

Д. А. Шергин^{1✉}, А. Н. Поликанин¹

Анализ уязвимостей веб-интерфейсов оптических роутеров

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: shergindanil717@gmail.com

Аннотация. В условиях активного использования телекоммуникационной инфраструктуры на оптоволоконные технологии доля абонентов, подключенных по технологии GPON, достигла максимального уровня за все время, что влечет за собой рост успешных атак на оптические терминалы с веб-интерфейсами управления. Актуальность работы обусловлена отсутствием специализированных автоматизированных инструментов для анализа защищенности данного класса устройств, а также ростом числа кибератак на сетевое оборудование в 2025 году. В данной статье проведен анализ актуальных уязвимостей веб-интерфейсов оптических роутеров на основе методики OWASP с учетом архитектурных особенностей встраиваемых устройств, а также разработан предварительный алгоритм автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров. В качестве нормативной основы анализа использована методика OWASP. В статье также определен перечень уязвимостей, наиболее актуальных именно для данного класса устройств.

Ключевые слова: информационная безопасность, безопасность инфраструктуры, оптический роутер, волоконно-оптическая линия передачи данных

D. A. Shergin^{1✉}, A. N. Polikanin¹

Development of a Virtual Stand for Practical Testing of Active Directory Information Security

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: shergindanil717@gmail.com

Abstract. As the telecommunications infrastructure actively shifts toward fiber-optic technologies, the share of subscribers connected via GPON has reached an all-time high, resulting in a growing number of successful attacks on optical network terminals with embedded web management interfaces. The relevance of this work is driven by the absence of specialized automated tools for security analysis of this device class, as well as the increase in cyberattacks targeting network equipment in 2025. This article analyses current vulnerabilities in optical router web interfaces based on the OWASP methodology, taking into account the architectural characteristics of embedded devices, and proposes a preliminary algorithm for automated software designed to assess the security of optical router web interfaces. The Open Worldwide Application Security Project (OWASP) methodology serves as the normative basis for the analysis. The article also identifies the set of vulnerabilities most relevant to this specific class of devices.

Keywords: information security, infrastructure security, optical router, optic data transmission line

Введение

На сегодняшний день активно развивается инфраструктура широкополосного доступа, которая представляет из себя совокупность из различных техниче-

ских устройств и сетей, обеспечивающих стабильное и высокоскоростное подключение к интернету [1]. Основой данного прогресса является оптическая передача информации, которая происходит посредством внедрения и популяризации волоконно-оптической линии передач, подключаемых к оптическим роутерам, как в частных домах, так и в организациях [2]. Каждое из этих устройств имеет встроенный веб-интерфейс, он служит для управления и настройки роутера. Данный веб-интерфейс является основной поверхностью атаки [3]. Оптический роутер, рассматриваемый как отдельно встраиваемое устройство, в отличие от отдельных корпоративных систем, часто не получает должного внимания [4]. Отсутствие практики регулярного обновления программного обеспечения, версии прошивки роутера, обновления учетных данных, все это подвергает опасности ключевые узлы в сети.

Злоумышленники не игнорируют этот факт. По данным «Информзащиты», за первые семь месяцев 2025 года число кибератак на сетевые устройства – маршрутизаторы, системы контроля доступа и камеры видеонаблюдения выросло на 24% по сравнению с аналогичным периодом 2024 года [5]. Основными жертвами стали организации из сферы информационных технологий и телекоммуникационного сектора, на которые пришлось 63% инцидентов. А статистика Positive Technologies показывает, что доля успешных атак на компьютеры, сервера и сетевое оборудование в период с середины 2024 по середину 2025 год является наибольшей среди всех категорий рис. 1 [6].

