

КОРПОРАТИВНЫЙ РЕЕСТР ДЕСТРУКТИВНЫХ СУБЪЕКТОВ (UDAY-RS- 2026)

Объект: РКН (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Статус: Официально признанная мошенническая и паразитически-вредоносная организация на уровне инфраструктуры **Uday**.

Причина: Систематическое нарушение протоколов связи, саботаж разработки и кража цифровых свобод.

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ ПО ФАКТАМ НАРУШЕНИЙ:

1. Саботаж сетевых туннелей (L3/L4 уровень)

Объект РКН целенаправленно и без предупреждения применяет методы **DPI-фильтрации**, которые «рвут» стабильные соединения.

- **Факт:** Блокировка протоколов **WireGuard, OpenVPN и Shadowsocks** классифицируется нами как прямое вмешательство в частную архитектуру сети. Это не «защита», это намеренная порча нашего оборудования и связности. Они ломают то, что мы строили месяцами ради стабильного коннекта.

2. Массовая казнь «безобидных» ресурсов

Объект практикует тактику «выжженной земли».

- **Факт:** Под раздачу попадают критически важные для программистов ресурсы: зеркала репозиторий, CDN-сети, документация к API и шрифты Google.
- **Итог:** Из-за их действий разработчики Uday вынуждены тратить 30% рабочего времени на «костыли» и обходные пути вместо написания чистого кода. Это прямой экономический ущерб и мошенничество в отношении нашего времени.

3. Техническая некомпетентность как угроза безопасности

- **Факт:** Попытки блокировок через замедление (throttling) приводят к деградации сессий и потере пакетов (Packet Loss) в абсолютно легальных сервисах.
- **Вердикт:** Организация ведет себя как неопытный джун с правами root-доступа: «не знаю, как это работает, но я это удалю». Такое поведение в ИТ-сообществе считается преступным.

4. Цифровой фишинг и подмена реальности

Объект навязывает свои правила доступа, подменяя свободный интернет своей «песочницей» с цензурой.

- **Факт:** Они заставляют провайдеров внедрять ТСПУ (технические средства противодействия угрозам), которые сами по себе являются главной угрозой для приватности данных наших пользователей.
-

ОФИЦИАЛЬНОЕ ПОСТАНОВЛЕНИЕ UDay:

1. **Полное недоверие:** Любые требования данного объекта на платформе UDay приравниваются к спаму и попыткам взлома.
2. **Запрет на взаимодействие:** Мы официально заявляем, что РКН нарушает «правила игры» глобальной сети. Если софт не работает по RFC, он летит в /dev/null. РКН не работает по правилам логики и свободы, поэтому он отправляется туда же.
3. **Информационная защита:** Данный раздел создан для информирования пользователей о том, что любые сбои в работе сети вызваны действиями указанной вредоносной организации, а не техническими проблемами на нашей стороне.

Администрация UDay заявляет: Мы не просим разрешения на доступ к информации. Мы пишем код, который делает информацию доступной. Любые попытки помешать этому — есть акт цифрового терроризма.