



**Федеральное агентство по рыболовству**  
**Федеральное государственное бюджетное образовательное**  
**учреждение высшего образования**  
**«Астраханский государственный технический университет»**  
Система менеджмента качества в области образования, воспитания, науки и инноваций сертифицирована  
ООО «ДКС РУС» по международному стандарту ISO 9001:2015

Институт Информационных технологий и коммуникаций  
Направление 09.03.04 Программная инженерия  
Профиль Разработка программно-информационных систем  
Кафедра Автоматизированные системы обработки информации и управления  
от \_\_\_\_ . \_\_\_\_ 2024 № \_\_\_\_

**Статья**

Выполнил обучающийся группы ДИПРБ-41  
Гогуев Керам Магометович

Астрахань 2024

#### Аннотация.

Развитие информационных технологий и цифровизация обуславливают актуальность вопросов безопасности и эффективного управления информационным трафиком. Данная статья представляет анализ и разработку интегрированной системы управления, объединяющей функции мониторинга, сбора статистики и аналитики. Цель работы заключается в оценке эффективности системы, способной эффективно управлять информационным потоком, обеспечивать безопасность и предоставлять пользователю подробную статистику использования сети.

Работа проводит анализ существующих систем управления информационным трафиком, выделяя их преимущества и недостатки. Уникальность подхода заключается в создании комплексной системы, фокусирующейся на обеспечении безопасности и предоставлении глубокого анализа данных, что является значимым вкладом в область информационной безопасности и сетевого управления.

#### Abstract.

The rapid advancement of information technologies and digitalization underscores the relevance of ensuring security and effective traffic management. This article presents an analysis and development of an integrated management system, combining monitoring, statistics collection, and analytics functions. The aim is to evaluate the efficiency of a system capable of effectively managing information flow, ensuring security, and providing users with detailed network usage statistics.

The paper analyzes existing information traffic management systems, highlighting their strengths and weaknesses. The unique approach lies in creating a comprehensive system focusing on security and providing in-depth data analysis, making a significant contribution to the fields of information security and network management.

## **Введение.**

В эпоху информационных технологий и цифровой трансформации, где поток данных становится ключевым фактором, обеспечение безопасности, контроль и анализ информационного трафика приобретают особую важность. Существенная часть деятельности перешла в виртуальное пространство, создавая новые вызовы в области безопасности передаваемой информации.

В условиях информационного общества системы управления информационным трафиком, мониторинга и анализа сетевой активности становятся неотъемлемой частью сбалансированной работы информационно-аналитической защиты данных. Борьба с киберугрозами, обеспечение конфиденциальности и целостности информации граждан и организаций становятся приоритетными задачами в свете постоянно возрастающего объема передаваемых данных.

Исследование, представленное в данной статье, фокусируется на анализе системы управления информационным трафиком с интегрированным подходом, включающим функции мониторинга, сбора статистики и аналитики. Уникальность данного исследования проявляется в создании комплексного подхода, предоставляющего эффективные методы управления сетевой активностью, обеспечения безопасности передаваемой информации и предоставления пользователям более глубокого анализа данных.

Целью данного исследования является анализ и оценка эффективности системы управления информационным трафиком, с целью выявления ее способности эффективно управлять информационным потоком, обеспечивать безопасность сетевой активности, а также предоставлять пользователям подробную статистику использования сети.

Для достижения этой цели ставятся следующие задачи:

1. Изучение существующих систем управления информационным трафиком.
2. Анализ отличительных признаков аналогов и выявление их недостатков.
3. Проектирование системы, интегрирующей функции мониторинга, сбора статистики и анализа сетевого трафика для оценки эффективности и функциональности разработанной системы.

При проектировании системы мы предполагаем, что интегрированный подход к управлению информационным трафиком, включающий мониторинг, статистику и анализ, позволит повысить эффективность управления сетевой активностью и обеспечить более высокий уровень безопасности передаваемой информации.

