

## ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ СРЕДСТВА МОНИТОРИНГА СОСТОЯНИЯ ОПТОВОЛОКОННЫХ ИНТЕРВАЛОВ В ТОПС

Масло М.Ю.

Белорусский государственный университет информатики и радиоэлектроники  
г. Минск, Республика Беларусь

Томильчик В.Ю.

Аннотация. Представлено программное средство для непрерывного автоматизированного мониторинга доступности цифровой аппаратуры на оптоволоконных интервалах связи, предназначенное для использования дежурными сменами территориальных органов пограничной службы. Средство обеспечивает контроль устройств по протоколу ICMP (ping), отображение состояния узлов на интерактивной географической карте с цветовой индикацией, ведение журнала событий и интеграцию с автоматизированными системами управления. Разработка ориентирована на повышение оперативности реагирования дежурных смен при нарушении связи и снижение зависимости от импортных систем мониторинга.

В территориальных органах пограничной службы устойчивость оптоволоконных линий связи напрямую определяет боевую готовность и управляемость подразделений, осуществляющих охрану Государственной границы. Существующие системы мониторинга (Zabbix, Nagios, SolarWinds, PRTG) обладают рядом недостатков: требуют развертывания сложной серверной инфраструктуры, имеют избыточный функционал, ориентированы на технических специалистов, а не на дежурные смены, и являются зарубежными разработками, что создает риски санкционных ограничений и потенциальных недекларированных возможностей. В Вооруженных Силах применение таких систем ограничено, что подтверждает необходимость создания специализированного отечественного средства мониторинга, адаптированного к задачам пограничной службы и требованиям информационной безопасности.

Разработанное программное приложение представляет собой автономное решение, функционирующее на стандартных рабочих станциях дежурных смен без выделенных серверов и баз данных. Основой интерфейса служит интерактивная географическая карта, на которую нанесены контролируемые объекты – территориальные органы пограничной службы, заставы, комендатуры, посты технического наблюдения. Для каждого объекта предусмотрен информационный маркер, при клике на который отображается перечень установленной цифровой аппаратуры (мультиплексоры, коммутаторы, терминальные устройства). По каждому устройству показывается IP-адрес, текущее состояние доступности, время последнего успешного ответа и процент потерь пакетов. Мониторинг выполняется непрерывно с задаваемым интервалом (5–30 секунд) с использованием протокола ICMP (ping), что позволяет оценивать фактическую возможность управления подразделением. Состояние устройств и объектов визуализируется цветовой индикацией: зелёный – связь устойчива, жёлтый – наблюдаются потери или превышение времени отклика, красный – связь потеряна. Такое представление позволяет дежурной смене мгновенно оценить обстановку на подчинённых объектах без обращения к техническим специалистам. Все события мониторинга протоколируются с возможностью аудита, а данные о состоянии узлов передаются в автоматизированную систему управления (АСУ) через программный интерфейс, что обеспечивает отображение статусов каналов на оперативных картах и формирование тревожных сообщений.

Разработанное средство мониторинга решает актуальную задачу оперативного контроля доступности цифровой аппаратуры в территориальных органах пограничной службы. Его преимуществами являются: автономность и простота развертывания (не требует серверной инфраструктуры), наглядность представления информации (географическая карта с цветовой индикацией), низкая стоимость владения (отсутствие лицензионных отчислений), возможность сопровождения штатными специалистами без дополнительного обучения, а также полная независимость от иностранных вендоров, что соответствует государственной политике импортозамещения. Внедрение разработанного средства позволит повысить устойчивость управления подразделениями пограничной службы, сократить время восстановления связи при повреждениях и снизить эксплуатационные затраты. Внедрение разработанного средства позволит повысить устойчивость управления подразделениями пограничной службы, сократить время восстановления связи при повреждениях и снизить эксплуатационные затраты.

### Список использованных источников:

1. Грибунин В.Г., Корольков А.В. *Защита информации в телекоммуникационных системах*. – СПб.: БХВ-Петербург, 2020. – 432 с.
2. Крылов С.В., Петров В.В. *Линии связи и их параметры*. – М.: Радио и связь, 2018. – 280 с.
3. Зима В.Н., Масло И.И. *Сравнительный анализ систем мониторинга сетевой инфраструктуры // Информатизация образования и науки*. – 2025. – № 4. – С. 45–52.