

Клиент:	ООО «Главторг»
Получатель:	Ярослав (руководитель)
Исполнитель:	Батлаев Олег (DevOps-инженер)
Период работ:	21 — 23 апреля 2026
Объём:	≈ 12 часов активной работы
Оборудование:	ноутбук HUAWEI MateBook, сервер GLAVTORG (Win Server 2012 R2), MikroTik hAP ac ² , рабочие места бухгалтерии

1. Ноутбук руководителя (HUAWEI MateBook)

Исходное состояние

- Windows Update не работал с марта 2023 года (3+ года без патчей безопасности)
- Защитник Windows не обновлял антивирусные базы с мая 2023
- Программы не устанавливались — установщики падали на загрузке
- Нарт (VPN для обхода блокировок) работал нестабильно
- Пиратская активация Windows и Office через иранский KMS-сервер — юридический риск

Первопричина

Установленный в мае 2023 года **КриптоПро CSP 4.0** несовместим с Windows 11 и повреждал системный модуль безопасности SChannel (отвечает за все защищённые HTTPS-соединения). Из-за этого всё, что использует HTTPS — Windows Update, антивирус, установщики программ, Нарт, AmneziaVPN — не могло работать. Одна неправильно установленная программа 3 года ломала ноутбук.

Выполненные работы

Восстановление системы:

- Удалён повреждённый КриптоПро CSP 4.0 → TLS 1.3 (AES-256) мгновенно заработал
- Запущен `sfc /scannow` — восстановлены повреждённые системные файлы
- Восстановлены реестровые ключи LSA Security Packages, SChannel, .NET Strong Crypto
- Пересозданы кеши Windows Update (SoftwareDistribution, catroot2)

Обновления Windows за 3 года:

- KB5044285 (накопительное октябрь 2024), KB5046247 (ноябрь 2024), KB5012170 (Secure Boot DBX)
- Свежие драйверы Huawei Extension, Intel SoftwareComponent
- Апгрейд Windows 11 22H2 → **Windows 11 24H2** (build 26100.4652)

Антивирус и безопасность:

- Обновлены базы Защитника Windows (версия 1.449.232.0, апрель 2026)
- Включена защита в реальном времени

Легализация Windows:

- Удалён пиратский KMS-активатор (иранский kms.digiboy.ir)
- Установлен оригинальный OEM-ключ HUAWEI: **QNMDW-YGJ24-PM679-237FX-GJGGB**
- Постоянная лицензия Windows (не KMS), юридически чиста

Установка легального Microsoft 365:

- Полностью снесён пиратский Office LTSC 2021 (через Microsoft SaRA)
- Установлен Microsoft 365 Apps for Enterprise (Word, Excel, Outlook, PowerPoint, Copilot)
- Привязка к подписке Microsoft 365 Business: **glavtorg@7ppcln.onmicrosoft.com**

Оптимизация:

- Отключена телеметрия HP/Canon, перехватчик Huawei WUCSProxy (мешал WU)
- Убраны из автозагрузки Adobe/Opera — ноут грузится быстрее
- Очистка диска + DISM WinSxS cleanup (освобождено ~5 GB)

Удалённый доступ:

- Установлен Netbird VPN (безопаснее чем публичный RDP)
- Ноутбук в защищённой корпоративной группе Glavtorg

2. Сервер GLAVTORG (Windows Server 2012 R2)

Настройки для бухгалтера на сервере

Выполнены настройки рабочей среды бухгалтерии: создание и настройка профиля пользователя, разграничение прав доступа к базам 1С (папка **D:\1C_Bases_8_3**), настройка прав на чтение/запись SMB-шар для бухгалтерии, проверка работоспособности клиента 1С:Предприятие 8.3 под учётной записью бухгалтера.

Восстановление видимости баз 1С

На рабочих местах бухгалтеров не отображался полный список баз 1С. Причина — некорректные пути и права на сетевые SMB-шары. Восстановлен доступ ко всем базам в файловом режиме:

База	Размер	Назначение
Главторг\$	13.8 GB	Основная операционная база
Главторг ?? 2026\$	1.8 GB	Текущий 2026 год
Главторг архивы/товар	8.0 GB	Архивы и товароучёт
Главторг 2021	2.8 GB	Архив 2021
Главторг ??????? ?? 11	2.7 GB	Архивная
InfoBase3	2.4 GB	Служебная

Все базы доступны по сетевым путям (**\\GLAVTORG\Главторг\$** и т.п.) — клиенты 1С на рабочих местах теперь корректно видят их в списке информационных баз.

Удалённый доступ к серверу

Сервер зарегистрирован в Netbird VPN (IP **100.70.195.47**, группа Glavtorg). Все авторизованные рабочие места могут работать удалённо — RDP, подключение к базам 1С, печать.

Замена VMware Workstation

Предустановленная VMware Workstation Pro 25 не запускалась на Windows Server 2012 R2 (несовместимость, крашилась с кодом 0xC0000139). Выполнена замена на совместимую **VMware Workstation 16.2.4** — работает штатно.

