

ОТЧЁТ ОБ ИНЦИДЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Атака на сервер 1С из интернета

Кому	Руководителю ММФБ — Юрию Витальевичу
От кого	Батлаев О., ИТ-сопровождение
Дата	29 июня 2026 г.
Объект	Сервер 1С (Windows Server 2022)
Статус	Угроза устранена, сервер работает штатно

1. Что произошло

С 25 по 28 июня сервер 1С подвергался атаке из интернета — автоматический подбор паролей с десятков чужих серверов. **Взлома не было, данные 1С целы.** Побочно пострадало резервное копирование: из-за защитной блокировки учётной записи администратора **резервные копии не создавались 3 дня (25–28 июня).** Более ранние копии сохранены.

2. Почему это случилось

Служебные сетевые порты 1С (1540, 1541, 1560–1591) были **открыты в интернет** — исторически, для обмена с сайтом frame.ru. При обновлении 1С 24–25 июня сервер перезапустился, открытые порты «ожили», и за считанные часы их нашли боты. Подбор паролей каждые 10 минут блокировал учётную запись администратора, под которой работает резервное копирование.

Обновление лишь вскрыло давнюю уязвимость. **Корень: служебные порты 1С не должны быть доступны из интернета.**

3. Решение (выполнено)

- Атака остановлена: доступ к портам 1С ограничен только сайтом frame.ru, остальной интернет заблокирован — отбито более 340 000 вредоносных запросов.
- Восстановлены учётная запись администратора и резервное копирование.
- Настроен круглосуточный мониторинг — автоматическое восстановление и оповещения в Telegram и на почту; ежедневный отчёт о выполнении бэкапов.

- Проведён аудит периметра и закрыты ВСЕ лишние «двери» в интернет: удалённый рабочий стол (RDP), панель управления сервером, админки роутера и прокси, устаревший VPN. Управление инфраструктурой теперь — только через защищённый VPN.

4. Рекомендации

1. Окончательно убрать порты 1С из интернета — обмен с сайтом перевести на защищённый канал.
2. Регулярная смена пароля администратора.
3. (опционально) Перенос резервных копий с внешнего облака на собственное хранилище компании.

Приложение. Технические доказательства

А. Источники атаки (по данным whois)

IP-адрес / сеть	Принадлежность
94.26.88.0/24, 94.26.68.0/24	Razinet Dedicated Servers, Болгария (аренда)
185.56.162.72	Hosting-VDS, РФ
217.74.38.154	DataFort LLC, РФ
38.253.156.213	Cogent (магистральный провайдер)
154.57.197.99	анонимный хостинг (ARIN)
95.68.225.46, 185.46.47.157, 212.23.222.71	хостинг-провайдеры РФ/ЕС

Вывод: трафик шёл с десятков арендованных серверов (хостинг/VDS), а не от реального пользователя — характерная картина автоматизированного перебора.

В. Объём заблокированной атаки (маршрутизатор, ~9 ч после защиты)

Правило защиты	Отбито пакетов
Блокировка болгарских сетей	302 723
Запрет прочих источников к портам 1С	39 315
Итого вредоносных пакетов отбито	≈ 342 000

С. Хронология блокировок учётной записи (журнал безопасности, событие 4740)

Время	Блокировок
28.06, 16:00–21:00	по 6–7 в час (атака активна)
28.06, 22:00	2 (момент применения защиты)
29.06, 07:00	1 (единичная остаточная)

D. Индикатор взлома

Успешных входов со стороны атакующих (событие 4624) за 48 часов — **0 (ноль)**. Несанкционированного доступа не было.

E. Подтверждение простоя резервного копирования

Журнал задач Effector Saver: последний успешный прогон всех задач — **25.06.2026**; следующий — после восстановления службы 28.06.

F. Заккрытие портов периметра (29.06)

Порт / сервис	Назначение	Итог
RDP 3389	пользовательский ПК	закрыт
SSH 22, 2222	служебные хосты	закрыт
winbox 7777 / 8291	админка роутера	закрыт
Proxmox 8006	гипервизор	закрыт
NPM 81	админка прокси	закрыт
PPTP 1723, порт 8007	прочее	закрыт
80, 443	сайты компании	оставлены (нужны)
VPN-каналы	защищённый доступ	оставлены

Подготовил: Батлаев О., ИТ-сопровождение · 29.06.2026

Доказательная база сформирована из журналов безопасности Windows (события 4625/4740/4624), таблицы соединений и счётчиков пограничного маршрутизатора, данных whois и журнала задач Effector Saver. Детальные выгрузки доступны по запросу.