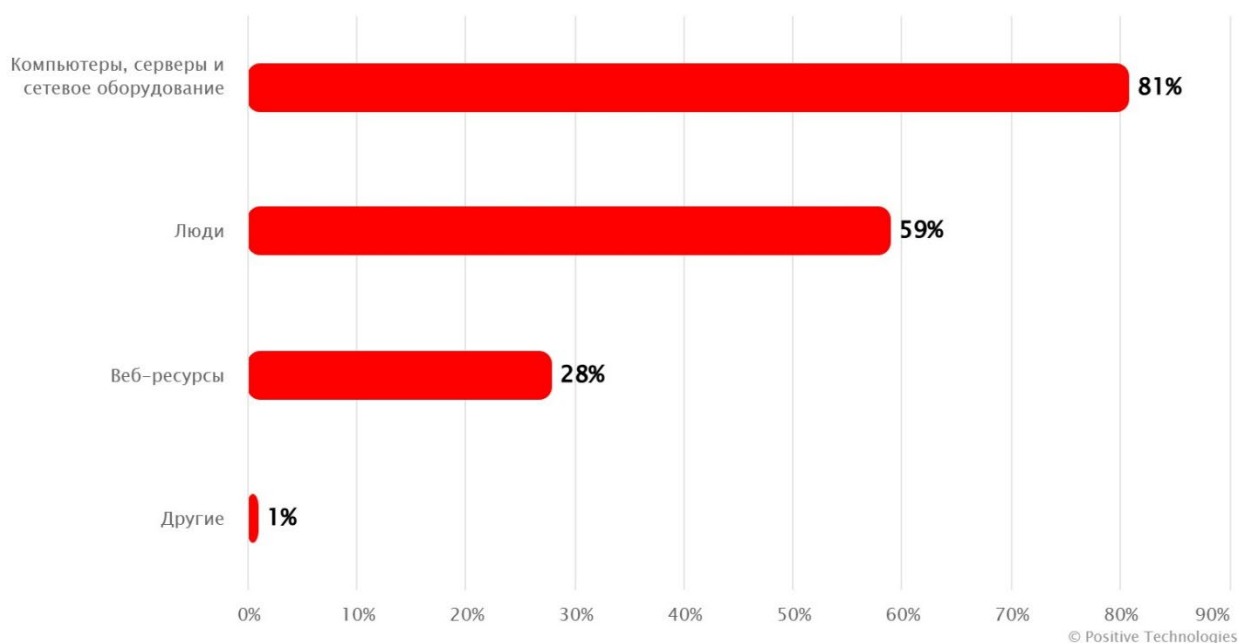


Рис. 1. Доля успешных атак от общего количества

Цель данной статьи: изучить и проанализировать основные уязвимости, которые могут содержать веб-интерфейсы оптических роутеров и разработать

предварительный алгоритм для автоматизированного программного обеспечения анализа защищенности веб-интерфейсов оптических роутеров.

Анализ актуальных уязвимостей

На текущий момент основной документ в сфере информационной безопасности, который определяет наиболее значимые риски для веб-приложений это методика Open Worldwide Application Security Project (далее – OWASP). Так как веб-интерфейс или система управления – это часть веб-приложения, то данную методику можно считать подходящей для текущего анализа [7-8].

В 2025 году OWASP опубликовали свежую подборку актуальных типов уязвимостей для веб-приложений. Они включают в себя:

- нарушение контроля доступа ();
- небезопасная настройка конфигурации ();
- использование компонентов с известными уязвимостями ();
- криптографические сбои ();
- инъекции ();
- небезопасная архитектура приложения ();
- сбой аутентификации;
- нарушение целостности программного обеспечения и данных;
- нарушение в работе системы регистрации и оповещения событий информационной безопасности;
- неправильная обработка ошибок.

Для веб-интерфейса оптического роутера наиболее актуальными уязвимостями были определены: сбой аутентификации, нарушение контроля доступа, инъекции, небезопасная настройка конфигурации и использование компонентов с известными уязвимостями. Выбор именно этих категорий обусловлен не произвольным решением, а совокупностью технических особенностей для данного класса устройств, которые описаны в статье далее.

Сбой аутентификации занимает особое место среди угроз для оптических терминалов. Так как парольная политика встраиваемых устройств часто не контролируется администратором, абонентское оборудование поступает к конечному пользователю с заводскими учетными данными, нередко одинаковыми для всей партии устройств конкретного вендора. Пользователь зачастую не меняет их либо из-за отсутствия технических знаний, либо потому что провайдер не требует этого явно. Так, в устройствах FiberHome AN5506 исследователи обнаружили более двадцати пяти жестко прописанных в прошивке учетных записей [9], а CVE-2021-27137 фиксирует аналогичную проблему в роутерах ZTE. Предсказуемость или полное отсутствие защиты на входе делает все остальное содержимое интерфейса открытым.