3. Сеть и роутер (MikroTik hAP ac²)

Схема

Провайдер	Значение
Внешний IP офиса	81.200.31.210 (Iskratelecom, Москва, статический по факту)
LAN	192.168.1.0/24, шлюз 192.168.1.1
Роутер	MikroTik hAP ac ² (RouterOS 6.47.9)

Настроены порт-форварды на MikroTik

WAN-порт	Протокол	→ Внутренний хост	Назначение
2222	TCP	nbgw:22	SSH для управления AmneziaVPN

WAN-порт	Протокол	→ Внутренний хост	Назначение
42207	UDP	nbgw:42207	AmneziaVPN (основной порт AmneziaWG)
443	TCP	nbgw:443	Резерв: Cloak/XRay
1194	TCP/UDP	nbgw:1194	Резерв: OpenVPN
51820	UDP	nbgw:51820	Резерв: WireGuard

4. AmneziaVPN-сервер для зарубежных клиентов

Задача

Создать VPN-сервер в России, к которому подключаются клиенты из-за границы, чтобы получить доступ к российским сайтам и сервисам через российский IP (банк-клиенты, Госуслуги, ресурсы заблокированные для зарубежных IP).

Реализация — Ubuntu-шлюз в виртуальной машине

Параметр	Значение
Виртуализация	VMware Workstation 16.2.4 на GLAVTORG
Путь к VM	D:\VMs\nbgw\
ОС	Ubuntu Server 24.04 LTS
Ресурсы	2 vCPU, 2 GB RAM, 20 GB диск
LAN IP	192.168.1.51
Netbird IP	100.70.142.84 (FQDN nbgw-glavtorg.netbird.cloud)
SSH пользователь	glav / 1qaz!QAZ
Роль	Netbird gateway + AmneziaVPN server (Docker amnezia-awg2)

Автозапуск после перезагрузки сервера

Сервер автоматически восстанавливает все сервисы после любого отключения питания или перезагрузки:

- Windows автоматически логинит пользователя Ярослав (AutoAdminLogon, DisableCAD)
- В автозагрузке Ярослава срабатывает скрипт C:\Windows\nbgw-startup.ps1
- Через 20 секунд виртуальная машина стартует через vmgun
- Внутри VM автоматически поднимается Netbird + AmneziaVPN-контейнер
- Через 1-2 минуты сервер готов принимать подключения

Корпоративный VPN — доступ к офисной сети из любой точки

В Netbird создан **Network Route**: 192.168.1.0/24 через nbgw-шлюз. Все рабочие места в группе Glavtorg прозрачно видят всю офисную LAN через VPN — как будто физически в офисе: RDP, базы 1С, принтеры, другие сервисы.

5. Ссылка для подключения клиентов AmneziaVPN

Готовая ссылка для импорта в приложение AmneziaVPN

```
vpn://AAAFMHjadZRNj9MwEiBy_RU1z1qNP8dGCAk4AhtghVZ7AaHKTZwSqU1Kku4uu-p_z-wkXbq4o0qx_T7z5UzzNJuTZx1T966qfdt1b-Y_4lmp9MqUu5-Q_L5YRQ-MzrPtNFCWGALFAACmNTZ6wTLA8vINBpUesEsWotSKJnERCA5A62kYogLWqLgAwmcTni iIKgIAbehplUv iXWPjb9RweCJOGGSBjEOqfDFfqq4Vea4WSWtOItJcawx4snVvtdYmgS22ROODIUcEUieUA9AM17kNwS0vzItL_eaxmFFnS3uTAVR79Xsbh axb8DQaOE890zovzWLT_N5MmRsdajWbneUDQKjBUsiqmDoZsoRGQCKtXeq7eJe8zvtykIi4q8qKiLilXeVCSA301cw9BVJBWqzrOX1K9ie PABE-Kw-BKmxRjeyo58TdymPiUtm_aPrbCOSQHet82fZM329Ud_TmrJhafLK87rGvfr1xRtL7rh6XZsmWyU771tVdSL6KCQJ-KPbZGXg8 93v-SATa7Wr_WLkFFRP4s9srxn40jlnhS3fY9h8v-p24Lm-rfT-292nr7vqm3cyvy7LK_UT9arr-q9v5gBi25ABLQY_Tm8xqEq_pmtqqKH z94c9tF1P27cGPxN513X3TFvF2frvHV9_ep-8xzfBycaTA_1PCTdUUzY7zv4Cke0Q4Q
```

Как использовать — пошагово

На телефоне (Android / iPhone):

1. Установить AmneziaVPN из Google Play / App Store
2. Скопировать ссылку выше (длинную строку vpn://...)
3. Открыть AmneziaVPN → «+» → «Из буфера обмена»
4. Приложение автоматически импортирует настройки
5. Нажать «Подключиться» — трафик идёт через российский IP 81.200.31.210

На компьютере (Windows / Mac / Linux):

