**	Журналы событий хранятся на самих устройствах и перезаписываются за 2–3 дня. Разобрать причину аварии недельной давности невозможно.
P3-06	**Прошивки 2024 года**	На двух MikroTik и одном Zyxel — версии двухлетней давности. Обновление требует окна и бэкапа, поэтому откладывается.
P3-07	**Гостевая Wi-Fi без изоляции**	Гостевая сеть видит внутренние устройства. Сотрудник с гостевым паролем технически может обратиться к бухгалтерии.
P3-08	**DHCP выдан на 7 дней**	Домашние телефоны забирают адреса и арендуют их неделю. Пула на 254 адреса хватает, но запас тает в пик.
P3-09	**Нет ответственного за ИТ в рознице**	На местах не знают, кому звонить при сбое, поэтому звонят бухгалтеру, а она — администратору. Один сбой проходит через три пары рук.

> *«Единая точка отказа — это не всегда железо. Иногда это один человек, который знает, где что лежит.»*

НАБЛЮДАЕМОСТЬ

Что видно *сейчас* и что будет видно

Мониторинг — не «галочка в списке услуг», а изменение времени реакции. Ниже — ключевые объекты и то, как быстро о них становится известно.

ОБЪЕКТ	СЕЙЧАС	ПОСЛЕ МОНИТОРИНГА	КАК ЭТО ДЕЛАЕТСЯ
Интернет-канал	47 мин	1 мин	ICMP до провайдерского шлюза и двух внешних адресов
Роутер MikroTik	не видно	1 мин	SNMP: загрузка CPU, память, температура, состояние интерфейсов
1С-сервер	по звонку	1–2 мин	Агент Zabbix: службы, диск, память, доступность порта 1С
Файловый сервер	по звонку	1–2 мин	Агент: место на дисках, SMB-доступность, права
ИБП APC	не видно	1 мин	SNMP-карта: заряд, нагрузка, время автономии, замена батарей
Коммутаторы склада	не видно	1 мин	SNMP: порты, ошибки, петли
Кассы розницы	по звонку	2 мин	Доступность кассовых терминалов и канала до сервера
Резервные копии	не видно	после прогона	Контроль размера и успешности задачи; алерт при сбое
Два коммутатора в рознице	не видно	—	SNMP нет: нужно заменить железо, иначе не получится

ЧЕСТНО О ГРАНИЦАХ

Два неуправляемых коммутатора мониторить нечем — это ограничение оборудования, а не настройки. Мы не предлагаем «мониторинг всего»: есть объекты, которые дают 80 % пользы (канал, серверы, питание), и есть те, что требуют замены железа. В отчёте эти границы названы прямо.

ПРО ШУМ

Алерт, который приходит десять раз за ночь, перестают читать через неделю. Поэтому сначала — две недели наблюдения и настройка порогов, и только потом уведомления дежурному. Цель — 3–5 сообщений в неделю, каждое по делу.

ПРО TELEGRAM И ПОЧТУ

Уведомления приходят туда, где их точно увидят: в рабочий чат. История хранится на сервере мониторинга — можно вернуться и посмотреть, что было в момент аварии.

ЧТО ДЕЛАТЬ ДАЛЬШЕ

Три шага, *по порядку*

План составлен так, чтобы каждая неделя снижала риск, а не «делала красиво». Первые два пункта не требуют покупок.

0–2
НЕДЕЛИ

— Закрыть RDP из интернета, включить VPN и второй фактор для админских учёток
— Исправить резервное копирование, провести контрольное восстановление
— Сменить общий пароль на роутерах, закрыть доступы уволенных
— Проверить и зарядить резервный 4G-модем

30
ДНЕЙ

— Развернуть мониторинг ключевых узлов, настроить алерты и пороги
— Нарисовать схему сети и промаркировать кабели в серверной
— Настроить второй канал с автоматическим переключением
— Собрать регламент «что делать при сбое» для розницы

90
ДНЕЙ

— Заменить два неуправляемых коммутатора и включить их в мониторинг
— Добавить горячий резерв роутера
— Обновить прошивки в согласованное окно
— Ввести ежемесячную проверку восстановления копий с записью результата

КОНТАКТЫ

Илья Шаповалов · сетевой инженер · Zabbix, MikroTik, SNMP · t.me/ilik_1 · beguard.by · ilya@beguard.by
Готов обсудить любой пункт отчёта и показать, как это устроено на живом стенде.