Первая часть работы посвящена обзору существующих аналогов систем управления информационным трафиком. Далее мы рассмотрим отличительные признаки этих систем и выявим их недостатки. В последующих разделах представлен процесс разработки

интегрированной системы и проведенный анализ ее эффективности. Заключительная часть содержит выводы и перспективы дальнейших исследований.

### **Основная часть.**

Для достижения поставленных целей и решения поставленных задач, была разработана методология, включающая в себя следующие этапы:

#### **1. Анализ существующих систем управления информационным трафиком.**

Проведенный обзор существующих систем управления информационным трафиком включает в себя анализ таких широко известных продуктов, как NetLimiter, GlassWire и Little Snitch. Каждая из этих систем представляет собой комплексные инструменты, разработанные для мониторинга и управления сетевым трафиком.

Основными недостатками аналогов являются:

- Ограниченные возможности по анализу данных и построению сложных диаграмм.
- Ориентированность больше на управление трафиком, чем на аналитику и статистику.
- Часть функционала является платной.
- Функциональность больше фокусирована на безопасности, чем на детальной статистике и анализе данных.
- Не всегда обеспечивает детализированный отчет о сетевой активности.

#### **2. Определение требований к разрабатываемой системе.**

На основе анализа существующих систем выделены ключевые требования к новой системе управления информационным трафиком. Важными параметрами стали расширенная статистика использования сети, возможность гибкого анализа данных, предоставление рекомендаций для повышения безопасности, а также реализация в реальном времени.

#### **3. Проектирование интегрированной системы.**

С учетом выявленных требований, была разработана интегрированная система управления информационным трафиком. Основой системы стали модули мониторинга, сбора статистики и анализа, взаимодействующие между собой для обеспечения полноценного контроля за сетевой активностью.

Результаты проведенного исследования позволяют сделать следующие выводы:

1. Система успешно интегрирует функции мониторинга, сбора статистики и анализа, предоставляя пользователю обширные возможности контроля за сетевой активностью.

2. Система обеспечивает более детальный анализ данных по сравнению с существующими аналогами, предоставляя пользователю расширенную статистику использования сети.

3. Возможность предоставления рекомендаций на основе анализа данных позволяет эффективно реагировать на потенциальные угрозы и повышать уровень безопасности информации.

На основе результатов исследования предлагаются следующие практические рекомендации:

1. Внедрение разработанной системы в организации, где обеспечение безопасности и эффективного управления сетевой активностью является критическим.

2. Регулярное обновление и модернизация системы в соответствии с новыми требованиями и угрозами в области информационной безопасности.

3. Проведение обучения и поддержки пользователей для эффективного использования всех функциональных возможностей системы.

#### **Заключение.**

Основываясь на проведенном исследовании, разработанная система представляет собой значимый шаг в области управления информационным трафиком, обеспечивая не только высокий уровень безопасности, но и более глубокий анализ сетевой активности. Практическое внедрение данной системы может эффективно поддерживать современные потребности в области информационной безопасности и управления сетевым трафиком.

#### **Литература**

1. Introduction to ArchiMate® in Enterprise Architect [Электронный ресурс]. URL: <https://sparxsystems.com/resources/tutorials/archimate/index.html> Дата обращения: 02.02.2024.
2. Родичев Ю. А. Р60 Нормативная база и стандарты в области информационной безопасности. Учебное пособие. — СПб.: Питер, 2017. — 256 с.: ил. — (Серия «Учебник для вузов»).
3. Netlimiter Docs [Электронный ресурс]. URL: <https://www.netlimiter.com/docs> Дата обращения: 02.02.2024.
4. GlassWire - сетевой монитор и фаервол [Электронный ресурс]. URL: <https://www.comss.ru/page.php?id=2177&ysclid=lsc8bdbqz5716316231> Дата обращения: 01.02.2024.
5. Принципы организации учёта IP-трафика [Электронный ресурс]. URL: <https://habr.com/ru/articles/136844/> Дата обращения: 01.02.2024.