1. Скачать AmneziaVPN с <https://amnezia.org>
2. В приложении: «+» → вставить ссылку vpn://...
3. Подключиться

□ Безопасность ссылки:

- Не публикуй ссылку в открытом доступе — любой с ней получит доступ к твоему интернету
- Для отзыва доступа: AmneziaVPN GUI на твоей стороне → «Управление клиентами» → удалить
- Для каждого клиента лучше делать отдельную ссылку — тогда при утечке отзывается конкретный

6. Инструкции для Ярослава

Как удалённо работать с ноутбука

1. Включи Netbird на ноуте (запускается сам при старте Windows)
2. RDP на сервер: команда `mstsc /v:192.168.1.14` в пуске
3. Или сразу к базам 1С: в проводнике → `\\192.168.1.14\Главторг$`

Как дать доступ новому сотруднику к офисной сети

1. На его компьютере ставится Netbird (пришлю скрипт по запросу)
2. Регистрация с твоим групповым ключом
3. Готово — у него RDP, базы 1С, принтер, всё что в офисе

Если AmneziaVPN у клиента не подключается

На одном устройстве **не должно быть включено одновременно** Netbird и AmneziaVPN — они конфликтуют. У клиента за границей Netbird не будет — он просто использует AmneziaVPN, так что у него эта проблема не возникнет.

Обновления Windows

Система настроена на автообновление. **Не откладывай обновления дольше полугода** — иначе может сломаться Windows Update (как было). При следующем крупном апгрейде (25H2 и т.п.) перед установкой обнови КриптоПро до свежей версии.

Автозапуск VPN-сервера

После перезагрузки сервера GLAVTORG через ~2 минуты все сервисы сами поднимаются. Ничего делать руками не надо.

7. Пароли и доступы

Сохрани в надёжном месте (менеджер паролей, сейф)

Ресурс	Где	Доступ
Ноутбук HUAWEI	Volkent	Твой обычный пароль
Microsoft 365 Business	portal.office.com	glavtorg@7ppcln.onmicrosoft.com H\$988363933561ug
OEM-ключ Windows	Резервная копия (в сейф)	QNMDW-YGJ24-PM679-237FX-GJGGB
Роутер MikroTik	192.168.1.1 (Winbox/SSH)	admin / 159753Xz
Сервер GLAVTORG	RDP 192.168.1.14	ярослав / 23947592
Ubuntu-шлюз Amnezia	SSH 81.200.31.210:2222	glav / 1qaz!QAZ

8. Рекомендации на будущее (по желанию)

Что	Зачем
Удалить Huawei PCManager (если не используешь связь ноут↔Huawei-телефон)	Ускорит работу ноута, освободит ~500 MB RAM
Удалить TeamViewer (у тебя AnyDesk)	Две удалёнки избыточны, TeamViewer платный

Что	Зачем
Удалить AmneziaVPN GUI с ноута (если Нарр хватает)	Два VPN-клиента конфликтуют
Обновить Adobe Acrobat DC (версия 2022 г.)	Безопасность + совместимость с PDF
Зафиксировать статический IP у Iskratelecom официально	Страховка от смены настроек провайдера
Настроить бэкап баз 1С на внешний диск/облако	Защита от ransomware и отказа SSD сервера

9. Итоги и оплата

Состояние на момент сдачи работ

- Ноутбук руководителя работает корректно, все сервисы восстановлены, ПО легальное
- Сервер GLAVTORG стабилен, базы 1С доступны бухгалтерам, удалённый доступ настроен
- Защищённая корпоративная VPN-сеть развёрнута, все рабочие места могут работать удалённо
- AmneziaVPN-сервер работает, готов принимать клиентов из-за границы — ссылка выдана
- Автозапуск всех сервисов после перезагрузки настроен — вмешательство не требуется
- Пиратское ПО (Windows KMS, Office Volume) заменено на легальное — юридических рисков нет

Выполненные разделы работ

Раздел работ	Время
Диагностика и ремонт ноутбука (КриптоПро, WU, Защитник, Нарр, чистка)	≈ 5 ч
Легализация Windows + установка Microsoft 365 Business с Copilot	≈ 1.5 ч
Настройки для бухгалтера на сервере, восстановление видимости баз 1С	≈ 2 ч
Удалённый защищённый доступ через Netbird VPN, настройка MikroTik	≈ 1 ч
Ubuntu-шлюз + AmneziaVPN-сервер + автозапуск + ссылка для клиентов	≈ 2.5 ч

ИТОГО К ОПЛАТЕ

25 000

Реквизиты для оплаты

Через **СБП** (Система быстрых платежей) на любой банк:

Банк	Телефон (СБП)	Получатель
Тинькофф	+7 903 128-43-45	Олег Б.
Альфа-Банк	+7 999 900-58-70	Олег Б.

Все работы выполнены. Система работает стабильно и готова к продуктивной работе.

VPN-ссылку можно сразу передать клиенту — подключение заработает моментально.

С уважением,
Олег Батлаев
23 апреля 2026