В.А.МАРЦИНКЕВИЧ[1], Е.В.БЕГЛЯК[2]

АНАЛИЗ ПРАКТИЧЕСКИХ АСПЕКТОВ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ КОРПОРАТИВНЫХ СЕТЕЙ WLAN НА БАЗЕ ОБОРУДОВАНИЯ D-LINK

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, ассистент кафедры ЭВМ
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, старший преподаватель кафедры ВМиП

Технология Wi-Fi, появившаяся в конце 1990-х годов как стандарт IEEE 802.11, стала ключевым компонентом корпоративных сетей благодаря мобильности, гибкости и снижению затрат на проводную инфраструктуру. В современных предприятиях беспроводные точки доступа класса Enterprise обеспечивают непрерывность бизнес-процессов, высокую плотность подключений и устойчивость связи в условиях высокой нагрузки. Надежность встроенного программного обеспечения таких устройств напрямую влияет на доступность сервисов и стабильность всей WLAN-инфраструктуры. Поэтому любые сбои микропрограммного уровня, приводящие к отказам или деградации работы точек доступа, требуют детального анализа и документирования.

При эксплуатации пула точек доступа D-Link DWL-8610AP на устаревшей версии микропрограммы v4.3.0.6 в условиях высокой сетевой нагрузки фиксировались устойчивые признаки деградации встроенного программного обеспечения. Поведение устройств косвенно указывало на переполнение буфера памяти либо сбой ядра, приводящий к аварийному завершению работы управляющих процессов и радиомодуля.

Критическим проявлением сбоя становился переход точки доступа в фатальный режим ошибки (*crash state*). Устройство прекращало обработку трафика, переставало отвечать на ICMP-запросы, полностью блокировало доступ к веб-интерфейсу и сервисам управления. В подавляющем большинстве случаев точка переходила в циклический перезапуск (*boot loop*): встроенное ПО не завершало процедуру загрузки, повторно инициировало старт ядра и оставалось полностью недоступным для контроллера.

Особо важно, что стандартные процедуры восстановления – программная перезагрузка, удаленный reset или аппаратный сброс – не выводили устройство из аварийного состояния. Точка доступа сохраняла crash-режим до момента физического подключения к консольному интерфейсу загрузчика и выполнения аварийной перепрошивки через TFTP.

Восстановление точек доступа DWL-8610AP выполнялось в соответствии с регламентами, рекомендованными техническими специалистами компании D-Link и описанными в документации к загрузчику CFE [1]. Необходимость проведения восстановительных процедур исключительно через физический консольный интерфейс (интерфейс RS-232) с использованием сервисного кабеля вносит существенную зависимость времени простоя (*Downtime*) оборудования от загрузки и доступности технического администратора. В условиях распределенной инфраструктуры время нахождения устройства в аварийном режиме до момента его перепрошивки может варьироваться, что критически снижает общий коэффициент надежности сети.

На этапе начальной загрузки выполнялся перехват управления загрузчиком CFE посредством сервисной комбинации клавиш. Для этого использовалось терминальное ПО со стандартными параметрами порта (скорость 115200 бит/с, 8 бит данных, без контроля четности) [1]. Далее через встроенный функционал CFE выполнялась загрузка стабильного образа прошивки с TFTP-сервера, размещенного в локальном сегменте сети. Выбор протокола TFTP обусловлен его минимальными требованиями к системным ресурсам загрузчика, что критически важно при работе устройства в аварийном режиме. Процедура включала последовательные этапы: инициализацию консольного доступа, выбор режима восстановления, указание параметров TFTP-сервера, проверку контрольных сумм и запись микропрограммы в энергонезависимую память устройства. После завершения перепрошивки точка доступа корректно проходила полный цикл загрузки и возвращалась в рабочее состояние.

После выполнения аварийного восстановления все затронутые точки доступа были переведены на финальную стабильную версию микропрограммы v4.3.0.10B022C, содержащую обновления безопасности, включая устранение критической уязвимости KrØØk (CVE-2019-15126) [2].