Нарушение контроля доступа логически продолжает предыдущую проблему. Даже при наличии формы входа многие CGI компоненты оптических терминалов допускают прямое обращение без предварительной аутентификации, достаточно знать путь. Это следствие архитектуры встраиваемых устройств и их веб-серверов. Разработчики прошивок нередко реализуют проверку сессии не

централизованно, а на уровне каждого обработчика по отдельности, что неизбежно приводит к пропускам.

Инъекции, прежде всего внедрение команд операционной системы (OS Command Injection), реализуются через поля, которые веб-интерфейс передает напрямую в системные вызовы: команды для диагностики ping и traceroute, поля настройки DNS и NTP. Встроенный веб-сервер выполняет их с правами суперпользователя, поскольку оптический терминал представляет из себя однопользовательскую систему без разделения привилегий. В результате злоумышленник может получить полный контроль над устройством через обычную строку в форме ввода. CVE-2023-28771 в оборудовании Zuxel и CVE-2024-21833 в ряде ONT-устройств подтверждают, что данный класс уязвимостей по-прежнему активно встречается в актуальных версиях устройств [10].

Небезопасная настройка конфигурации в контексте оптических роутеров проявляется прежде всего в том, что веб-интерфейс зачастую работает по протоколу HTTP, а не HTTPS, то есть все передаваемые данные, включая учетные данные, не шифруются. Параллельно с веб-интерфейсом нередко остаются включены Telnet и незащищенный SSH со стандартными портами.

Отключение неиспользуемых сервисов и принудительное использование защищенных протоколов является базовым требованием безопасности, которое производители бюджетного абонентского оборудования систематически игнорируют.

Использование компонентов с известными уязвимостями, наиболее системная проблема. Прошивки оптических терминалов строятся на базе открытых компонентов: веб-серверов GoAhead и mini_httpd, интерпретатора BusyBox, библиотек OpenSSL. Производители фиксируют версии этих компонентов на момент выпуска устройства и крайне редко выпускают обновления прошивки, а если и выпускают, пользователи их не устанавливают. В результате устройство, работающее пять лет без обновлений, несет в себе весь накопленный за это время груз известных CVE в своих зависимостях.

Остальные категории из методики OWASP не могут быть применимы к веб-интерфейсам оптических роутеров либо сложно верифицируемы автоматически без доступа к исходному коду прошивки, либо не формируют самостоятельного вектора атаки в рамках анализа именно веб-интерфейса. Это не означает их отсутствия в реальных устройствах, однако их исследование выходит за рамки задач автоматизированного сканирования и требует иных методов – в частности, анализа прошивки [11].

Практическая часть исследования

В рамках практической части исследования были отобраны основные актуальные типы уязвимостей, которые способно обнаружить автоматизированное программное обеспечение и построен предварительный алгоритм будущего автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров рис. 2.