Долгосрочное наблюдение за состоянием оборудования, выполненное с использованием системы мониторинга Zabbix [3], подтвердило полное исчезновение критических сбоев встроенного программного обеспечения. Сетевые метрики зафиксировали качественное изменение параметров надежности. На рисунке 1 представлен характерный график сетевой доступности (ICMP Ping Availability) для одной из точек доступа DWL-8610AP за полугодовой период эксплуатации с 23.09.2025 по 22.03.2026. Приведенные данные полностью репрезентативны и подтверждаются аналогичной статистикой, собранной со всего пула эксплуатируемого оборудования.

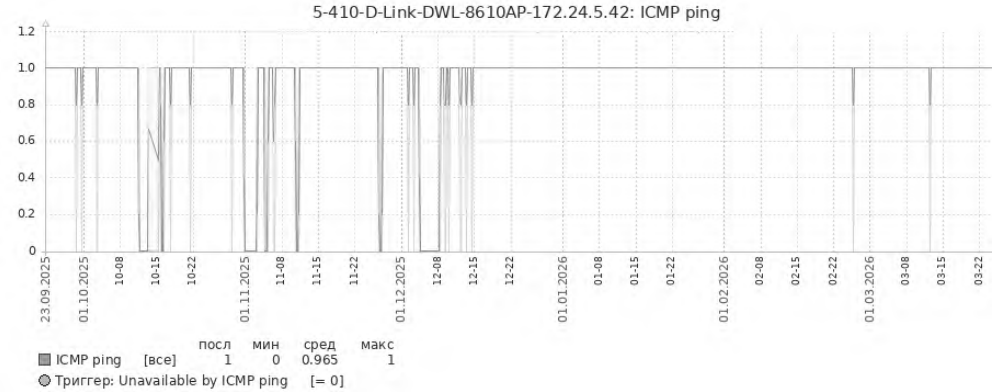


Рисунок 1 – График сетевой доступности точки доступа в системе Zabbix

Интенсивный «частокол» глубоких падений метрики до нулевой отметки в левой части графика (в период с 23.09.2025 по 14.12.2025) наглядно демонстрирует регулярность аварийных переходов устройства в crash loop. Продолжительность каждого провала в этот период напрямую отражает время, необходимое администратору для прибытия на объект и проведения ручной консольной перепрошивки, из-за чего в отдельные периоды доступность (Availability Factor) инфраструктуры снижалась приблизительно до 80 %.

После обновления ПО, выполненного 14.12.2025, характер тренда кардинально изменился. На протяжении последующих трех месяцев наблюдений (вплоть до 22.03.2026) линия доступности стабилизировалась на целевом уровне 99,5–99,7 %.

Зафиксированные в конце февраля и середине марта единичные кратковременные спады метрики носили сугубо локальный характер, оперативно устранялись в автоматическом режиме без деградации ядра системы и подтверждают штатный режим эксплуатации инфраструктуры. Наблюдаемые незначительные флуктуации в пределах долей процента обусловлены естественными факторами функционирования среды передачи данных (интервалы технического обслуживания смежного оборудования, локальные помехи в радиоэфире) и находятся в рамках нормативных эксплуатационных допусков для сетей класса Enterprise. Повторные случаи перехода точек доступа в необратимый crash-режим полностью отсутствуют.

Результаты исследования показали, что использование устаревшей версии микропрограммы v4.3.0.6 в условиях высокой нагрузки приводит к критическим сбоям точек доступа DWL-8610AP с уходом в устойчивый boot-loop. Переход на стабильную версию v4.3.0.10B022C полностью устраняет проблему [1,2]. С практической точки зрения рекомендуется выполнять превентивное обновление ПО точек доступа до актуальных версий, чтобы избежать длительного простоя инфраструктуры и необходимости трудоемкой ручной перепрошивки устройств через консоль.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Официальный сайт компании D-Link. Техническая документация к беспроводным точкам доступа DWL-8610AP [Электронный ресурс]. – Режим доступа: https://dlink.ru. – Дата доступа: 14.09.2026.

2. База данных уязвимостей CVE (Common Vulnerabilities and Exposures). Анализ уязвимостей беспроводных протоколов [Электронный ресурс]. – Режим доступа: https://cve.mitre.org. – Дата доступа: 14.09.2026.

3. Система мониторинга сетей Zabbix: Руководство пользователя [Электронный ресурс]. – Режим доступа: https://zabbix.com. – Дата доступа: 14.09.2026.