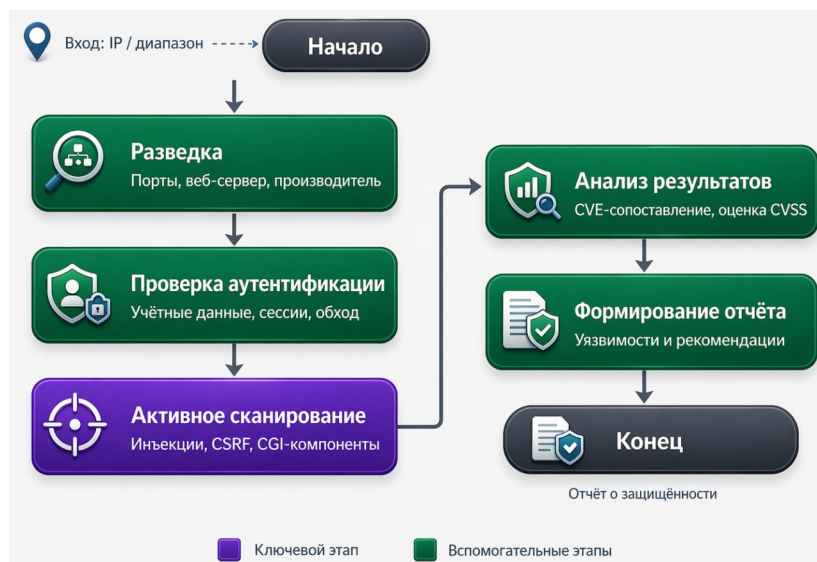


Рис. 2. Предварительный алгоритм программы

Цель данного алгоритма заключается в полном или практически полном покрытии всех поверхностей атаки и поиске уязвимостей, которые учитывают специфику оптических роутеров, их архитектуру и условия эксплуатации

Заключение

Данное исследование является аналитической основой разработки автоматизированного программного обеспечения для анализа защищенности веб-интерфейсов оптических роутеров. Предполагается, что данный анализ поможет лучше разобраться в специфике уязвимостей исследуемых устройств. В результате данной работы были определены актуальные уязвимости для веб-интерфейсов оптических роутеров, учитывающие специфику программных и архитектурных характеристик исследуемых устройств.

Дальнейшее исследование предполагает программную реализацию описанного алгоритма, его тестирование на реальных устройствах и разработку адаптированной метрики оценки критичности обнаруженных уязвимостей с учетом специфики устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кодиров Ф. Э. Технология GPON / Ф. Э. Кодиров, В. Г. Ачилова // Математическое и информационное моделирование: сб. статей. – Тюмень, 2018. – С. 176-181.
2. Оптоволоконные технологии в системах передачи данных / Е. А. Бадеева, Д. А. Усачев, И. А. Чернов [и др.] // Вестник Пензенского государственного университета. – 2022. – № 2(38). – С. 64-69.
3. Магжанов, М. М. Выявление недостатков аутентификации при проверке наличия пользовательской сессии в веб - интерфейсе администрирования домашнего роутера / М. М. Магжанов // фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации : сборник статей Международной научно-практической конференции,

Уфа, 27 декабря 2020 года. Том Часть 2. – Уфа: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2020. – С. 54-57.

4. Казарин О. В. Безопасность программного обеспечения компьютерных систем. - / О.В. Казарин. – М.: Московский государственный университет леса, 2003. – 212 с.

5. CNEWS. «Информзащита»: атаки на сетевое и охранное оборудование выросли почти на четверть в 2025 году. – Текст : электронный // OWASP : [сайт]. – URL: https://safe.cnews.ru/news/line/2025-08-15_informzashchita_ataki_na (дата обращения 01.04.2026).

6. Актуальные киберугрозы для организаций в СНГ: H2 2024 – Q3 2025. – Текст : электронный // Positive Technologies : [сайт]. – URL: <https://ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025> – (дата обращения: 30.03.2026).

7. OWASP. OWASP Top 10:2025. – Текст : электронный // OWASP : [сайт]. – URL: <https://owasp.org/Top10/2025/> (дата обращения 01.04.2026).

8. OWASP. OWASP IoT. – Текст : электронный // OWASP : [сайт]. – URL: <https://owasp.org/www-project-internet-of-things/> (дата обращения 12.04.2026).

9. ANTI-MALWARE. В роутерах FiberHome нашли три десятка бэкдоров и других уязвимостей. – Текст : электронный // ANTI-MALWARE : [сайт]. – URL: <https://www.anti-malware.ru/news/2021-01-18-114534/34750> (дата обращения 07.04.2026).

10. NIST. CVE-2023-28771 Detail. – Текст : электронный // NIST : [сайт]. – URL: <https://nvd.nist.gov/vuln/detail/cve-2023-28771> (дата обращения 12.04.2026).

11. Зонов, А. С. Сканер прошивок оптических роутеров: подходы к обнаружению программных закладок / А. С. Зонов, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2025. – Т. 6. – С. 65-69.

© Д. А. Шергин, А. Н. Поликанин, 2026